# (IN)SECURE

Issue 39 / September 2013.

FREE

DIGITAL GRAPHOLOGY: IT'S ALL IN THE SIGNATURE

WITH BIG DATA COMES BIG RESPONSIBILITY

PROTECTING CORPORATE ASSETS FROM ATTACK

SECURE A COMPANY'S CHINESE DEVELOPMENT CENTER

## WEB APPLICATION SECURITY

## INSIGHT FROM INDUSTRY LEADERS

## STATISTICS & TIPS

## WEB APPLICATION SECURITY SPOTLIGHT

Hot topics and industry buzzwords come and go, but there are certain aspects of information security that, with time, have become essential. Many considered Web 2.0 to be just a wave of weird project names and mostly useless services. However, with time, some small websites became huge and big software players started offering their own web apps. Here we are a decade later, and we can't even imagine using the Internet without accessing many of these services.

For today's Internet, web application security is not only important, it's essential, and that's why we decided to cover it in this issue.

Mirko Zorz
Editor in Chief

**Visit the magazine website at www.insecuremag.com**

## (IN)SECURE Magazine contacts

Feedback and contributions: Mirko Zorz, Editor in Chief - mzorz@net-security.org
News: Zeljka Zorz, Managing Editor - zzorz@net-security.org
Marketing: Berislav Kucan, Director of Operations - bkucan@net-security.org

## Distribution

## Exploring attacks against PHP applications

Imperva released its September Hacker Intelligence Initiative report which presents an in-depth view of recent attacks against PHP applications. The report also finds that hackers are increasingly capable of packaging higher levels of sophistication into simpler scripts, and identifies PHP SuperGlobals as a prime target that yields a high return on investment.

The PHP SuperGlobal parameters are gaining popularity within the hacking community because they incorporate multiple security problems into an advanced web threat that can break application logic, compromise servers, and result in fraudulent transactions and data theft.

In one month, Imperva's research team noted an average of 144 attacks per application that contained attack vectors related to SuperGlobal parameters. Furthermore, researchers witnessed attack campaigns lasting more than five months with request burst floods of up to 90 hits per minute on a single application.

Imperva researchers observed that attackers are capable of mounting complex attacks and packaging them into simple-to-use tools. However, while an impressive demonstration of attack strength, the PHP method has pitfalls. An application security solution that can detect and mitigate a single stage of the attack can render the entire attack useless.

## NSA's quest to subvert encryption, install backdoors

Journalists from the NYT and ProPublica have joined efforts and have published the most explosive article to date dealing with revelations about NSA spying efforts.

Backed by the documents shared by NSA whistleblower Edward Snowden, they state that the US National Security agency has actively and for years now concentrated on thwarting or subverting encryption efforts via a number of ways, and that their endeavors have largely been successful.

"The agency has circumvented or cracked much of the encryption, or digital scrambling, that guards global commerce and banking systems, protects sensitive data like trade secrets and medical records, and automatically secures the e-mails, Web searches, Internet chats and phone calls of Americans and others around the world, the documents show," they claim.

"Many users assume — or have been assured by Internet companies — that their data is safe from prying eyes, including those of the government, and the NSA wants to keep it that way. The agency treats its recent successes in deciphering protected information as among its most closely guarded secrets, restricted to those cleared for a highly classified program code-named Bullrun."

They pointed out that after the NSA lost the very public dispute in 1994 about whether it should be allowed to fit a backdoor into all encryption, they decided they won't going to be stymied by this setback and opted to simply continued their efforts - this time in secret.

They did not concentrate on breaking encryption as much as making its use irrelevant. They did start using faster and faster supercomputers for breaking cryptographic keys, but they also, among other things:

• Secured the collaboration - either voluntary or legally forced - from US and foreign Internet and telecom companies to gain the needed access to the communications they wanted to review before they were encrypted. Alternatively, when neither of those two approaches worked, they would steal the companies' encryption keys or secretly alter their products to contain a backdoor only known to the NSA.

• Hacked into computers / endpoints before the messages were encrypted.

• Influenced the US National Institute of Standards and Technology (NIST) and the International Organization for Standardization to adopt an encryption standard that has been made by the NSA to include a weakness known only to them.

All these things were, of course, done in secrecy. "The full extent of the NSA's decoding capabilities is known only to a limited group of top analysts from the so-called Five Eyes: the N.S.A. and its counterparts in Britain, Canada, Australia and New Zealand," the reporters shared.

"The NSA has turned the fabric of the internet into a vast surveillance platform, but they are not magical. They're limited by the same economic realities as the rest of us, and our best defense is to make surveillance of us as expensive as possible," Bruce Schneier pointed out. "Trust the math. Encryption is your friend. Use it well, and do your best to ensure that nothing can compromise it. That's how you can remain secure even in the face of the NSA."

It's interesting to note that both the NYT and ProPublica have been asked by US intelligence officials not to publish this last article, saying that "it might prompt foreign targets to switch to new forms of encryption or communications that would be harder to collect or read."

However, both publications have declined to comply with that request.

## New discovery will allow large-scale quantum cryptography networks

Researchers from Toshiba have discovered a method to build quantum cryptography communication networks with a far greater scale than ever before. It will allow quantum cryptography to be used beyond its current niche applications, for example as part of the Smart Community Networks that will manage and control energy generation and consumption in the future.

Quantum cryptography shows great potential to revolutionize the way sensitive data is protected. It can be used to distribute secret digital keys with a security that is not vulnerable to advances in computing, mathematics or engineering, and means any hacker that "taps" an optical fiber will be detected. At the same time, it could become the first prevailing technology to harness the peculiar laws of quantum physics.

However, major obstacles still have to be overcome in order to make quantum cryptography viable for widespread use, particularly regarding the number of users than can be connected to a single network. Up until now, implementing a quantum cryptography network has required an elaborate photon detector for each additional user.

The Toshiba team has discovered a technique to allow many users to share a single detector and thereby greatly reduce the complexity of the network. The breakthrough means that with current technology, it would be possible for 64 users to connect to a single detector in a Quantum Access Network.

## Barracuda WAF now on Windows Azure

An Intel study, “What’s Holding Back the Cloud,” (May 2012), reported that 87 percent of the IT professionals surveyed were concerned about security and data protection and 28 percent have experienced a public cloud–related security breach, an increase over the number of breaches experienced in their traditional IT security infrastructure.

With the new cloud edition of the Barracuda Web Application Firewall (www.barracuda.com/WAF) that can be deployed on Microsoft Azure (www.barracuda.com/WAFonAzure), organizations now have the flexibility to deploy the same strong protection in the cloud or on premise.

The Barracuda Web Application Firewall has blocked over 11 billion real world attacks since 2007. Organizations using the Barracuda Web Application Firewall get a strong security platform that performs deep inspection of all Web traffic, enabling it to provide a wide range of attack prevention capabilities at both the network and application layers. These include SQL injections, XSS attacks, session tampering and buffer overflows as well as volumetric and application-based DDoS protection.

As a full proxy, the Barracuda Web Application Firewall blocks or cloaks attacks, while preventing outbound data leaks of information such as credit card or Social Security numbers. In addition, the Barracuda Web Application Firewall mitigates broken access control to applications by preventing cookie tampering and corruption of an application’s access control system. With the most flexible range of deployment options that span hardware, virtual and cloud, the Barracuda Web Application Firewall provides a complete security solution for all of your applications in any environment.

## 61% of IT pros don't report security risks to executives

A new Ponemon Institute study examined the disconnect between an organization's commitments to risk-based security management and its ability to develop the collaboration, communication styles and culture necessary to security programs effective across the organization.
Key findings from the survey include:

- 61 percent said they don't communicate security risk with senior executives or only communicate when a serious security risk is revealed
- 38 percent said that collaboration between security risk management and business is poor, non-existent or adversarial. 47 percent rated their communication of relevant security risks to executives as "not effective".

Dr. Larry Ponemon, chairman and founder of the Ponemon Institute said: "Even the most secure and sophisticated organizations experience risk because there are too many variables in play. Effective communication and collaboration across the organization are crucial in mitigating this risk."

## Arbor Networks acquires Packetloop

Arbor Networks has acquired Packetloop, an innovator and provider of Security Analytics. Terms of the deal were not disclosed. Packetloop's solution delivers real-time, network-wide situational awareness through a combination of packet capture, big data analytics, security forensics and visualizations that help enterprises identify malware, targeted attacks and attackers. Their capabilities complement Arbor's NetFlow visibility, anomaly detection, application intelligence and identity tracking.

## Are you nomophobic?

Nomophobia – the fear of being out of mobile phone contact is still a very real problem for the majority of the population. Over 54% admit to suffering from the condition with women 17% more likely to suffer from it than men. The study of 1000 people in employment, sponsored by AppRiver and conducted by OnePoll, found people are so obsessed with the need to be connected to their phones that even when away on annual leave, 42% will take them down to the beach.

While it might seem harmless, there is a serious aspect of these habits. Fred Touchette, security analyst at AppRiver explains, "It's clear that we're a society totally reliant on our phones not only for personal use but business too. Even when on holiday, lying in bed or on a dinner date the study revealed many of us just can't help looking at our emails, no matter the time or situation. What is worrying is that, with so much information stored on them - from confidential office information, contact details, emails, photos, bank details, etc., when they get lost or stolen and end up in the wrong hands the information can easily be exploited."

Just 50% of people bother to secure phones with a password, or any other form of security, and 70% have no way to remotely wipe the device. Fred concludes, "Our advice is always protect your phone, at the very least with a password, and if you're using it for work get your IT department to secure them with a little more, such as encryption."

## Persistent adversaries can identify Tor users

Using the Tor network will not you grant perfect anonymity - in fact, a group of researchers from the US Naval Research Laboratory and Georgetown University say that "Tor users are far more susceptible to compromise than indicated by prior work."

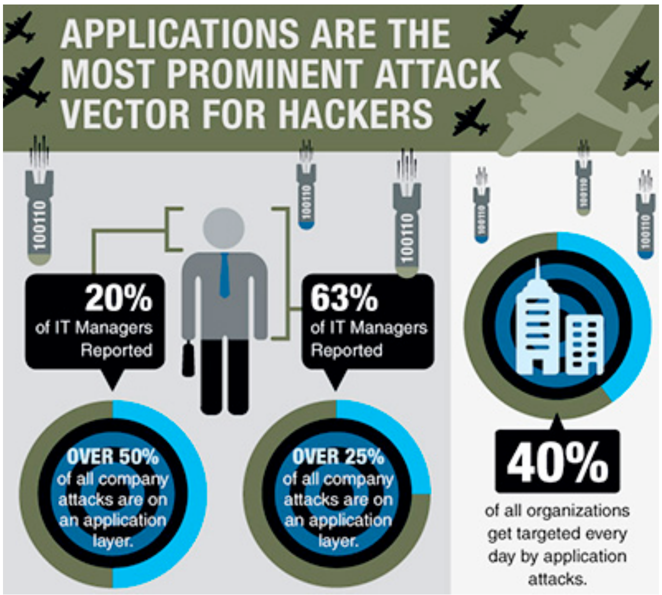
"Tor is known to be insecure against an adversary that can observe a user's traffic entering and exiting the anonymity network," the researchers shared in their paper. "Quite simple and efficient techniques can correlate traffic at these separate locations by taking advantage of identifying traffic patterns. As a result, the user and his destination may be identified, completely subverting the protocol's security goals."

They pointed out that prior research didn't take in account indications of how secure a type of behavior is, nor the fact that a single organization often controls several geographically diverse autonomous systems (AS) or Internet exchange points (IXP). "That organization may have malicious intent or undergo coercion, threatening users of all network components under its control," they suggest.

In order to get to an accurate assessment of the peril Tor users are under when using it, they have developed an analysis framework for evaluating the security of various user behaviors on the live Tor network, a model of a network adversary that includes an accurate system for AS path inference and an analysis of the threat of IXPs and IXP coalitions, and a realistic Tor path simulator.

"Our analysis shows that 80% of all types of users may be de-anonymized by a relatively moderate Tor-relay adversary within six months. Our results also show that against a single AS adversary roughly 100% of users in some common locations are de-anonymized within three months (95% in three months for a single IXP)," they shared.

## Most security managers don't trust their apps



Application vulnerabilities are a major factor in the cybercrime game. More than 500 CISOs and Security managers have been interviewed by Quotium about the security state of their applications, the frequency of attacks in their organizations and the solutions in place to mitigate these security threats.

The first fact that arises from the study is that most of the big organizations interviewed currently have processes in place to test their web applications vulnerabilities. Most of them use penetration testing services, automated testing tools - mostly applications scanners or static code analyzers – or web application firewalls to secure their assets.

However, a majority of security managers are unsure of the current level of their application security state and do believe that a hacker could manage to exploit their applications.

## NSA internal audit reveals thousands of privacy violations

An internal NSA audit document and several other seen by The Washington Post journalists prove that there have been over a 1,000 violations of FISA and presidential executive orders each year since the agency was granted broader surveillance powers in 2008.

Some of the violations were caused by computer errors and other by operators. For example, in 2008, a computer mistake has resulted in the interceptions of calls made from Washington D.C. (US area code 202) instead of those made from Egypt (international dialing code 20). As a reminder: 2008 was an election year.

In a statement reacting to the piece, a NSA official stated on the record that the NSA is "a human-run agency operating in a complex environment with a number of different regulatory regimes, so at times we find ourselves on the wrong side of the line."

And they are right. The problem is not in the fact that errors are made, but that they are swept under "statistical addendum" rugs and reports of this kind are often not shared with people who should decide whether the NSA should be allowed to continue with the practices or not. If they are, they often don't include the actual number of innocent American citizens that have been affected.

"The NSA uses the term 'incidental' when it sweeps up the records of an American while targeting a foreigner or a U.S. person who is believed to be involved in terrorism. Official guidelines for NSA personnel say that kind of incident, pervasive under current practices, 'does not constitute a . . . violation' and 'does not have to be reported' to the NSA inspector general for inclusion in quarterly reports to Congress," writes Gellman, and points out that once added to the databases the communications of Americans may be searched freely if there are not other restrictions in place.

In addition to this, Carol Leonnig reports that the Foreign Intelligence Surveillance Court does not have the means to verify whether government reports regarding the spying programs are accurate and whether the included mistakes are actually unintentional, and is, therefore, forced to take the information at face value.

"The court's description of its practical limitations contrasts with repeated assurances from the Obama administration and intelligence agency leaders that the court provides central checks and balances on the government's broad spying efforts," she writes, adding that several US legislators who are members of the House and Senate intelligence committees have said that they are limited in their efforts to question NSA officials about the work they do.

## Facebook spamming is a hugely lucrative business

Italian researchers that have previously unearthed the big business behind fake Twitter followers have now calculated that Facebook spammers are raking in as much as $200m every year. The team headed by Andrea Stroppa and Carlo De Micheli has been searching for and analyzing Facebook spam, the fake fan pages that serve it, and the third-party scam sites to which the spammy links lead to.

They have discovered that creating fake fan pages is a thriving business. "The spam posters get paid an average of $13 per post for pages that have around 30,000 fans, up to an average of $58 to post on pages with more than 100,000 fans," De Micheli shared.

## Would you publicly report a security breach?

Research by AlienVault revealed that only 2% of surveyed EU companies would be willing to go public should they suffer a security breach. 38% opted to inform the relevant authorities and 31% said they would tell their employees. A mere 11% said they would share the information with the security community.

Organizations who suffer a security breach face a Catch 22, said Barmak Meftah, President and CEO of AlienVault. "On the one hand, publicising a breach would help other businesses avoid falling prey to attacks. On the other, damage to your brand and reputation could be significant."

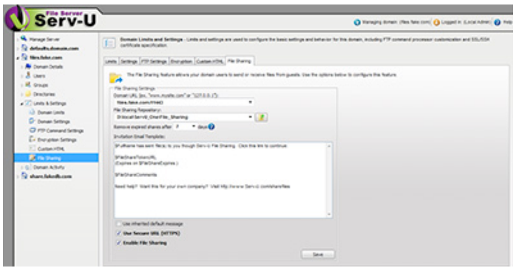
He says this is even more pertinent when considering the European Commission's proposed overhaul of its data protection laws, that will see companies face fines of up to 2% of their global annual turnover should they suffer a breach. "This would see the fallout from a breach being potentially disastrous not only for a company's good name, but also for their bottom line.”

## Windows 8 shouldn't be used on government computers, say IT experts

Internal documents of the German Ministry of Economic Affairs perused by a reporter of news outlet Zeit Online show that IT professionals working for the government don't consider computers running Windows 8 secure enough for government and business use.

Given the latest news about Microsoft collaborating with US intelligence agencies, the German Ministry of Economic Affairs believes that the company can ultimately be forced to allow the agency direct access to foreign computers.

## Secure enterprise file sharing from SolarWinds



SolarWinds announced new secure file sharing capabilities to its managed file transfer solution, SolarWinds Serv-U Managed File Transfer (MFT) Server.

Serv-U MFT Server (www.serv-u.com) provides secure file transfer – and now file sharing – hosted on Windows and Linux machines. It enables users to support file uploads and downloads using FTP, FTPS, SFTP, HTTP and HTTPS over IPv4 or IPv6 networks. Administrators can control access to files, monitor activity, automate notifications, and configure from any location through a secure Web management console.

# Dear CSO, do you know how to build security culture?

by Kai Roer

What do you really know about security culture? I am going out on a limb here and claim you know very little, if anything at all.

Your day job is about security, and like most CSOs out there, you have an IT background. Most likely, you are still quite handy with the tech, and if forced to, you are able to set some firewall rules, and possibly even change a routing table or two.

You are likely to have picked up on the trend that people are the weakest link in your security chain, and you most probably have some sort of user awareness training in place. You know it is important, and everybody does it, at least that is what your training supplier tells you. And you can tick that box off on your compliance sheet.

Like many other CSOs, you are also likely to not have reached the level of user awareness you imagined and hoped for, and you may have reached the level of frustration of Dave Aitel, who last year went all out and said that "You should not train employees for security awareness".

The human mind has many flaws. Yours does, and mine does too. We are jumping to conclusions without considering all the relevant information. We are constructing facts from fiction, because it makes us able to do what we want, not what is right. We are extremely vulnerable to peer pressure. We are blind to things we do not know about.

This implies that even if you know a lot about security, you are likely not to know a lot about people, how they function, and how groups form and interact. You may (and probably do) think that you know a lot about people. Consider this, then: do you have a minor, or a major, in a social science? Do you know what social science is, anyway?

Social sciences is a collective term describing the different sciences about humans, human interaction and groups, including (but not limited to):

- Psychology
- Sociology
- Social anthropology
- Organizational theory.

One of the things we have learned from social sciences and their research is that humans come pre-wired with biases. These biases impact how we see and perceive the world, how we respond to it, and how we interact with it. Let’s take a look at the blind spot bias which I mentioned above.

The blind spot bias works to help you focus on what you have to focus on, and avoid being interrupted by thoughts that are not relevant. The flip-side of the blind spot bias is that it is very hard to accept things you do not know. For example, if you have grown up in the western world, you are likely to consider insects in any form to be inedible. Traveling to a part of the world where insects are part of the human diet, blind spot bias may have you respond with disbelief and decide that locals are crazy, wrong and plain stupid. If, however, you grew up in an environment where insects are a regular part of the diet, you would consider such a response from a visitor strange and stupid.

The blind spot bias works against you by making it very hard for you to accept and realize other possible solutions, and the further away the solution is from your "known environment", the harder the blind spot bias will oppose such solutions.

Setting out to create and maintain security culture in your organization is not a job you should be doing alone.

Another interesting bias is the confirmation bias: the need to find evidence that confirms our theories and beliefs, which makes us disregard information that contradicts them. If we use Dave Aitel as an example (sorry, Dave), the confirmation bias made him see only the faults of and problems with user awareness trainings. The more proof he found that he was right, the less likely he was to look for contradictory evidence.

By theorizing that you have no knowledge about culture and social sciences, I'm making the same mistake right now. Instead of doing serious research, I just look at the CSOs I know to confirm my theory. Then I apply another bias to my somewhat limited sample of evidence - I generalize. By generalizing, I take whatever information I have, and scale it up to make it applicable to what I have set out to prove.

As a writer, I'm allowed to make such errors to make a point. As a scientist, doing the same should be and is a deadly sin. As a human, I'm always going to make these errors. It is, according to science, hardwired in our brains. My responsibility is to exercise strong self-control, and to be humbled for and by the errors I make.

"What does this have to do with security culture?," you may ask. Let us define culture. According to the Oxford dictionary, culture is "the ideas, customs and social behaviors of a particular people or society". By this definition, we see that culture is about the things we all do in a group of people. Security culture may then be the "ideas, customs and behaviors that impact security, both positive and negative, in a particular group of people".

In that definition, security is only a part of the whole, just like security is in most organizations around the world. It is your part, that is right. As I demonstrated above, you are likely the expert on security, but not on human behavior. Setting out to create and maintain security culture in your organization is not a job you should be doing alone.

Consider this instead: If you know security, who knows culture in your organization? And this: why don't you work to build your security culture with those who know culture and human behavior?

Kai Roer is a Senior Partner at The Roer Group (www.roer.com).

# How to secure a company's Chinese development center

by Michael S. Oberlaender

Suppose you have a company - let's call it WorldSoft - that is planning to do a big part of its software development in China. A fairly new and growing economy, access to inexpensive but highly educated development resources from local universities, one of the most important future Asian markets and similar motivations might be the reasons for that. Given the multiple and complex challenges, how would it be possible to secure that from a corporate perspective?

We will go first through a couple of basic assumptions, define the known facts, and picture the assumed risk profile before diving into the plethora of counter measures that are both possible and (most likely) necessary at the various levels (organizational, process, technological) of the organization.

The shown options are prioritized already (not withstanding there are always reasons you could prioritize differently), and suggest that you start at the organizational level, go then into the process level, and finally support all this with the technology level (not vice versa as far too many organizations do) in a combined fashion as shown in the summary section of this concept study.

WorldSoft uses a globally distributed development environment using scrum and similar methods. IP laws are enacted based on WTO and World Intellectual Property Organization (WIPO) memberships and also China has signed a Trade Related Intellectual Property Agreement (TRIP) - but these are not enforced.

WorldSoft's products and solutions address a highly competitive market, major other players / competitors compete both for market share and the most comprehensive product solution in WorldSoft's product space. The company has worldwide customers in all industries, governments, and security relevant organizations such as military or critical infrastructure.

The global economy is in a weak phase where recession and rebound are alternating, the level of uncertainty is very high and competitive advantage can make the difference for a company to succeed or fail entirely. Preventing industrial espionage or unauthorized access to IP data is therefore critical. Furthermore, the built trust with the existing customer base about code quality, stability, integrity and integration is very important to defend the company's reputation.

Acquired companies or third parties such as service or outsourcing partners must also be integrated into the security environment without changing the risk profile in an uncontrolled fashion. Currently software companies tend to allow administrative rights for developers, and often have no general blocking mechanism in place for mobile data storage such as thumb / USB drives, DVD, and other such items.

## Foundational assumptions / known facts

Security is complex and cannot always be solved with a "one-size fits all" approach, especially when business requirements must be considered / given preference.

Concepts such as defense-in-depth, need-to-know, minimum privileges, standards where possible, risk-aligned controls, re-use of certified solutions, attack-surface-reduction, increase attack-costs, security-by-design (www.createspace.com/4043003) (not by obscurity), etc., should be applied entirely. Still, the weakest link most likely will get exploited, security is not 100% and instead an agreed upon risk profile.

To reach this aspired level of security, it must be addressed at all structural levels: organizational (people and policies), process (end-to-end), and technological (automated vs. manual; physical and logical). Prioritization is always required to maximize benefit and minimize necessary expenses, and also to focus on the most important assets / risks / issues first. Potential solutions shall be created to minimize business impact and inconvenience for employees / third parties, etc. This will reduce the risk that they will be objecting to / bypassing security measures. Proactive solutions are way more efficient and effective than reactive ones, and are to be preferred. However, in some cases a reactive approach is cheaper, and also still necessary (Incident Response).

## Risk potential

High level risks:

- Loss of integrity: trust / brand reputation if breached / hacked, corrupted data (code or configuration data), corrupted cloud services or business intelligence data -> could impact decision-making. If WorldSoft locations / infrastructure are used in another (external) attack (i.e. against critical infrastructures), also potential liability.

- Loss of confidentiality: Intellectual Property (IP), strategic business plans, designs, sensitive customer data, specific know-how, wiretapped communications. Industrial and state espionage. Potential liabilities (customers, third parties, joint ventures, shareholders).

- Loss of availability: either at the network level (Great Firewall of China), or the data centers (non-reliable infrastructure, regional conflict, counter-attack on critical infrastructure such as energy / power plants). Potential liabilities (customers, shareholders).

External threat actors:

- People (competitors, nation state, hacktivists, former employees) or elementary (natural disasters), power outage, etc.

Internal threat actors:

- People (non-intentional errors [employees or 3rd parties], disgruntled employees, infiltrated spies [competitors or state sponsored]).

- Based on publicized research, the vast majority of man-made attacks are happening via (automated) malware and hacking on both servers and clients / user devices (end points), followed by some physical attacks, some social engineering and finally misuse (by authorized people).

- Hacking by an APT is currently the highest potential man-made threat and risk.

After having shown the risk potential, we now look into the various countermeasures at the different levels of any organization.

## Potential countermeasures at the organizational level

At the organizational level (that is people and policies), we can do the following:

1. Global multi-level policy structure that defines clear objectives and acceptable risk levels (incl. BCP), and provides for regional or local additions / changes. Standards and procedures, ITIL and similar change controls prevent errors (unintentional wrongdoing).
2. Contracts with employees and third parties that will specify clearly the duties to protect IP, copyrighted material, internal and confidential information handling, access and change of information, need to know and the other principles such as not lending passwords, physical access cards, smartcards, etc., to others. The contracts should spell out clear fines and enforce those with pre-paid escrow accounts (for third parties), or choose third parties with compensating assets in other countries such as EU / US.
3. Have NDAs / CAs (Confidentiality Agreements) signed by all employees, contractors, subcontractors, etc., as part of their employment relationship. Prefer contractors with (indirect) assets in EU / US where litigation is enforced and binding.
4. Require a Certificate of No Criminal Conviction ("CNCC") from the potential employee (especially for leadership positions), use these both before hire and during tenure. Observe and act upon changes in behavior – a disgruntled employee will often show warning signs.
5. Regularly educate all employees, contractors, third parties about their expected behavior, let them sign their agreement and participation of those trainings. Awareness programs that are positive and contain interesting and professionally made material will change behavior (IP and security in general). Top management must adhere to all measures to "set the tone at the top". Incentivize positive behavior, (aggressive) profit sharing schemes and leverage local JVs to prevent their need for infringement.
6. Use detectives / trusted parties (non-government) to identify misuse or illegal copies. Adhere and enforce the procedures in case of wrongdoing to deter others.
7. Protect IP rights before enforcement is needed. To reduce trademark squatting, register early.
8. Job rotations could also help find fraud and reduce collusion.
9. Acquisition of other companies: do risk assessments of their environment (at the organization, process, and technology levels) before connection to infrastructure.

The next organizational level is the process level where is defined how things shall work, and how a company runs its business. At this level, a lot of improvements should be made, this is part of the "secret sauce" of any organization, and those most sustainable will have highly efficient and effective processes. One could argue that this still is all organizational, but on the other hand we strive to structure the approach in the best way and that is why I present it this way.

## Potential countermeasures at the process level

• Design all security measures into the right chain link within the process (efficient, effective, easy).

• (Document and) automate processes to reduce error and unintentional wrongdoing.

• Ingrain security requirements in the SDLC (from the beginning to the end) and approve only those solutions where the security requirements are reached.

• Split code development such that no one has access to the entire code / product base but only those snippets that are needed (see technology: source code vault, Access Control).

• Separate development, testing, piloting, and production and adhere to strict change control for transfers.

• Design and operate a development environment that doesn't need local storage and installations (see VDI on next page).

• Digitally sign, fingerprint, and watermark code that has been verified and is secure. Integrate those used technologies.

- Verify customer licenses and proper code use when doing support for that customer.

- Classify all documents upon creation and adhere to the processes accordingly throughout their lifecycle.

- Define and optimize the entire Incident Response process.

- Provide employees who need to access secure areas a locker room to prevent mobile devices in those areas.

- Before entering into partnerships with third parties (providers, etc.), assess the potential risks and do security process verification.

Now I will describe how to best support these above organizational and process security controls by leveraging technology solutions in their best potential ways. It is again important to note that not one single technical solution will solve all problems. Instead, the useful integration of the various products with a well-thought-through architecture will support the intended security level.

## Potential countermeasures at the technological level

Technological (automated vs. manual; physical and logical):

- Physical controls such as fences / gates, cameras, AC, secure zones, no cell phones and flash drives, etc., tracking of people within the data centers or other secure zones, assigned accompanying guards for third party access to sensitive areas. Compartmentalization approach for important assets.

- Create different user profiles (classes) with access accordingly to their roles (sales not in developer area / network segment, etc.)

- Leverage smartcards with biometry where possible and integrate physical and logical contexts.

- Use a VDI (Virtual Development Infrastructure) in trusted locations with VPN and other encrypted connections.

- Use network segmentation (Development / Test / Production), NGFW, VPNs, VLANs, NAC, DLP, SIEM, WAF, etc. with an integrated design architecture.

- Use static and dynamic code analysis tools, black-box and white-box scanners.

- Secure servers in data centers, antimalware, antivirus, firewalls, strong authentication and AC, backup, DR (also against the natural threats).

- Secure storage networks (SAN / NAS etc. / encryption / AC / separation, [AV / AM]) – incl. DR.

- Secure endpoints with antimalware, AV, personal (endpoint) firewalls, PKI / encryption / signature / hash, proper SW installs, backup-tools.

- Track local port usage, data flow, DLP, find code signatures, leverage RMS, SIEM, etc. dashboard, use a strict code-tracing technique to monitor copying.

So far the potential solution options – as you can see they are manifold.

## Differentiated but also integrated approach

Based on the aforementioned options, it is best to prioritize the risks and compare the value at risk with the associated costs of mitigating controls. The combination of counter measures at the three different layers (people, process, technology) is best, therefore an integrated approach between risk and corporate security, legal, IT security, product security, cloud security, service and other units should be used.

What you don't measure you can't really manage, so a few KPI examples here:

- Percentage of employees that have their background verified (with a CNCC, prior employment, claimed education).

- Percentage of contracts with third parties with NDA / CA signed that's enforceable (s.a.)

- Number of performed and validated awareness educations and signed records.

- Percentage of registered IP items (of all assets) in China vs. other locations or global average.
- Percentage of customers found with unregistered / counterfeited WorldSoft products or pieces in China.
- Percentage of unsecured ports / thumb drives seen in the environment.
- Percentage of solved incidents from IR and any further details on that.

Finally, the business aligned security strategy should be adapted based on the success of the measures and seen change in measurements.

***Hint:*** To get the necessary active support from management and employees, incorporate security into the(ir) annual performance goals.

Michael S. Oberlaender (www.linkedin.com/in/mymso) is a world-renowned security executive, thought leader, author and subject matter expert and has worked in executive level security roles (CSO / CISO) and in IT both in the US and EU for over two decades. He holds a Master of Science (Physics) from the University of Heidelberg, Germany and is CISSP, CISM, CISA, CRISC, GSNA, ACSE certified. His new book - "C(I)SO - And Now What?" - is available at www.createspace.com/4043003.

Want to reach a large audience of security pros by writing for (IN)SECURE?
STOP
Send your idea to mzorz@net-security.org

# WEB APPLICATION SECURITY SPOTLIGHT

Stephen Pao, GM, Security Business at Barracuda Networks, on web application security

The state of web application security in numbers

Web application exploitation with broken authentication and path traversal

Joel Smith, AppRiver CTO, on web threats

# Stephen Pao, GM, Security Business Barracuda Networks on web application security

by Mirko Zorz

Stephen Pao serves as General Manager, Security Business, at Barracuda Networks, where he is responsible for strategic product direction, definition, program management, and development for all of the company's security products. In this interview he talks about web application security threats, offers tips for securing applications in the cloud, and much more.

**What are some of the most overlooked web application security threats at the moment?**

When it comes to web application security, the media likes to focus on new and exotic attacks. You read articles about APTs, DDoS, BEAST TLS attacks, and other high publicity exploits. However, in regard to web applications, it’s the same old attacks that are causing the most problems. These are the tried-and-true SQL injections that have been an issue for more than a decade, yet they are still in the OWASP Top 10. This is mainly due to the huge amount of sensitive data stored in databases that are accessed by web applications, and therefore prime targets for criminals. All it takes is a simple coding error or an unescaped input to open the door to a serious breach. It is not sexy stuff but it is critically important to secure against these old but effective attacks.

The problem is compounded with the move from hardware to virtual—and now to cloud deployments. Often security is forgotten when the focus shifts to deployment modes and how to leverage new deployments for cost savings and efficiency. The biggest threat in this context isn’t new and exotic attacks, but the introduction of gaps or blind spots when organizations move applications to different deployment modes. Fortunately, what works in the on-premises hardware server world is easily transferable to virtual and cloud worlds. As long as organizations remember to deploy the same security processes that have worked for them previously, there is a good chance that the same security will continue to protect their applications.

**What advice would you give to security professionals who want to make sure their applications in the cloud have the same level of security as traditional on-premises applications?**

Conceptually, the way to look at the cloud is simply as a new way to deploy an application. We've already seen the migration of applications from physical to virtual servers. Cloud migration is simply the next step. With cloud deployments, there may be substantial implementation and economic differences. There may also be differences in ownership of assets and distribution of tasks within organizations. However from an application security perspective much remains the same.

In a cloud environment, applications are still vulnerable to the same SQL injections, DDoS, and other attacks experienced by on-premises applications. This is because the underlying protocol, source code, and business logic associated with the applications are the same, regardless of deployment mechanism.

Consequently, things like form input fields, cookies, HTTP/S protocol, and SSL encryption have the same potential vulnerabilities. Consequently developers need to use secure coding practices as well as deploying a device like a web application firewall (WAF) for cloud applications. The good news is that security expertise and best practices are readily transferable once the operational and deployment aspects are figured out.

The primary challenge is that sometimes the current WAF vendor does not have a model that can run on the cloud platform of choice. This is especially the case with vendors that provide WAF as part of their application delivery controller (ADC) platforms. Organizations could wait for their existing vendor to catch up, but given the rapid adoption of the cloud, it may be better to consider products that are readily available today. There are a few leading vendors (including Barracuda) that have made the investment in delivering WAFs in the cloud that can be readily plugged into cloud platforms today.

**What are the challenges involved in protecting large web applications that are concurrently used by a vast number of consumers?**

Coding for small applications is not different than coding for large applications. But the sheer scale and complexity of organizations can create challenges. Simply put, organizations must manage all of the moving parts and the changes to the website without introducing any issues.

The more people and different technologies involved, the higher the risk of security misconfigurations, code errors, or becoming the target of hacktivists or criminals. For this reason, we stress that the best way to address the issue is to take a systematic approach and analyze the people, processes, and technologies involved. It is only with a coordination of all three aspects that we can hope to mitigate existing and future risks.

**Earlier this year we've seen automated botnet attacks targeting WordPress. What type of advanced protection would you recommend to the users of similar web platforms?**

At Barracuda, we've dealt with botnets for more than 10 years. Many of the botnets we see today were yesterday's spam-bots. As an industry, we've made excellent progress in decreasing the efficacy of spam and viruses over email. The bad news is that these same bots are now being repurposed for other activities like DDoS against WordPress, banking websites, and other valuable web assets.

When dealing with bots and in particular DDoS, there are two types of attacks to consider. The first are volumetric attacks where bots overwhelm an application with a flood of traffic. Fortunately there are a number of solutions to handle a volumetric DDoS attack today:

1. Content delivery networks (CDN) can provide the volume and scale against simple volumetric attacks.
2. Network firewalls and WAFs can provide on-premises protection against volumetric attacks.

The second category is application DDoS attacks that are best handled by WAFs because of their abilities to inspect traffic at the application layer. The ability to control application protocols and application logic enables WAFs to throttle asymmetric application DDoS attacks like Slowloris. In short a good WAF can:

- Fingerprint client requests to detect bots or malicious clients
- Inject CAPTCHA or other automated challenges to slow down DDoS
- Limit client access based on GeoIP
- Protect against HTTP or SSL protocol-based attacks
- Rate control or cut off client based on risk profile or IP reputation
- Block access form anonymous proxies or TOR network nodes.

It is equally important to select a good WAF vendor with flexible deployment options that give you the ability to deploy WAF technology to secure on-premises or cloud applications. Ideally the vendor should provide hardware, virtual, and cloud-deployable models, giving organizations the ability to scale and/or re-architect their deployments to meet the organization's needs.

It is equally important to select a good WAF vendor with flexible deployment options that give you the ability to deploy WAF technology to secure on-premises or cloud applications.

**Securing applications against automated attacks can be very time consuming. What steps can an organization take to make sure their web applications are secure at all times?**

Application threats are dynamic and consequently, defenses against automatic attacks should be dynamic as well. While there are no silver bullets, using a systematic approach can greatly mitigate risk. This does not mean simply chaining security devices. It's more effective to implement both a technological and a people/process solution.

A good example is the process a large Fortune 100 company that we are working with today follows. For every application, they categorize and assign a risk profile prior to deployment. For example, if it is an Internet facing application handling sensitive data, there is a stringent security assessment that includes both a vulnerability scan, a penetration test by a third party, and a web application firewall deployed in front of the application.

On the other end of the spectrum are the "internal only" applications with static information. These only need to go through a basic audit and a basic vulnerability scan. The point here is that there are processes based on risk profile in addition to technology that greatly reduce risk.

Finally, one of the under-appreciated processes in place is the segmentation of responsibility between the development, security, and infrastructure teams.

The development team does not have any input into the security process and cannot modify procedures or configure the security tools. The security team has full responsibility for keeping the applications safe and has the authority to block applications from being deployed. The infrastructure team deploys the application and enforces firewalls, WAFs, and rules on available ports and protocols.

While some may argue that this may slow down the development process, it need not be the case. In this organization, because of the clear communication of corporate policy and security standards ahead of time, the development team builds the testing into its release schedule.

More importantly, it forces the team to think about security and implement the secure coding best practices upstream during the development cycle.

**How has the cloud impacted web application security?**

The cloud has been a great benefit to organizations looking to optimize and scale applications:

- Organizations no longer have to over-provision capacity just to handle high traffic loads that only occur for short periods of time. A classic example is in retail when organizations have to buy equipment that is way over capacity just to handle the few days around Black Friday when sales typically hit an annual peak.
- The network and physical security for leading providers are often as good or better than the organization's own data centers.
- The cloud can also help solve the issue of finding experienced IT professionals that are capable of implementing and maintaining a secure data center.

The biggest downside to the cloud, however is that in the rush to migrate, security is often relegated to a secondary consideration as companies accelerate the adoption of the cloud for their own financial and commercial benefits. Developers of new cloud applications and IT administrators tasked with migrating existing applications to the cloud are under enormous cost and time pressure to get it done.

Often, established guidelines for safe application programming or deployment are not heeded or the tools needed to successfully migrate are not yet available. In the end, this results in programming errors because major security aspects are deliberately disregarded or are simply forgotten.

As a result, critical business processes that seemed secure within the corporate perimeter are suddenly freely accessible in the cloud. Conventional security strategies such as network firewalls, WAFs, code scanners, or other standard security tools may no longer be available or expedient, depending on the choice of cloud provider.

Having the ability to terminate and control traffic is critical to providing the necessary security and application acceleration capabilities necessary for today's web applications.

**What makes a WAF truly great? What features should IT professionals be on the lookout for?**

We are starting to see more and more vendors offering WAF-type solutions. Unfortunately, many of the new solutions are bolted onto unrelated technology like network firewall, IDS/IPS, or even SSL VPN platforms. This is not optimal because these solutions do not provide the ability to control and secure all elements of their WAF. We at Barracuda recommend organizations choose a platform that:

***Is built ground up as a reverse proxy WAF product.*** Having the ability to terminate and control traffic is critical to providing the necessary security and application acceleration capabilities necessary for today's web applications.

***Includes an easy-to-manage interface.*** One of the most common but under-appreciated risks is misconfiguration of the security solution. Consequently, it is advantageous to use a WAF solution that is intuitive and easy to manage.

***Provides pre-built templates to enable quick deployment.*** Too many solutions require constant tuning or learning, which results in an inability to deploy active protection or keep up with changes to applications.

***Is a mature product with a long history of customer success.*** Many solutions can provide simple signature-based protection against things like SQL injections, but few have the layered defense architecture to secure against advanced attacks without affecting application performance.

**What's the difference between using a virtual appliance and a physical appliance for protecting web applications?**

Given sufficient hardware resources, in theory virtual WAFs are just as effective as physical WAFs from a technical standpoint for most use cases. In practice however, it depends on the deployment scenario and the organization's IT group's structure.

In an enterprise scenario there are often three groups involved with application security:

1. Infrastructure group
2. Security / compliance group
3. Application development group.

Depending on the process and ownership, a WAF could be deployed or managed by a single group or co-managed by a few groups. If the infrastructure group controls deployment and has to manage the WAF, then it is possible to design a process to virtualize both the deployment of the application and a virtual WAF to protect it.

However, if the WAF is owned by the security team that does not own the deployment of the applications, then it might be difficult to consolidate servers using a virtual appliance without first redefining the ownership boundaries.

In smaller organizations, the roles are not as distinct and often the same group completes some, if not all of the tasks. In this situation, the decision is primarily a deployment scenario and depends on how the organization wants to architect its network.

If the decision is to put the WAF close to the end servers, then it is possible to consolidate and virtualize both the WAF and application servers. If the decision is to deploy the WAF as part of an ADC platform that needs to support a number of application delivery and acceleration tasks, or is located in the DMZ, then it is easier to keep the existing network configuration than re-architect the network.

Mirko Zorz is the Editor in Chief of (IN)SECURE Magazine and Help Net Security (www.net-security.org).

# The state of web application security in numbers

## Serious website vulnerabilities continue to decrease

The 2013 edition of the WhiteHat Security Website Security Statistics Report correlated vulnerability data from tens of thousands of websites from more than 650 organizations, with software development lifecycle (SDLC) activity data obtained from 76 survey respondents.

In 2012, the average number of serious vulnerabilities per website continued to decline, going from 79 in 2011 down to 56 in 2012.

Of the serious vulnerabilities found, on average 61 percent were resolved and only 18 percent of websites were vulnerable for fewer than 30 days in 2012. On average, resolving these vulnerabilities took 193 days from the first notification.

**86%**

of all websites tested were found to have at least one serious vulnerability exposed to attack every single day of 2012.

“Website security is an ever-moving target, and organizations need to better understand how various parts of the SDLC affect the introduction of vulnerabilities, which leave the door open to breaches,” said Jeremiah Grossman, co-founder and CTO of WhiteHat Security.

A closer look revealed that:

• With the exception of sites in the IT and energy sectors, all industries found fewer vulnerabilities in 2012 than in past years.

• The IT industry experienced the highest number of vulnerabilities per website at 114.

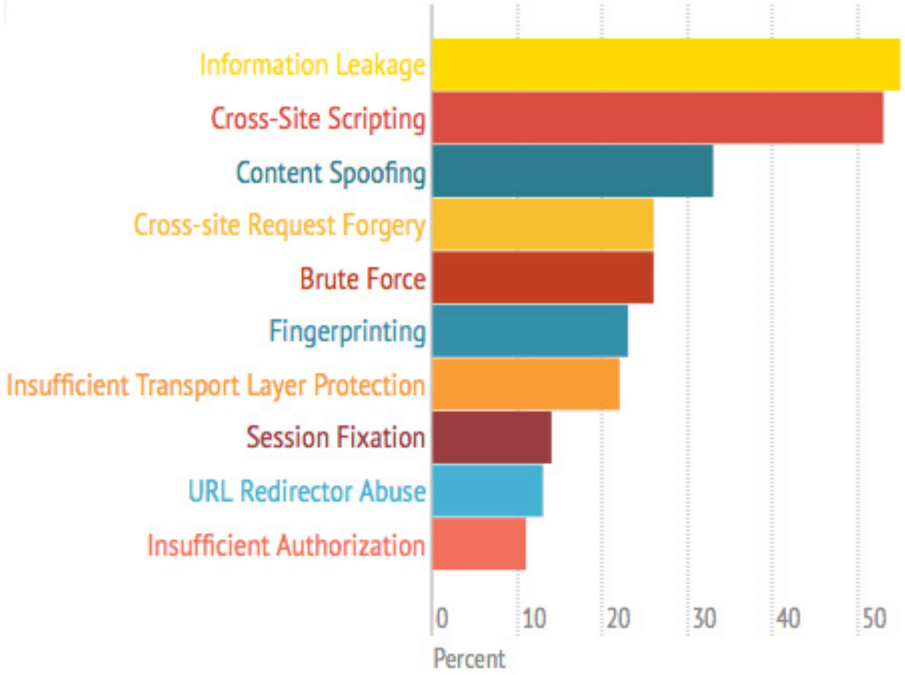
• Government websites had the fewest serious vulnerabilities with eight detected on average per website, followed by banking websites with 11 on average per website.

• Entertainment and media websites had the highest remediation rate (the average percentage of serious vulnerabilities resolved) at 81 percent.

• In years past, the banking industry had the fewest vulnerabilities and fixed the most vulnerabilities of any industry. This year, banking came in second with 11 average serious vulnerabilities found per website and a below average remediation rate of 54 percent (average is 61 percent across all industries).

**Top ten vulnerability classes**

The most prevalent vulnerabilities classes are calculated based upon their percentage likelihood of at least one instance being found within any given website. This approach minimizes data skewing in websites that are either highly secure or extremely risk-prone.



**Best practices may not result in better security**

In correlating the survey results with vulnerability data, WhiteHat Security could see how software security controls, or “best practices” impacted the actual security of organizations.

Some of the findings include:

• 57 percent of organizations surveyed provide some amount of instructor-led or computer-based software security training for their programmers.

These organizations experienced 40 percent fewer vulnerabilities, resolved them 59 percent faster, but exhibited a 12 percent lower remediation rate.

• 39 percent of organizations said they perform some amount of Static Code Analysis on their websites underlying applications. These organizations experienced 15 percent more vulnerabilities, resolved them 26 percent slower, and had a 4 percent lower remediation rate.

• 55 percent of organizations said they have a WAF in some state of deployment. These organizations experienced 11 percent more vulnerabilities, resolved them 8 percent slower, and had a 7 percent lower remediation rate.

Some of this data implies that best practices such as software security training are effective, yet some of the statistics clearly show that following best practices does not necessarily lead to better security.

▼7%

SQL Injection continued its downward slide from 11% in 2011 to 7% in 2012, no longer making the Top 10.

**Accountability and compliance**

In the event an organization experiences a website or system breach, WhiteHat Security found that 27 percent said the Board of Directors would be accountable.

Additionally, 24 percent said Software Development, 19 percent Security Department, and 18 percent Executive Management.

Should the organizations also provide software security training to its programmers and also perform static code analysis, Software Development was held most accountable in the event of a breach.

Additionally, the correlated data revealed that compliance is the primary driver for organizations to resolve vulnerabilities, but also the number one reason organizations do not resolve vulnerabilities. In other words, vulnerabilities are fixed if required by compliance mandates; however, if compliance does not require a fix, the vulnerability remains, despite possible implications to the overall security posture of the site.

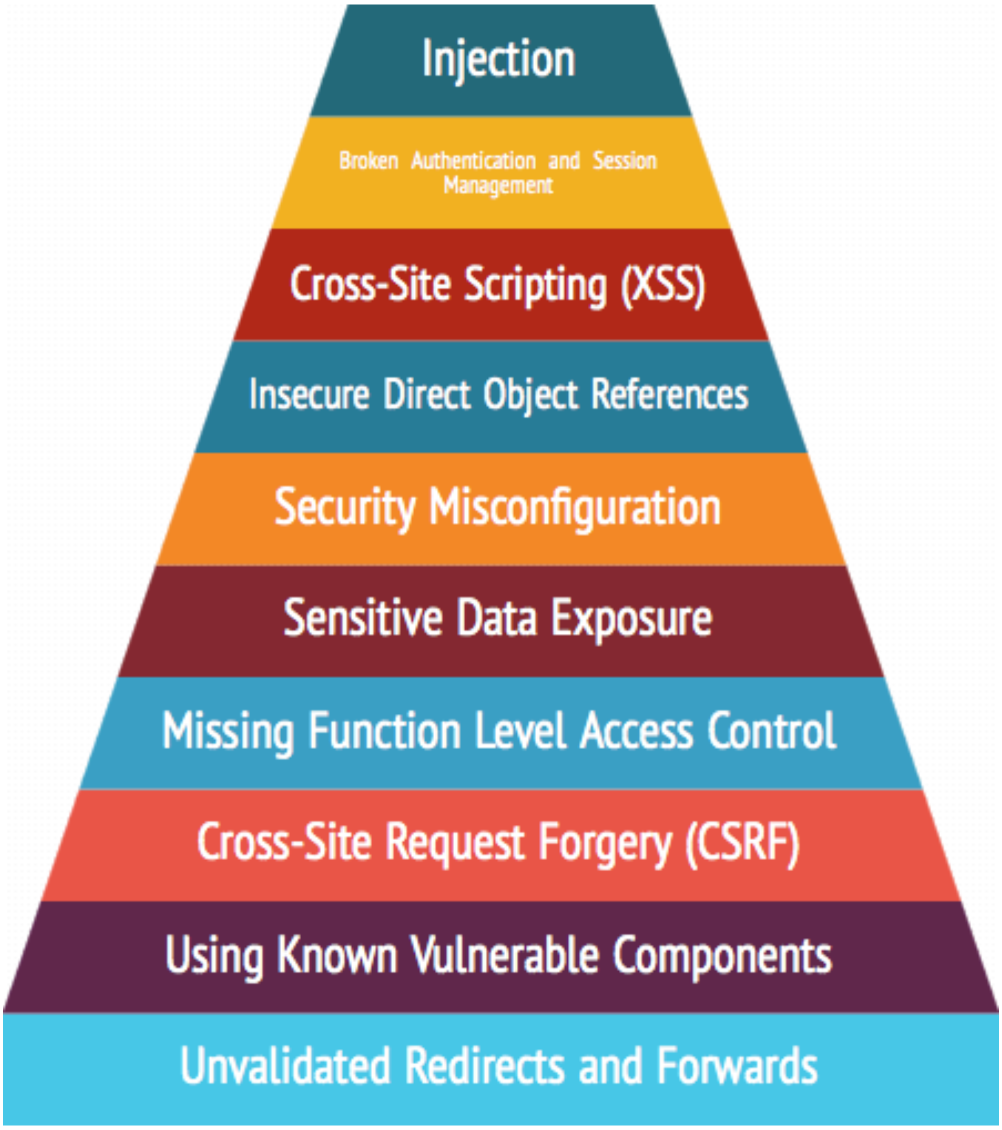
“This collective data has shown that many organizations do not yet consider they need to proactively do something about software security. It is apparent that these organizations take the approach of ‘wait-until-something-goes-wrong’ before kicking into gear unless there is some sense of accountability," said Grossman.

"This needs to change, and we believe there is now an opportunity for a new generation of security leaders to emerge and distinguish themselves with an understanding of real business and security challenges. Our hope is that they will address these issues we have identified and base their decisions on a foundation of data to improve the state of Web security over time,” added Grossman.

## OWASP top 10 web application risks for 2013

Since 2003, application security researchers and experts from all over the world at the Open Web Application Security Project (OWASP) have carefully monitored the state of web application security and produced an awareness document that is acknowledged and relied on by organizations worldwide, including the PCI Council, US DoD, FTC, and countless others.

OWASP has released its 2013 top 10 list of risks associated with the use of web applications in an enterprise, and they are illustrated and explained on the following page.


Injection
Broken Authentication and Session Management
Cross-Site Scripting (XSS)
Insecure Direct Object References
Security Misconfiguration
Sensitive Data Exposure
Missing Function Level Access Control
Cross-Site Request Forgery (CSRF)
Using Known Vulnerable Components
Unvalidated Redirects and Forwards

***Injection*** - Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

***Broken Authentication and Session Management*** - Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

***Cross-Site Scripting (XSS)*** - XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

***Insecure Direct Object References*** - A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

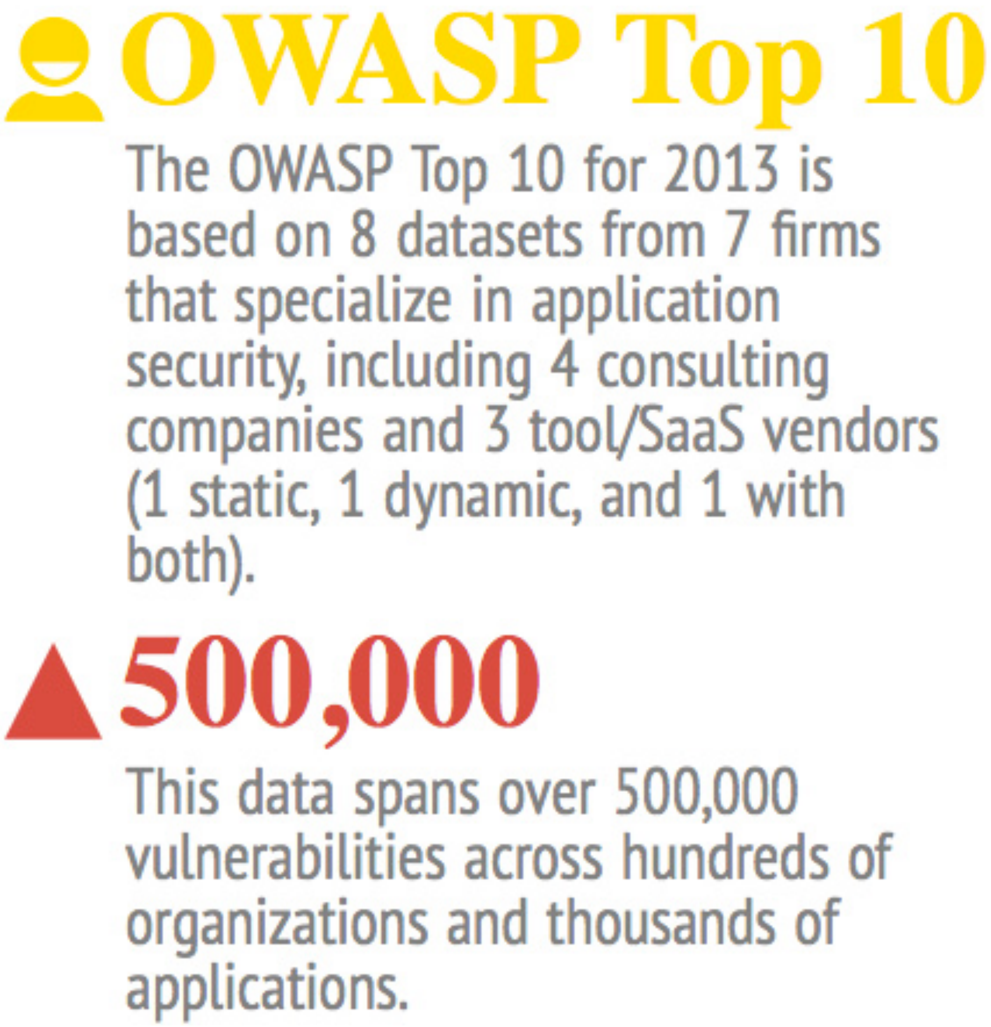
***Security Misconfiguration*** - Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

***Sensitive Data Exposure*** - Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

***Missing Function Level Access Control*** - Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

***Cross-Site Request Forgery (CSRF)*** - A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.



## OWASP Top 10

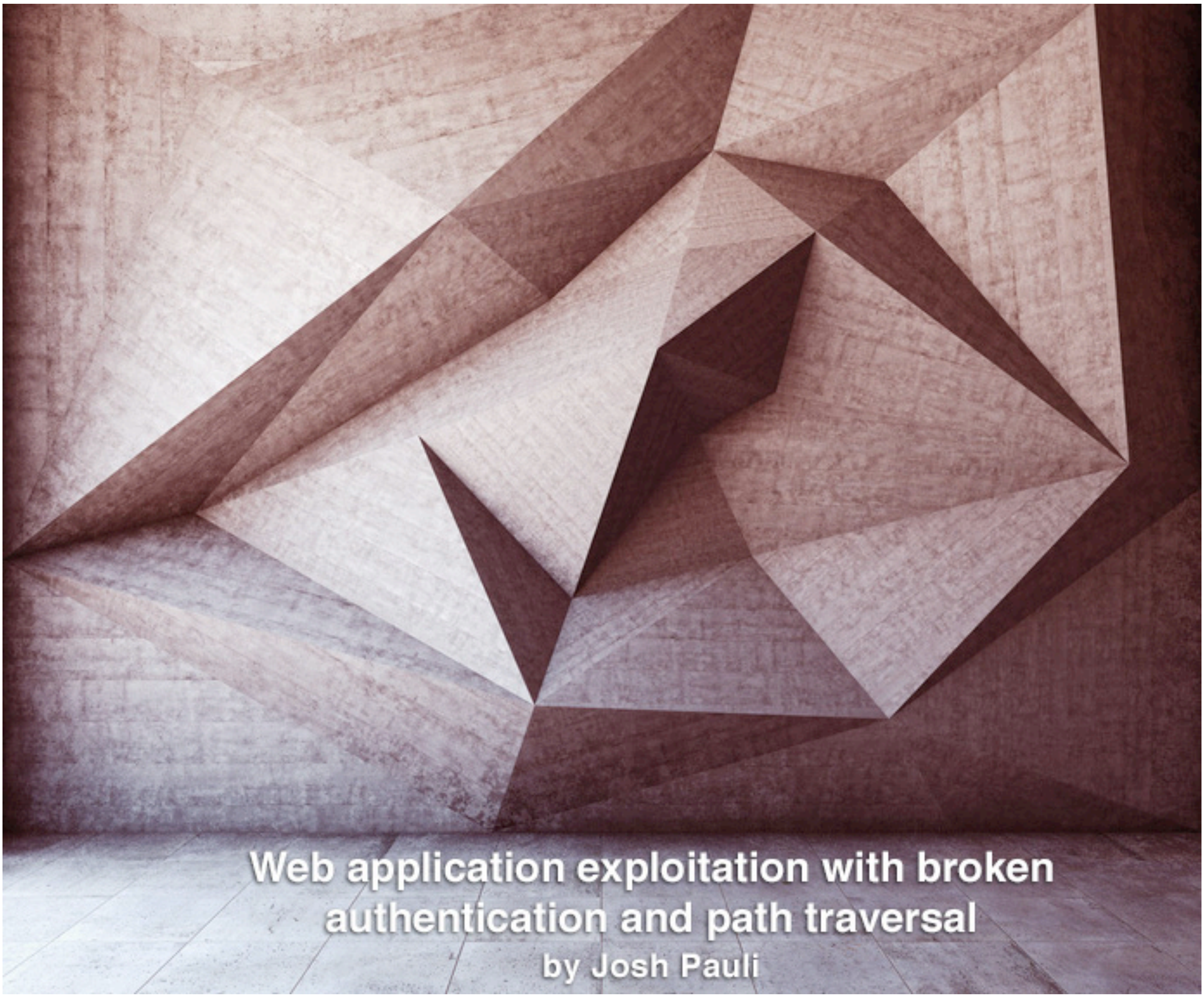
The OWASP Top 10 for 2013 is based on 8 datasets from 7 firms that specialize in application security, including 4 consulting companies and 3 tool/SaaS vendors (1 static, 1 dynamic, and 1 with both).

## 500,000

This data spans over 500,000 vulnerabilities across hundreds of organizations and thousands of applications.

***Using Components with Known Vulnerabilities*** - Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

***Unvalidated Redirects and Forwards*** - Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.



# Web application exploitation with broken authentication and path traversal

by Josh Pauli

This article covers a combination of very important vulnerabilities that affect almost every single web application: broken authentication mechanisms, poor handling of sessions, and the ability for hackers to browse the operating system of the web server via path traversal.

Authentication allows us to sign in to a web application so we have a personalized browsing experience, while session management keeps tracks of the requests and responses so we can perform multi-step actions such as shopping and bill paying. They are really two peas in a pod. Neither authentication nor session management was considered when the HTTP protocol was invented as it is a stateless protocol. So using these two features as the Internet has matured has proven to be a very difficult situation.

Unfortunately, authentication and session management are wrought with vulnerabilities in many web applications. The tools and techniques used to exploit each differ slightly, but because of the close relationship of authentication and session management it makes perfect sense to investigate them together.

Path traversal attacks occur when hackers are allowed to traipse through the directory structure of the web server. This is most common when web applications allow upload functionality and the user (attacker) crafts a malicious input value that is processed by the web application and allows access to sensitive directories on the web server.

We will look at the directories that are often under attack in both Windows and Linux environments and how these attacks actually take place!

## Authentication and session vulnerabilities

Today's Internet has been twisted and contorted to use authentication and session management, essentially breaking both. The most common authentication attack uses a proxy-based attack tool (Burp Suite's Intruder, for example) to brute force the login credentials of a legitimate user. There is not a lot of stealth to this type of attack, but it's very successful because users continue to pick weak passwords. We will be using Burp Intruder as our tool of choice along with a list of the most commonly used weak passwords.

There are several aspects of authentication throughout the web application that need to be considered for these attacks, such as:

- Application login
- Password change
- Secret questions
- Predictable usernames
- Predictable initial password
- Passwords that never expire.

Throughout this article, the term "cookie" will be used to mean "session cookie" or "session identifier". Session management attacks are only possible in two flavors: 1) attacking how strongly the session identifier is generated (measuring entropy); and 2) attacking how the cookie is used and handled by the web application.

Attacking how a cookie is generated is very difficult because most of the session management frameworks bundled with web servers are capable of creating cookies that are very difficult to guess even when a hacker has tons of processing power to generate thousands of cookies in short order. A much more applicable attack is to investigate how the application uses the cookie. This type of attack doesn't require understanding how a cookie was generated, but instead focuses on accessing and using the cookie in a nefarious manner. A hacker will gladly steal and use a securely generated cookie!

## Path traversal vulnerabilities

When a web server is installed and configured, the web application is given a slice of the file system on the web server that the application is allowed to live in. These allowed directories are usually a couple of folders deep into the file system of the web server and include 100% of what the web application needs to perform in normal circumstances: the code, the images, the database, the style sheets, and everything else that the application may need. The application should never attempt to access resources that are outside of its prescribed directories because the other resources on the web server aren't applicable to the application's scope. The ability for a hacker to break outside this confined world and access resources on the web server that he shouldn't is the core concept of path traversal attacks.

## Brute force authentication attacks

Authentication actually takes place in many other parts of the web application other than the main login page. It is also present when you change your password, update your account information, use the password recovery functionality, answering secret questions, and when you use the remember me option. If any of these authentication processes is flawed, the security of all the other authentication mechanisms may be compromised.

The frightening thing about authentication vulnerabilities is that they can open the door for all other accounts to be compromised. Imagine the carnage when an administrator's account is compromised because of poor authentication!

We will be using the Brute Force exercise in DVWA as our guide to complete an online brute force authentication attack. It is an HTML form-based authentication page; just like over 90% of web applications use. Despite ongoing efforts to include additional factors into the authentication process, such as CAPTCHA and challenge questions, the traditional username and password is still the most popular authentication mechanism.

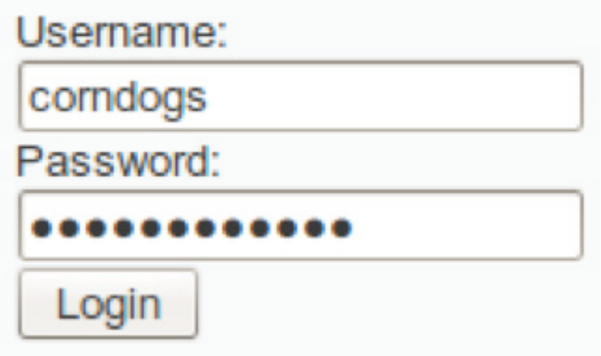
This attack is much different than the offline password hash cracking that we completed with John the Ripper. We will now be interacting directly with the web application and database that process the username and password parameters during authentication.

Online brute force authentication hacking is much slower than offline password hash cracking because we are making repeated requests to the application and must wait for it to generate a response and send it back.

## Intercepting the authentication attempt

Browse to the Brute Force exercise in DVWA and ensure Burp is configured as the proxy with your browser. We want to intercept a login attempt that we send to the application, so make sure Burp Intercept is set to on. We aren't trying to guess the username and password manually in this HTML form, but rather this step is just priming the pump so we understand what parameters are sent to the application during a normal authentication attempt. It makes absolutely no difference what we provide for username and password. I've entered *corndogs* for the username and *sureareyummy* for the password as shown in Figure 1.

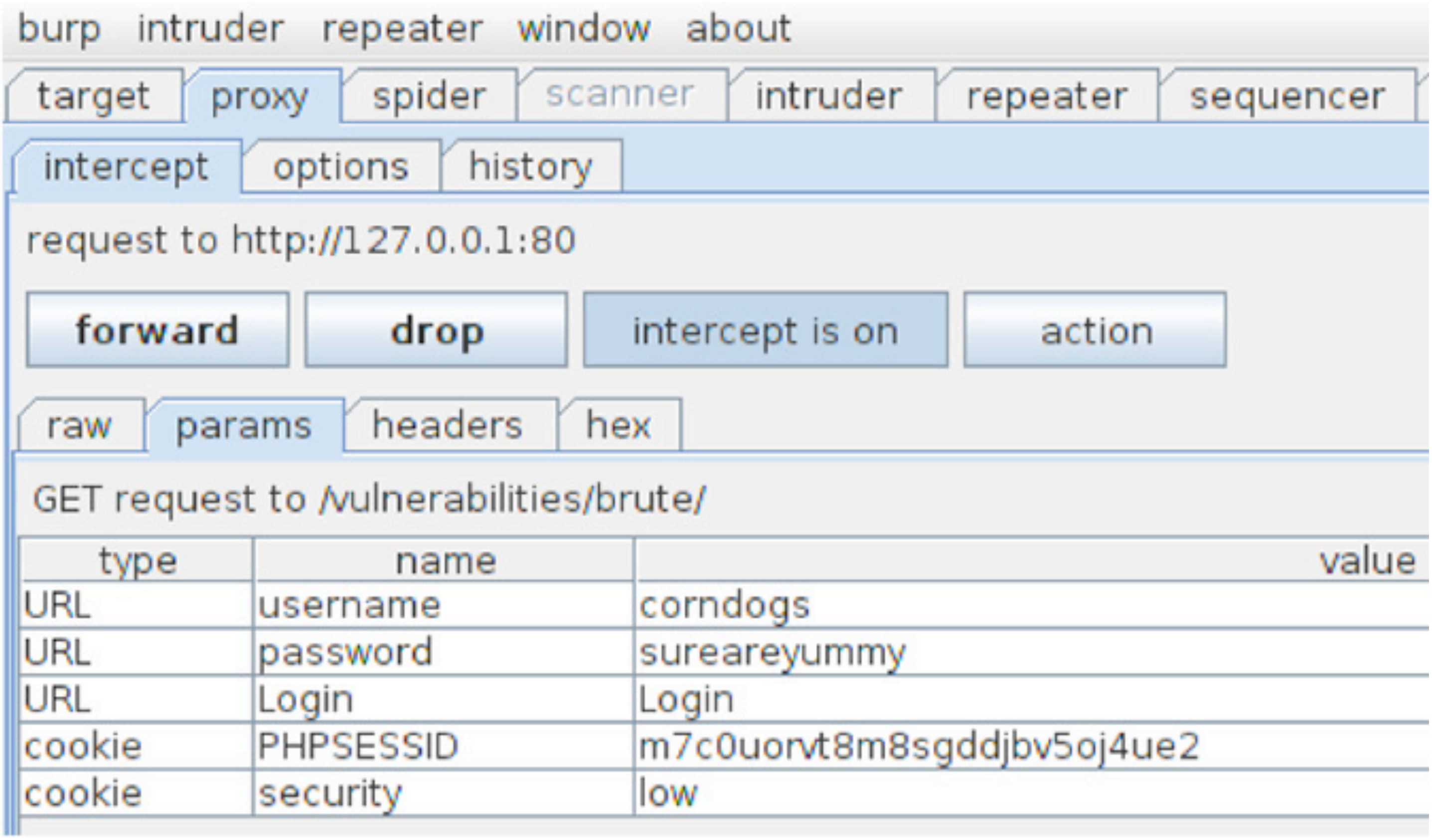
Once you submit this login attempt with the Login button, you can see the parameters in the Params tab in Burp Intercept that are used during an authentication attempt as shown in Figure 2.



Username: corndogs

Password: ●●●●●●●●●●●●●

Figure 1 - Initial login attempt to be captured by Burp Intercept.



request to http://127.0.0.1:80

GET request to /vulnerabilities/brute/

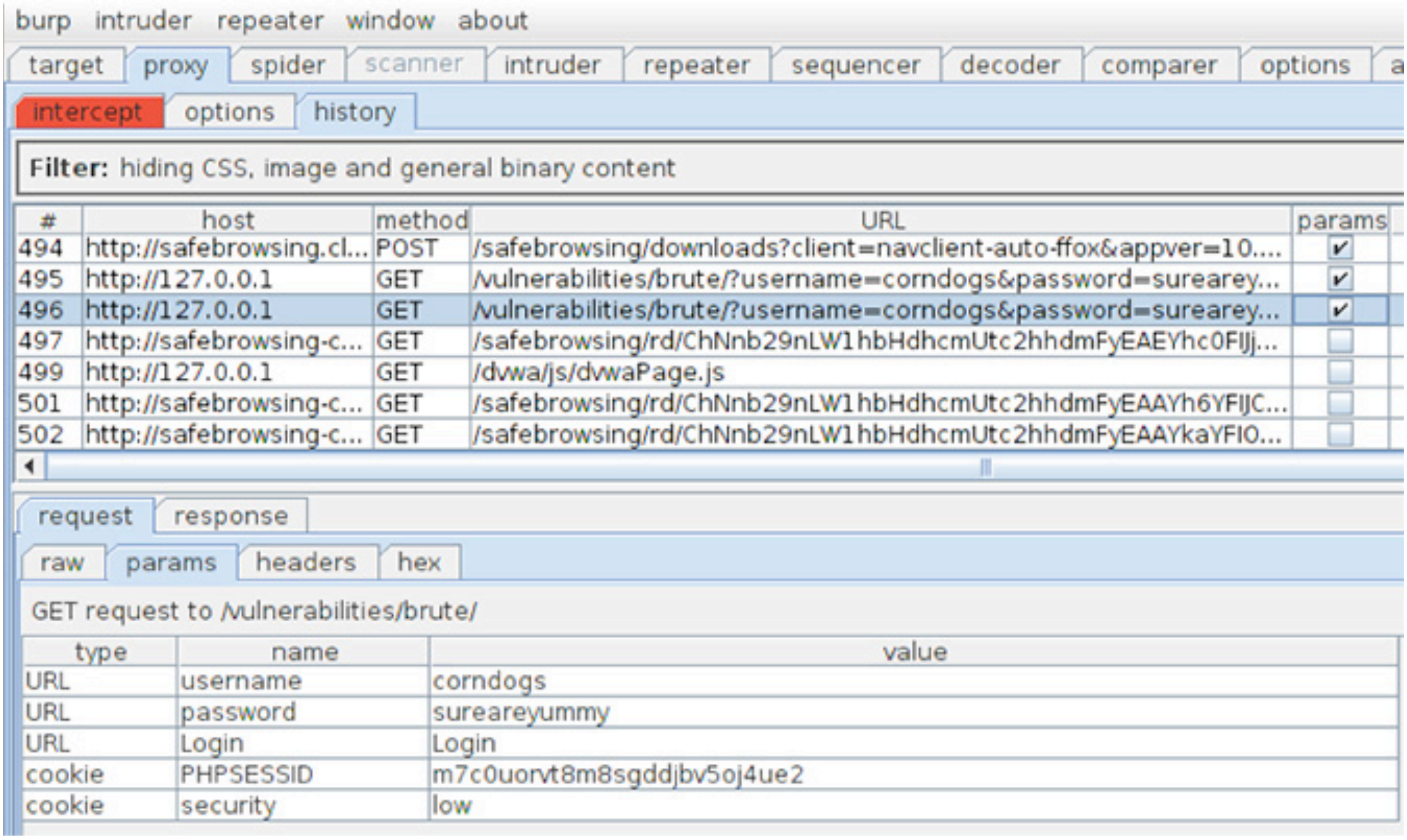
| type | name | value |
|---|---|---|
| URL | username | corndogs |
| URL | password | sureareyummy |
| URL | Login | Login |
| cookie | PHPSESSID | m7c0uorvt8m8sgddjbv5oj4ue2 |
| cookie | security | low |

Figure 2 - Intercepted authentication parameters in DVWA.

We are only concerned with the username and password parameters for this attack; the other three will be left alone. Remember, we fully expect this login attempt to fail. Our only goal right now is to get a valid authentication attempt in our proxy history so we can changes the parameters' values to exploit the weak authentication process.

You can now forward this request to the application as well as the subsequent responses until you get the Username and/or password incorrect message on the page.

One feature of a web proxy that is often overlooked is that it catalogs every single request and response cycle that passes through it. You can then go back and inspect (and reuse) any request that you have already made. This is exactly why you primed the pump with the sure-to-fail authentication attempt. It was surely going to fail, but you needed a request that had everything correct except the username and password! You can review all the requests you've made in the history tab in the Proxy tool of Burp. You are specifically looking for the authentication attempt you just made with the *corndogs* username and *sureareyummy* password combination as shown in Figure 3.


burp intruder repeater window about
target proxy spider scanner intruder repeater sequencer decoder comparer options a
intercept options history

**Filter:** hiding CSS, image and general binary content

| # | host | method | URL | params |
|---|---|---|---|---|
| 494 | http://safebrowsing.cl... | POST | /safebrowsing/downloads?client=navclient-auto-ffox&appver=10.... | ☑ |
| 495 | http://127.0.0.1 | GET | /vulnerabilities/brute/?username=corndogs&password=surearey... | ☑ |
| 496 | http://127.0.0.1 | GET | /vulnerabilities/brute/?username=corndogs&password=surearey... | ☑ |
| 497 | http://safebrowsing-c... | GET | /safebrowsing/rd/ChNnb29nLW1hbHdhcmUtc2hhdmFyEAEYhc0FIJj... | □ |
| 499 | http://127.0.0.1 | GET | /dvwa/js/dvwaPage.js | □ |
| 501 | http://safebrowsing-c... | GET | /safebrowsing/rd/ChNnb29nLW1hbHdhcmUtc2hhdmFyEAAYh6YFIJC... | □ |
| 502 | http://safebrowsing-c... | GET | /safebrowsing/rd/ChNnb29nLW1hbHdhcmUtc2hhdmFyEAAYkaYFIO... | □ |

GET request to /vulnerabilities/brute/

| type | name | value |
|---|---|---|
| URL | username | corndogs |
| URL | password | sureareyummy |
| URL | Login | Login |
| cookie | PHPSESSID | m7c0uorvt8m8sgddjbv5oj4ue2 |
| cookie | security | low |

Figure 3 - Authentication attempt retrieved from the proxy history of Burp Intercept.

If you're overwhelmed by the sheer amount of requests in this history view, it is helpful to look for requests that have parameters (look for the checked checkbox in the Params column) as well as ordering the requests by date/time.

You can see the username and password that you submitted in the parameters view in the lower part of the screen.

## Configuring Burp Intruder

You can now use this request as your skeleton to attempt to exploit this authentication page with different usernames and passwords. To do this, simply right-click on the request and select send to intruder as shown in Figure 4 on the following page.

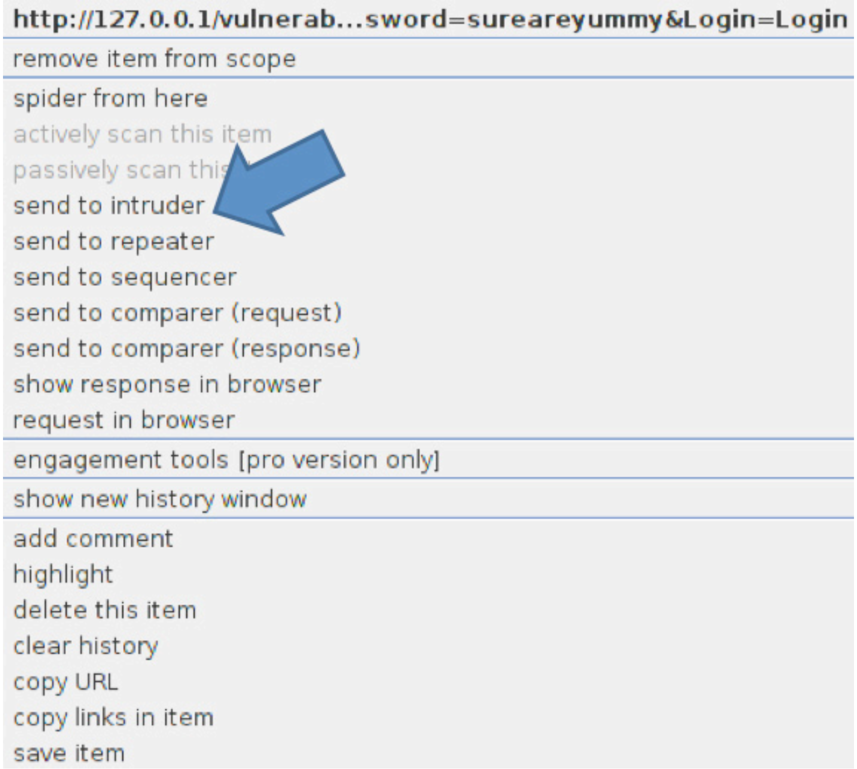
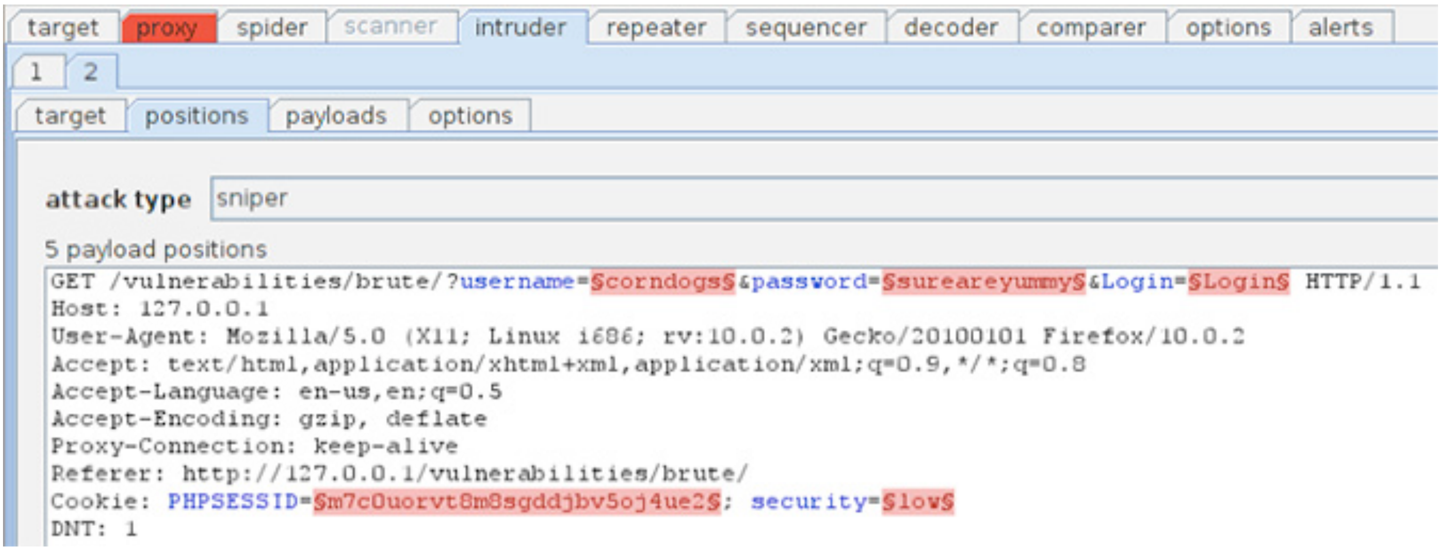


Figure 4 - Sending the authentication attempt to Intruder.

Burp Intruder is a tool for automating customized attacks against web applications, but it is not purely a point-and-click tool. You need to configure Intruder to only attack the parameters that you choose and with the exact payloads that you select. In the Positions tab of Intruder you can see there are five automatically highlighted parameters that you may want to brute force as shown in Figure 5.



attack type: sniper

5 payload positions

```
GET /vulnerabilities/brute/?username=§corndogs§&password=§sureareyummy§&Login=§Login§ HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:10.0.2) Gecko/20100101 Firefox/10.0.2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Proxy-Connection: keep-alive
Referer: http://127.0.0.1/vulnerabilities/brute/
Cookie: PHPSESSID=§m7c0uorvt8m8sgddjbv5oj4ue2§; security=§low§
DNT: 1
```

Figure 5 - Automatically identified parameters in Burp Intruder.

These five parameters should look very familiar, as they are the exact same parameters that you saw in the intercepted request. You are only concerned with the username and password parameters and the other three can be left alone. In order for Intruder to ignore these three benign parameters, you need to clear the payload markers (the squiggly markings before and after each parameter value) by highlighting them and clicking the clear button. One you've successfully done that, you will have only two positions marked: username and password.

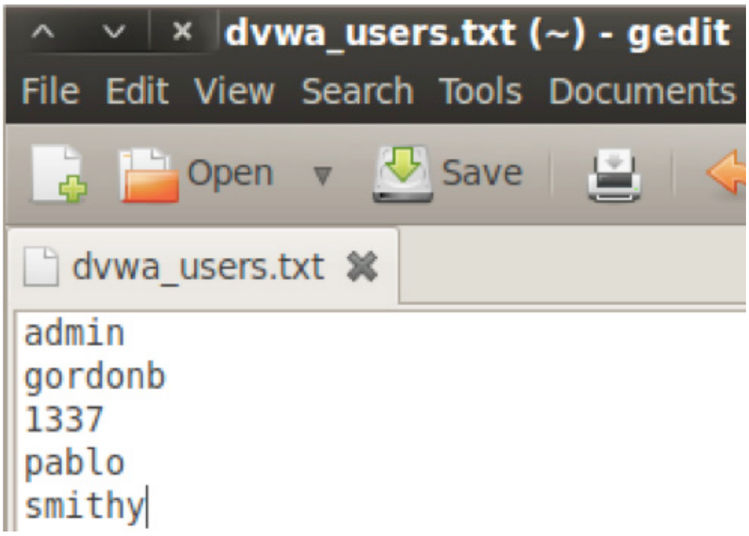
### Intruder payloads

You also need to consider the attack type that we want to conduct. Intruder has four different attack types that you can select from the pull-down menu.

1. **Sniper:** This attack uses a single set of payloads and targets each position in turn before iterating to the next value. This is most applicable when fuzzing for vulnerabilities such as cross-site scripting (XSS).
2. **Battering Ram:** This attack also uses a single set of payloads, but inserts the same payload into all of the marked parameters at once. This is most applicable when an attack requires the same input to be inserted in multiple places such a username in the cookie header and the message body simultaneously.
3. **Pitchfork:** This attack uses multiple payload sets for each marked parameter and iterates through all payload sets simultaneously. This is most applicable when an attack requires related values to be used in several parameters in the request such as a user_ID parameter and the corresponding first_name parameter. A pitchfork attack will advance each of these payloads in parallel so the first values of each payload will execute, followed by the second value of each payload, and so on.
4. **Cluster Bomb:** This attack uses multiple payload sets, but a different payload set for each marked parameter and iterates through each payload set in turn to ensure all possible combinations are used. This attack is most applicable when an attack requires different input to be used in multiple places in the request such as a username and password. The cluster bomb attack will lock in the first payload (username, for example) and iterate all of the passwords with this first username. Once all the password values have been tried for the first username, the username is changed to the second username and the entire password list is used with this second username.

Obviously you are going to use the cluster bomb attack type for the authentication hack, but knowing when to use each of these attack types is a great weapon in your arsenal. The Help menu is Burp Suite has additional documentation on these attack types if you'd like further explanation. Once you've selected Cluster bomb from the drop-down menu, you can select the Payloads tab in Intruder. A payload is the values to iterate through during the brute forcing. You have two positions available to send payloads to: the username and the password. The Payload set drop-down menu in Intruder indicates which parameter you are targeting and they are processed in the same order that they appear in the positions tab, so username is up first.

There are many options for the username payload, but perhaps the most useful is the runtime file that can be fed to Intruder during the attack. Such a file is a great place to store usernames that you gather during the previous recon steps. We already know the five valid users for DVWA so it's an easy task to start gedit, create a text file full of valid users, and save it as dvwa_users.txt in the root directory that we can use in Intruder as shown in Figure 6.


dvwa_users.txt (~) - gedit
File Edit View Search Tools Documents
Open
Save
dvwa_users.txt

```
admin
gordonb
1337
pablo
smithy
```

Figure 6 - Creating the dvwa_users.txt file to be used by Burp Intruder.

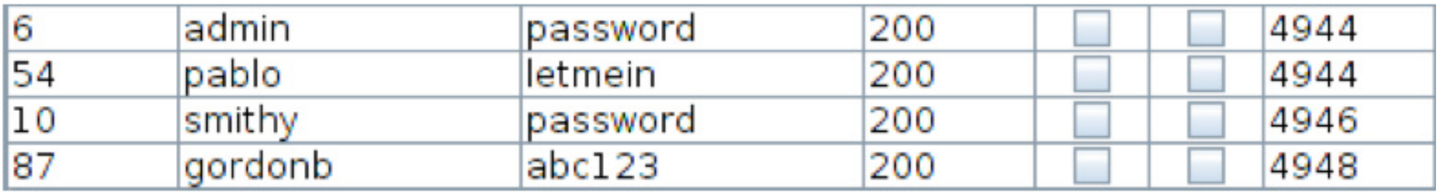
We are going to use a readily available password list as the runtime file for the password parameter. It is the 500 Worst Passwords list from the team at Skull Security that can be downloaded as a .bz2 file from **`http://www.skullsecurity.org/wiki/index.php/Passwords`**. Save this file in your root directory and then open a terminal and run the following command to extract it to a text file.

```
bunzip2 500-worst-passwords.txt.bz2
```

Once you've successfully downloaded and unzipped this password list, run an ls command to ensure the text file is in your root directory. If everything goes as intended, both the username file (dvwa_users.txt) and password file (500-worst-passwords.txt) will be available as text files in your root directory. With these lists ready and the payload markers set in Intruder, the only remaining task before attempting this exploit is to assign each text file as a runtime file. There is a "Payload Options (Runtime file)" section where you can browse your local hard drive to select your text file for each payload. Remember position 1 is for dvwa_users.txt and position 2 is for 500-worst-passwords.txt.

## Running intruder

You can execute this exploit by selecting start attack from the Intruder menu. Burp Intruder will alert you that the free version is throttled to attack slower, so you will need to click-through this prompt. Because you're most likely using the free version of Burp Suite, this attack will take approximately 30-40 minutes to finish because of the nearly 2,500 requests with a one second delay between each request running on only one thread. The pro version, however, will tear through this attack very quickly! The vast majority of your authentication attempts will fail, but it's easy to identify the few requests that are a different length as successful logins when sorting by response length as shown in Figure 7.



| | | | | | | |
|---|---|---|---|---|---|---|
| 6 | admin | password | 200 | □ | □ | 4944 |
| 54 | pablo | letmein | 200 | □ | □ | 4944 |
| 10 | smithy | password | 200 | □ | □ | 4946 |
| 87 | gordonb | abc123 | 200 | □ | □ | 4948 |

Figure 7 - Successful brute force logins via Intruder.

You can also include custom string terms to search for so it's easier to identify a successful login under the options tab in Intruder. Perhaps you want to search for the term Welcome! as a known string when authentication is successful. Just make sure you know an actual string that will be displayed with a valid authentication attempt otherwise it will return no results.

## Session attacks

Here are some of the most popular session attacks that are currently being used by hackers to exploit session vulnerabilities.

- *Session Hijacking:* This is when a user's session identifier is stolen and used by the attacker to assume the identity of the user. The stealing of the session identifier can be executed several different ways, but cross-site scripting (XSS) is the most common.

- *Session Fixation:* This is when an attacker is assigned a valid session identifier by the application and then feeds this session to an unknowing user. This is usually done with a web URL that the user must click on the link. Once the user clicks the link and signs into the application, the attacker can then use the same session identifier to assume the identity of the user. This attack also occurs when the web server accepts any session from a user (or attacker) and does not assign a new session upon authentication. In this case, the attacker will use his or her own, pre-chosen session, to send to the victim. These attacks work because the session identifier is allowed to be reused (or replayed) in multiple sessions.

- *Session Donation:* This is very similar to session fixation, but instead of assuming the identity of the user, the attacker will feed the session identifier of the attacker's session to the user in hopes that the user completes an action unknowingly. The classic example is to feed the user a valid session identifier that ties back to the attacker's profile page that has no information populated. When the user populates the form (with password, credit card info, and other goodies), the information is actually tied to the attacker's account.
- *Session ID in the URL:* This is when session identifiers are passed as URL parameters during the request and response cycle. If this functionality is present, an attacker can feed such a URL to the user to conduct any of the attacks described above.

## Cracking cookies

One of the first activities that new security researchers always attempt is cracking session-generating algorithms so they can predict session identifiers. I was even a faculty supervisor for such an adventure! My team created an application that logged into an application, archived the assigned cookie, logged out of the application, and repeated that cycle millions of times.

Once we gathered over one million session identifiers, we mined the database for any instance of duplicate cookies. None were to be found. We then turned our attention to trying to crack the algorithm that created these cookies. No dice. We calculated that it would take several hundreds of years before compromising the algorithm. If you think that attacking these algorithms is the path of least resistance to web application compromise, you're doing it wrong.

There was a time when session identifiers were created using weak algorithms, but those days are long gone. Unless a web administrator totally misses the boat when configuring the application environment or somebody decides to roll their own session creation algorithm (always a terrible idea), there is little hope in attacking the algorithm that generates session identifiers. Is it mathematically possible? Absolutely! Is it a good use of your time and resource? Not in a million years (which is how long some of the cracks will take)!

## Burp Sequencer

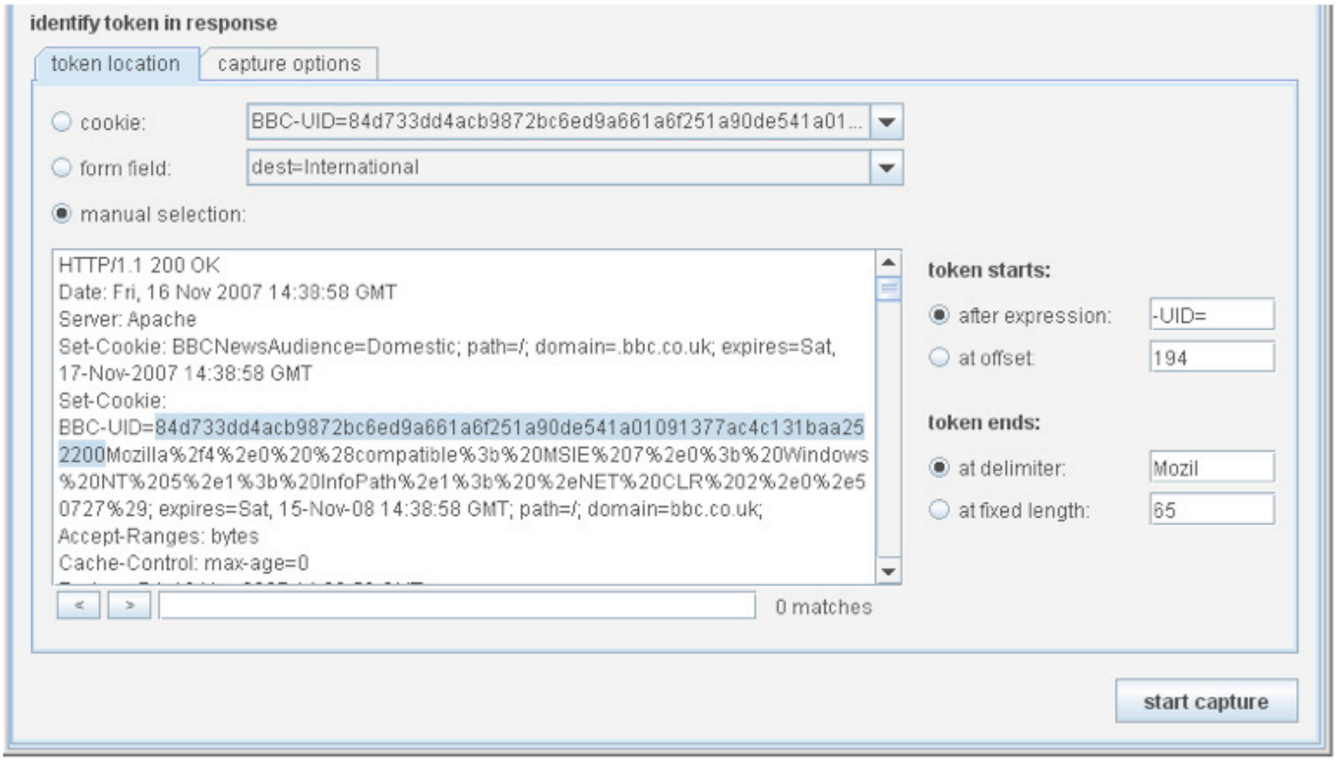
You can test how strongly session identifiers are generated by using Burp Sequencer, which tests for randomness in session values where the security of the application relies on unpredictability of these random session identifiers. It's a very handy tool that performs extensive analysis on gathered session IDs and displays the results in easy to understand graphs and tables.

Burp Sequencer tests a hypothesis (”the session identifier is actually randomly generated”) against a collection of gathered session identifiers to calculate the probability of actual randomness. This is fancy talk for “it checks to see if the sessions cookie is actually random compared to tons of other session cookies”. If this probability falls below the significance level, the session identifier is categorized as non-random. By default Sequencer uses the .0002-.03% FIPS standard for significance, but you are free to adjust this measurement for your own uses. FIPS is the Federal Information Processing Standards that is used government-wide for security and interoperability of Federal computer systems. The steps to conduct a Sequencer test and analysis are very easy to perform:

**1.** Find a request in your proxy history that has a session identifier in its response. This session identifier is what we want to test and analyze with Sequencer.
**2.** Use the right-click menu on this request to send to sequencer.
**3.** Identify the session identifier in Sequencer if it's not automatically identified. Sequencer will automatically identify most stock web environments' session identifiers.
**4.** Set any options you'd like in Sequencer such as the thread count and request speed to dictate the speed in which the session identifiers will be gathered. Remember it's critical that you get the session identifiers are quickly as possible without losing sessions to other users. If you can get a large consecutive stream of session identifiers, your testing will be more accurate.
**5.** Click the Start Capture button. You can review results as soon as Sequencer has been issued 100 session identifiers. The FIPS standard mandates 20,000 session identifiers to be reliable.

**6.** Review the results of the tests in the generated charts.

Here is a screenshot identifying the session identifier right after sending the request to Sequencer. This is a screenshot of Daf conducting this analysis on the BBC news website, not us using DVWA. Notice the token starts and token ends options on the right side of the screen that identify the exact parameter that you'd like tested as shown in Figure 8.



○ cookie: BBC-UID=84d733dd4acb9872bc6ed9a661a6f251a90de541a01...

○ form field: dest=International

● manual selection:

```
HTTP/1.1 200 OK
Date: Fri, 16 Nov 2007 14:38:58 GMT
Server: Apache
Set-Cookie: BBCNewsAudience=Domestic; path=/; domain=.bbc.co.uk; expires=Sat,
17-Nov-2007 14:38:58 GMT
Set-Cookie:
BBC-UID=84d733dd4acb9872bc6ed9a661a6f251a90de541a01091377ac4c131baa25
2200Mozilla%2f4%2e0%20%28compatible%3b%20MSIE%207%2e0%3b%20Windows
%20NT%205%2e1%3b%20InfoPath%2e1%3b%20%2eNET%20CLR%202%2e0%2e5
0727%29; expires=Sat, 15-Nov-08 14:38:58 GMT; path=/; domain=bbc.co.uk;
Accept-Ranges: bytes
Cache-Control: max-age=0
```

0 matches

**token starts:**

● after expression: -UID=

○ at offset: 194

**token ends:**

● at delimiter: Mozil

○ at fixed length: 65

Figure 8 - Identifying the session identifier in Burp Sequencer.

The results of the Sequencer testing can be viewed from an overall significance level perspective and at the bit level perspective. Here are results for varying levels of significance where it is discovered that there is over 170 bits of entropy for the .001% significance level (bottom bar in the chart). Entropy is a measure of unpredictability. So the higher the entropy in the session identifiers, the more confident we are that they are randomly generated.

If you mandate FIPS compliance, the bit level results are especially applicable because you can cycle through several tabs across the top of the graph that provides several different FIPS test results.

Sequencer is a great tool for quickly testing the randomness of session identifier generation. It is very rare that you will find problems with session identifiers even when you gather 15,000 or 20,000 of them for analysis.

## Other cookie attacks

Viable attacks against session identifiers all revolve around the concept of reusing a cookie. It doesn't matter whom the cookie was issued to, how the hacker stole the cookie, or how the hacker plans to reuse it. It only matters that the application is perfectly functional with old cookies being used more than once. It's that simple. You can complete a series of tests against any application once you've received a valid session identifier to check if it's vulnerable to cookie reuse.

- Log out of the application, click the back button in your browser, and refresh the page to see if you can still access a page in the web application that should require an active session such as an my account page.
- Copy and paste your valid session identifier into a text file (so you have a copy of the value) and use it again after logging out. You can use an intercepting proxy to plug in your old session identifier.

- Simply walk-away from, or stop using, your browser all together for several hours to test the time-out limits of the application after you've received a valid session identifier. It's all too common to simply have to click OK when it warns you that your session has been terminated when it actually hasn't.
- Many applications will issue you a cookie when you first visit the site even before you log in. Copy and paste that session identifier into a text file and then log in. Compare the session identifier that was issued to you when you first visited the site and the session identifier you were issued after successfully authenticating. They should be different. If they aren't, this is a big vulnerability related to session donation.
- Log into the same application from two different browsers to see if the application supports dual logins. If both sessions persist, do they have the same session identifier? Is the first session warned that the same account has been logged into concurrently from a different location?

There are several variants of the manual tests above that you can develop on your own. It's all about testing to see how the application deals with the session identifier during normal usage. We will return to session attacks when we cover attacking the web user.

## Path traversal attacks

Path traversal attacks take place when a hacker attempts to circumvent any safeguards and authorization checks that the web server administrator and web programming team have set up to keep all web application users only in the specified directories. These attacks are often executed by authenticated users of the application; that way they can fully inspect what a normal authenticated user has access to so they can better craft malicious reference request. Trying to identify what parameters are in play during normal usage of the application from a guest account would be very difficult. Think of all the extra functionality (thus parameters and pages) that is made available to you as soon as you log into an online store or bank.

## Web server file structure

If you use Linux for your web environment, the directory structure will vary depending on the exact web server, but for our DVWA installation, the directory structure will resemble what is introduced in Figure 9.

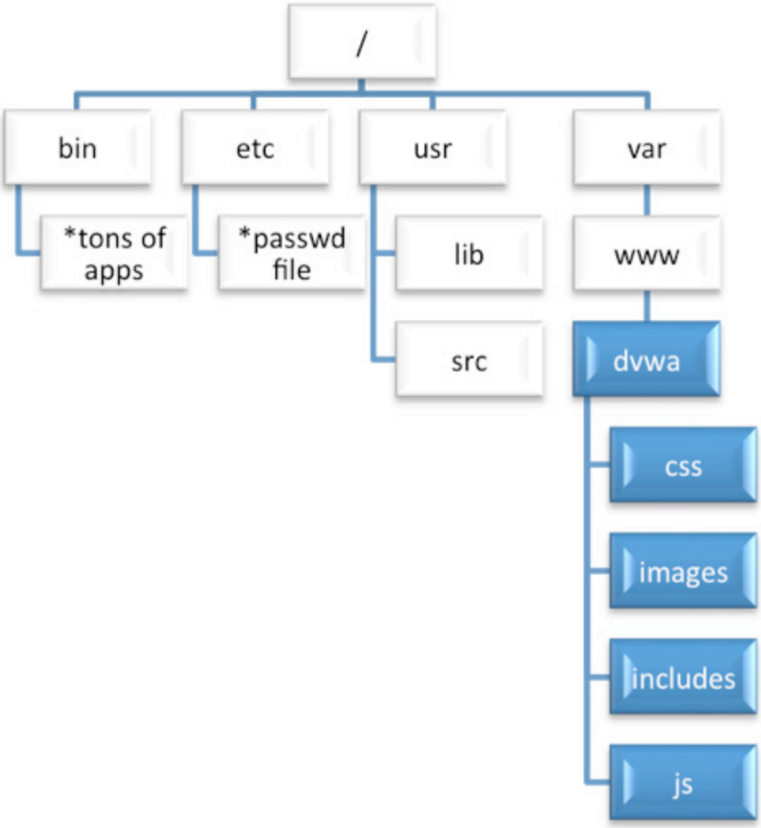
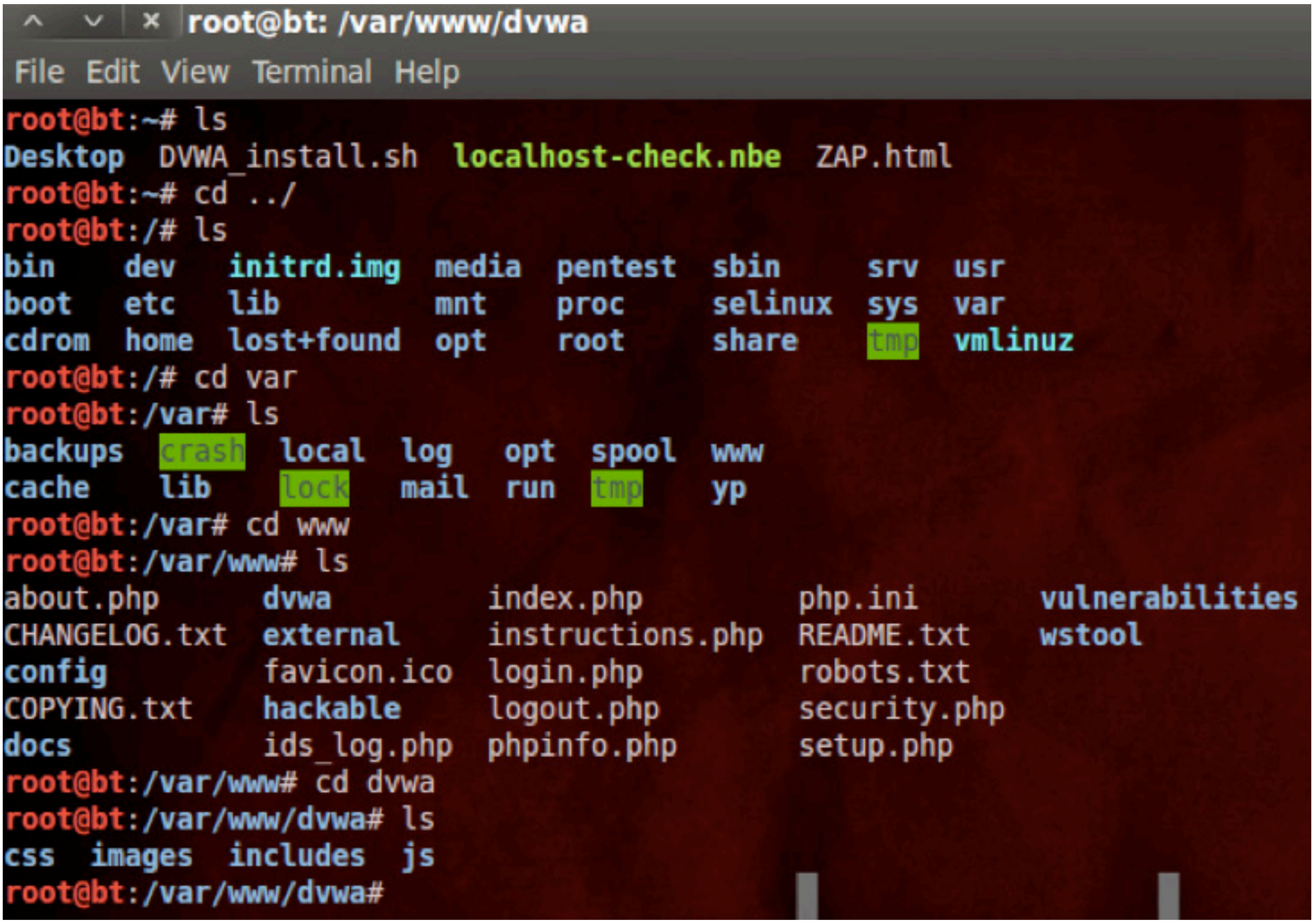


Figure 9 - Partial directory structure for DVWA on the web server.

The shaded directories with white type are the directories on the web server that the web application is allowed to access. All other directories (many more not shown at the root level) are intended to be accessed only by the web server administrator.

If you were curious what the directory structure is for other Linux installations, I would recommend taking a stepwise approach to discovering them. Run a series of cd and ls commands so you can see the changes from one directory level to the next as shown in Figure 10.



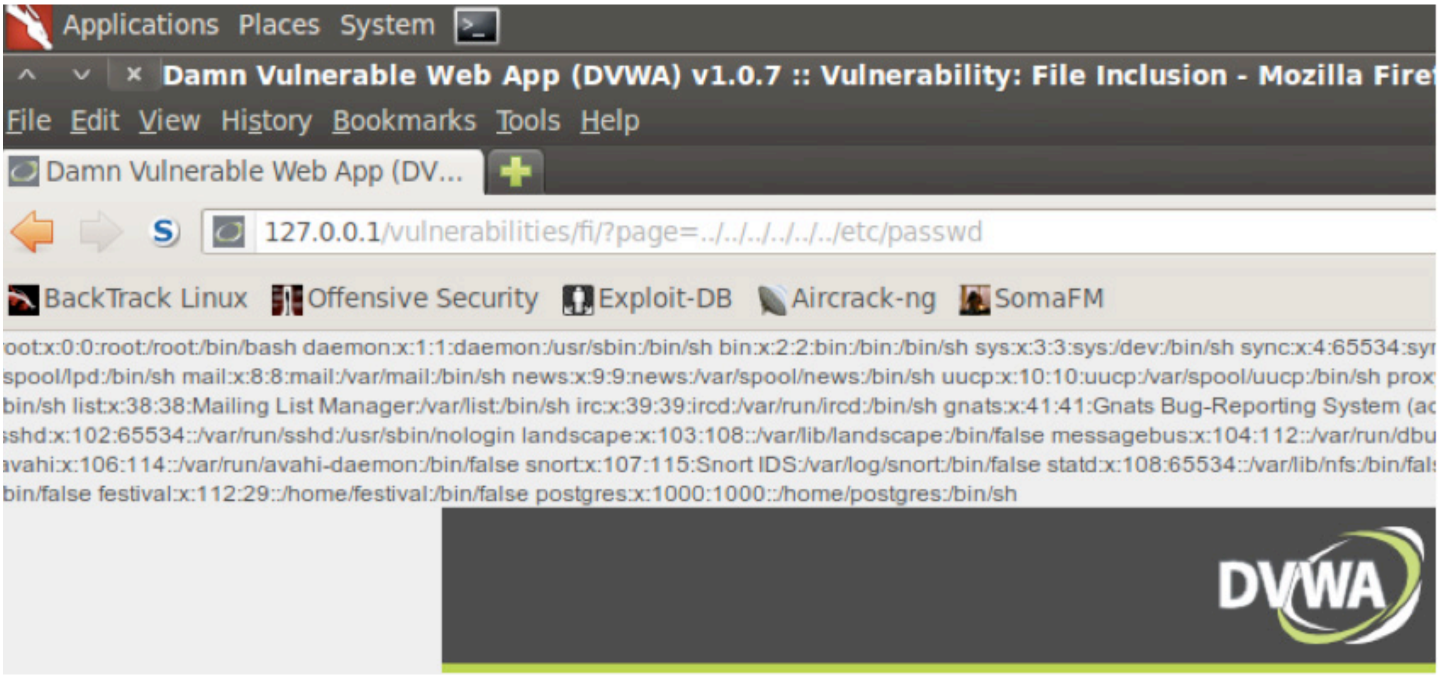
```
root@bt:~# ls
Desktop  DVWA_install.sh  localhost-check.nbe  ZAP.html
root@bt:~# cd ../
root@bt:/# ls
bin    dev   initrd.img  media  pentest  sbin     srv  usr
boot   etc   lib         mnt    proc     selinux  sys  var
cdrom  home  lost+found  opt    root     share    tmp  vmlinuz
root@bt:/# cd var
root@bt:/var# ls
backups  crash  local  log   opt  spool  www
cache    lib    lock   mail  run  tmp    yp
root@bt:/var# cd www
root@bt:/var/www# ls
about.php      dvwa         index.php         php.ini       vulnerabilities
CHANGELOG.txt  external     instructions.php  README.txt    wstool
config         favicon.ico  login.php         robots.txt
COPYING.txt    hackable     logout.php        security.php
docs           ids_log.php  phpinfo.php       setup.php
root@bt:/var/www# cd dvwa
root@bt:/var/www/dvwa# ls
css  images  includes  js
root@bt:/var/www/dvwa#
```

Figure 10 - Web server directory discovery for DVWA environment.

You will be executing a path traversal attack (a.k.a. directory traversal) to retrieve resources from the web server that you have no authorization to in the File Inclusion DVWA exercise. Specifically you will retrieve files from the most notable directories on the DVWA web server. This vulnerability also provides a mechanism to upload, install, configure, and execute additional tools on the web server.

The first step in this attack is to realize where in the file system the application is housed. You won't normally have access to the web server's file system to run **cd** and **ls** commands to fully map out where the application is allowed to operate. You know that you need to break out of the assigned directories, but you just don't know where exactly you are in the overall file structure. I always liken this to stumbling around a dark room looking for a way out. You know there's a door somewhere, but you don't know where it is because of the darkness. Your best bet is to simply walk along the wall until you find the door. If you come to a corner before the door, you just walk along the new wall. Sooner or later you will find the door to escape.

In the context of our path traversal attack, this hunting is done with the up a directory command, which is represented by ../ in the web application world. You can use this dot-dot-slash command as many times as you want once you've identified the path traversal vulnerability. It's not important that you know how many levels deep you are in the directory structure, because when you reach the root directory and attempt to go up a directory, you will stay in root. You could be three or seven or 14 levels deep; as long as you put in 14 or more up commands, you will reach the root directory regardless of where you start. Trying to go up a directory when you'll at the root directory will simply keep you in the root directory, so error on the side of using too many! You can then drill down into your intended directory that you'd like to pillage as shown in Figure 11.


Applications Places System
Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: File Inclusion - Mozilla Fire
File Edit View History Bookmarks Tools Help
Damn Vulnerable Web App (DV...
BackTrack Linux
Offensive Security
Exploit-DB
Aircrack-ng
SomaFM
DVWA

127.0.0.1/vulnerabilities/fi/?page=../../../../../../etc/passwd

```
oot:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sy
spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh prox
bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (ac
sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin landscape:x:103:108::/var/lib/landscape:/bin/false messagebus:x:104:112::/var/run/dbu
avahi:x:106:114::/var/run/avahi-daemon:/bin/false snort:x:107:115:Snort IDS:/var/log/snort:/bin/false statd:x:108:65534::/var/lib/nfs:/bin/fal
bin/false festival:x:112:29::/home/festival:/bin/false postgres:x:1000:1000::/home/postgres:/bin/sh
```

Figure 11 - Retrieving the /etc/passwd file via a path traversal vulnerability in DVWA .

In order for this attack to work as described, ensure that your DVWA is still running with the "low" security level that you configured earlier in the book. Here we are using six instances of ../ when we know that we really only need to use four of the commands to reach the root directory. Once we've reached the root directory, we then request the /etc/passwd file. The contents of the passwd file are displayed back to our web application.

We just used the web application to reach into parts of the file system that it was not authorized to do and extract out sensitive information! All from the comfort of our browser interacting with the application like a normal user.

The ../ rarely works in its natural format like it does here. There are tons of sanitization routines that attempt to identify and remove path traversal characters from user requests. The battle then becomes understanding how these sanitization routines work and how you can circumvent them to still have your attack exploit this vulnerability. A firm understanding of encoding and regular expressions will serve you well in this battle.

## Forceful browsing

Another example of direct object reference is forceful browsing (i.e. forced browsing) where the hacker simply enumerates known filename and directories in search of resources that he shouldn't have access to retrieve. This is exactly what ZAP's Brute Force tool and Nikto do when they search for directory names during the scanning phase.

You can also do this very attack with a custom list in Intruder. This is another place where information gathering in the web server recon and web application recon steps will come in handy. There's no sense in using a list full of typical Microsoft .NET web folder names if you are interacting with a LAMP stack application.

You could even specify several individual parameters to target during a forced browsing attack on any URL as shown here:

```
https://bigbank.com/reports/2013/q1/financial/CashFlow.pdf
```

You could create a list of years, say 2004 through 2013, to cycle through for the 2013 value of this URL. The q1 obviously means the first financial quarter, so q2, q3, and q4 are appropriate directory names to try.

The financial directory could be replaced with any other department in the bank such as loan, HR, legal, travel, and any others that you can come up with. And finally, the CashFlow.pdf file gives us several clues. First, they are using capitalized hump notation for their filenames and .pdf as the filetype. Just these two factors alone would lead to a large collection of possible values to attempt to retrieve.

Consider BalanceSheet.pdf, LoanSummary.pdf, LoanPortfolio.pdf, FinancialStatement.pdf, AnnualReport.pdf, and tons more! Just using ten years, four quarters, five departments, and seven file names gives us 1,400 unique URLs to forcefully request!

Dr. Josh Pauli received his Ph.D. in Software Engineering from North Dakota State University (NDSU) and now serves as an Associate Professor of Information Security at Dakota State University (DSU) in Madison, SD. He has published nearly 30 international journal and conference papers related to software security and his work includes invited presentations from the Department of Homeland Security, NSA, Black Hat Briefings, and Defcon. This article is an excerpt from his latest book, The Basics of Web Hacking, published by Syngress (ISBN: 9780124166004).

# Joel Smith, AppRiver CTO on web threats

by Mirko Zorz

Joel Smith is the CTO of AppRiver. He co-founded AppRiver with CEO Michael Murdoch in 2002, bringing with him more than a decade of experience in the technology sector where he focused primarily on network security and e-mail efficiency. In this interview he discusses web threats, security innovation, and much more.

**How are web threats impacting the way businesses work today?**

Malware has made the move from a primarily email-borne threat to one that is now spread mostly by infected web sites. These are often legitimate sites that have been exploited and now host the malware itself, or have been injected with malicious Javascripts that redirect visitors to sites that host the payload. Other times these legitimate sites will simply serve up malware-laden advertisements from ad networks with minimal security submission processes.

Businesses rely on the Internet to do business these days, so there's little to be done to avoid it. Malware authors and cybercriminals know that and are taking full advantage of the situation. Those especially at risk are those businesses that allow full Internet access to their employees without proper protections in place.

That's why we always recommend a multi-layered approach – a combination of web security, email filtering, desktop AV, a properly configured firewall and other network security appliances and software. However, appliances are most helpful for companies that have trained staff to properly monitor and configure devices. If they are configured poorly, these devices have the potential to do more harm than good.

**Is there innovation in the web application security space or is the industry merely keeping up with the fast-paced threat landscape?**

At times it's a cat-and-mouse game. The biggest obstacle to advancement in the Web application security realm is user convenience. The user experience seems to always take priority over user security. From their perspective, delays caused by in-depth scanning are unacceptable. In fact, recent studies have shown that most users who are faced with a built-in browser block page simply click past them when given the option to do so. Businesses really need to lock down their networks and limit their risk by restricting employee access to all but sites that are necessary to do their jobs. The principle of least privilege is very important to network security.

**What steps are involved in the process of evaluating, implementing and maintaining a successful web application security strategy in a large organization?**

As with any major change in infrastructure, it's important to evaluate new products or solutions in a controlled setting. You have to be sure that adding something new and different isn't going to break anything critical to your operations. It's also important to compare like products to see which is going to be most effective and provide the best return on investment.

Web application security is no different, except that it's sometimes met with grumbling from employees if filtering slows their Internet. If the delays are significant, employees may try to circumvent the filters, which is obviously a big security risk to a business network. It's important to block things such as proxy sites and force DNS resolving at the gateway to avoid the most likely means for employees to get around the filter.

**Based on the ongoing AppRiver analysis, what are the most significant web server exploits at the moment?**

It's clear why attackers go after web servers as their primary targets. Web servers are always on, have more bandwidth and provide a larger target audience. Instead of going out to every one of their intended victims, they can just infect a single web server and wait for their victims to come to it. As they infect hundreds or even thousands of web servers, their pool of potential victims increases exponentially.

A few of the major web server exploits include WordPress PHP Injections, Cross Site Scripting (XSS) attacks, Local File Inclusion (LFI) attacks and even simple password guessing or brute force attacks.

**How dangerous are server-side vulnerabilities? What can organizations do to protect themselves?**

Server-side vulnerabilities are a major concern. If attackers access a company's server, not only can they steal information from that computer, they can also use its trust to pivot into other computers on the network. It's not hard to protect against these threats, but the safeguards are frequently overlooked.

Browser requests to company sites, including web forms, should be sanitized to weed out fraudulent web requests such as Local File Inclusion attacks. They should be restricted to specific input to avoid a common technique known as Cross Site Scripting. A proper (or improper) entry into a web form can potentially lead to access to company databases and all of the information within. Further, all-important company and client data should remain encrypted while at rest to make it worthless to attackers if they get it.

The subject of passwords is one we talk about ad infinitum. That's because good passwords are easy to create and use. Yet people continue to use simple passwords that are short, easily guessable and often used across many sites. That means an attacker guesses one and they've got them all.

Companies need to enforce strict password policies, and the key word here is enforce. Strong group policies are necessary to force employees to comply with strong password protocols and frequent changes. It may be beneficial to consider implementing a multi-factor authentication procedure to give employees access. Even the use of a USB token in addition to a password can go a long way toward creating a more secure environment.

Mirko Zorz is the Editor in Chief of (IN)SECURE Magazine and Help Net Security (www.net-security.org).

## Analysis of Poison Ivy remote access tool

A FireEye report highlights the resurgence of Poison Ivy, a malware Remote Access Tool (RAT) that has remained popular and effective eight years after its original release - attacking dozens of Fortune 1000 firms. In conjunction with the research, the company also released Calamine, a set of free tools to help organizations detect possible Poison Ivy infections.

Poison Ivy has been used in several high-profile malware campaigns, most famously, the 2011 compromise of RSA SecurID data. In the same year, Poison Ivy powered a coordinated attack dubbed “Nitro” against chemical makers, government offices, defense firms, and human rights groups.

The  report identifies several ongoing nation-state threat actors currently using Poison Ivy, including:

- **admin@338:** Active since 2008, this actor mostly targets the financial services industry. FireEye has also observed activity from this actor in telecom, government, and defense sectors.

- **th3bug:** First detected in 2009, FireEye has observed this actor targeting a number of industries, primarily higher education and healthcare.

- **menuPass:** Also first detected in 2009, FireEye research suggests that this actor targets U.S. and overseas defense contractors.

With the Calamine package, security professionals can identify telltale indicators of a Poison Ivy attack – including the attacker’s Poison Ivy process mutex and password, decoded command and control traffic to identify exfiltration/lateral movement, and a timeline of Poison Ivy malware activity.

This evidence is especially useful when it is correlated with multiple attacks that display the same identifying features.

## ZeroAccess developers continue to innovate

A while ago a group of researchers has analyzed and tested the resilience of P2P botnets, and has discovered that while Zeus and Sality botnets are highly resilient to sinkholing attacks, Kelihos and ZeroAccess botnets have weaknesses that can be used to disrupt them.

Sophos researchers have discovered new variants that use new techniques to assure its persistency on the affected computers, and now Symantec researchers say that they have spotted a change in the malware's use of the P2P communication protocol.

"On June 29, 2013, we noticed a new module being distributed amongst ZeroAccess peers communicating on the UDP-based peer-to-peer network that operates on ports 16464 and 16465," they noted. "ZeroAccess maintains a second UDP-based network that operates on ports 16470 and 16471. ZeroAccess peers communicate to other peers connected to the same network; peers do not communicate across networks."

They also made some other changes to the peer-to-peer functionality to decrease the likelihood of outsiders taking control of the botnet, including the introduction of a secondary internal peer list - stored as a Windows NTFS alternate data stream - that can hold over 16 million peer IP addresses instead of the previous 256, and a different logic according to which the peer chooses to contact other peers.

It's interesting to note that while this code changes are already available on the UDP 16464/16465 peer network, they have not been yet implemented on the UDP 16470/16471 network.

"Most of the code changes made by the ZeroAccess authors in this update seem to be in response to published research on ZeroAccess or other perceived weaknesses the authors found in the code. These changes are also further evidence that ZeroAccess continues to be actively developed and remains a threat," the researchers say.

## Got malware?

94.7 percent of Americans received at least one email containing a virus, spyware, or malware, according to Halon. About one in eleven (8.8%) opened the attachment and infected their computer.

Almost a third (30.2%) came dangerously close to doing the same, opening the email but stopping short of opening the attachment. These spam emails bogusly claim to come most often from banking institutions (15.9%), social media sites like Facebook or Twitter (15.2%), and online payment services (12.8%).

One in three Americans admit they would open an unsolicited email—even if it seems suspicious—depending on its subject line. For women, spam email messages containing invites from social networks are alluring, while men are tempted to open ones with the time-tested suggestions of money, power, and sex.

Specifically, the survey found that women are more likely to open emails from social-media related accounts (8.2% to 5.6%), but that men are nearly three times as likely to open unsolicited bulk emails that promise monetary rewards (9.4% to 3.8%) and far likelier to open emails professing to include naked photos of celebrities (2.8% to 0.6%), themselves (2.3% to 0.9%) or friends (1.1% to 0%).

People were alerted to email spam in many cases by a message’s subject line (70.5%), more than half of the time (42.9%) when the text in the subject line was in “ALL CAPS.” Other common triggers that made users aware of spam were the senders email address (67.9%), strange formatting (62.4%) and strange language (56%).

## Popular Windows downloader has secret DDoS capability

Unbeknownst to its users, the popular Windows download manager Orbit Downloader has been outfitted with a DDoS component. The DDoS component has been discovered by ESET researchers while doing a routine examination of the software, and subsequent analysis of previous versions has shown that it was added to orbitDM.exe sometime between the release of version 4.1.1.14 (December 25, 2012) and version 4.1.1.15 (January 10, 2013).

The thing functions like this: the installed software contacts Orbit Downloader's server (at orbitdownloader.com) to download a configuration file containing a list of target URLs and IP addresses, and a Win32 PE DLL file to perform the attack against them.

The software can perform two types of DDoS attacks, depending on whether a third-party tool (WinPcap) is bundled with the Orbit Donwloader.

When this tool is present, the software sends specially crafted TCP SYN packets to the targeted machines on port 80, and masks the sources of the attacks with random IP addresses. If WinPcap is not present, OD sends a wave of HTTP connection request on port 80 and UDP datagrams on port 53 to the targeted machines.

"These attacks, while basic, are effective due to their throughput: On a test computer in our lab with a gigabit Ethernet port, HTTP connection requests were sent at a rate of about 140,000 packets per second, with falsified source addresses largely appearing to come from IP ranges allocated to Vietnam," the researchers noted.

## NetTraveler APT group is back, adds watering hole attacks to its arsenal

The "Red Star" APT group employing the NetTraveler malware family is still active, but has changed its modus operandi. Its targets remain the same: government institutions, embassies, the oil and gas industry, research centers, military contractors and activists.

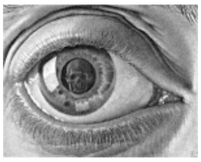
But, while earlier this year they mostly relied on spear phishing emails to deliver a booby-trapped attachment, now they try to lead users to a booby-trapped site or they inject certain websites with malicious JavaScript that will redirect them to such sites.

"Immediately after the public exposure of the NetTraveler operations, the attackers shutdown all known C2s and moved them to new servers in China, Hong Kong and Taiwan," noted Kaspersky Lab's Costin Raiu. "However, they also continued the attacks unhindered."

The latest round of attacks targets Uyghur activists: by spear-phishing emails purportedly carrying a link pointing to a statement made by the World Uyghur Congress regarding a recent massacre, and by compromising the official website of an Uyghur-related website and make it redirect a NetTraveler-related domain where an exploit drops a backdoor on the visitors' computer.

The group has yet to be seen exploiting zero-day vulnerabilities, so for now keeping one's OS, Java and other software updated is enough to prevent becoming a victim.

## Leaked FinFisher presentation details toolkit's spying capabilities



Mikko Hypponen has shared several interesting slides from a presentation that displays the wide range of capabilities offered by the FinFisher commercial spyware toolkit.

Sold by UK-based Gamma Group International, the toolkit was apparently created by Martin J. Muench, one of the founders of the BackTrack pentesting Linux distribution and at the time its main developer.

The presentation mentions FinUSB Suite, a special USB stick designed to covertly extract data from public and target systems. In the hands of an attacker that has physical access to such systems, the device can execute a quick forensic analysis and to extract intelligence.

The FinIntrusion kit is able to discover Wireless LANs and Bluetooth devices, retrieve the 64 or 128 bit WEP passphrase required to access the WiFi network in 5 minutes tops or break the WPA1 and WPA2 passphrase using dictionary attacks, and even emulate a rogue wireless access point.

Once it has gained access to the LAN, it monitors both the wired and wireless network traffic and extracts usernames and passwords for Gmail, Hotmail, Facebook, online banking, and so on - even if the login information is protected by SSL/TLS. It can also remotely break into email accounts, remote infrastructure and webservers by using netwok-, system- and password-based intrusion techniques.

FinFly USB, the backdoor tool deployed from a USB drive, can execute automatically on Windows 2000/XP systems and with one click on Windows Vista and 7, and can apparently even infect switched off target systems when the hard disk is fully encrypted with TrueCrypt.

Finally, FinSpy Mobile is able to compromise iOS, Android, BlackBerry, and Windows Mobile / Windows Phone devices, record incoming and outgoing emails, calls, SMS / MMS messages, perform live surveillance via silent calls, track the victim's location via GPS data and cell IDs, and more.

## Obad Android Trojan distributed via mobile botnets

Difficult to analyze, using a bug in the Android OS to extend Device Administrator privileges to itself without being listed in the list of apps that have them, and lacking an interface, the Obad Android Trojan is extremely stealthy and persistent, and can perform a variety of data stealing, premium-rate messaging, additional malware downloading actions.

Its owners have been taking advantage of four distinct distribution methods, one of which has never been detected before: dissemination via mobile botnet created by using different mobile malware.

It goes like this:

**1.** The victim receives a text message saying “MMS message has been delivered, download from www.otkroi.xxx”.

**2.** By clicking on the link the users downloads the Opfake SMS Trojan which, once run, contacts a C&C server that instructs it to send a message saying “You have a new MMS message, download at - hxxp://otkroi.xxx/” to all he contacts in the victim’s address book.

**3.** By clicking on the link, the recipients automatically download the Obad Trojan. Again, the user must run the file in order for the malware to be installed and start functioning.

According to the researchers, the initial messages are spreading fast, but not all lead to the Obad Trojan, leaving them to conclude that its creators have rented only part of the mobile botnet to spread the malware.

# With big data comes big responsibility: The (in)security of OLAP systems

by Dmitry Chastukhin and Alexander Bolshev

Business intelligence is essential for any enterprise. The process of creating it is based on large amounts of data, which is usually collected over a long period of time. Its results facilitate crucial management decisions that can determine the fate of the company. Is the security of this data worth worrying about? No doubt. But are the technologies used in business intelligence secure?

Business intelligence (BI) is a set of theories, methodologies, processes, architectures, and technologies that transform raw data into meaningful and useful information for business purposes. Consider BI as a software kit designed to help an executive to analyze the information about the company and the environment.

Setting up appropriate BI requires working with large amounts of data. The sources of the data may be a lot of various systems deployed in the corporate network, ranging from ERP system to checkpoint turnstiles.

Big Data from various sources must be unified and structured. It is necessary to optimize the requests made to the analyzed data. But the described methods are certainly not enough if data is processed and stored in classic OLTP (Online Transaction Processing) systems. OLTP systems are optimized for small discrete transactions. But a request for complex information (for example, quarterly sales dynamics for a certain product in a certain branch), which is typical for analytic applications, will lead to complex table conjunctions and to viewing of whole tables. One such request will consume lots of time and computing resources, and current transaction processing will be inhibited.

This is the reason why BI systems use the data processing technology called OLAP (Online Analytical Processing), where aggregated information based on large data arrays is converted into multidimensional structures.

The technologies of Big Data and Business Intelligence gain more and more popularity among large enterprises. In 2011, Gartner analysts distinguished Big Data as the second most important IT trend after virtualization. The amount of processed data in the world is predicted to grow by 48 times in 2020 in comparison to 2009.

OLAP systems are used and developed in many spheres of modern world, from governmental systems for statistical data analysis to ERP systems and online advertising. This kind of solution is used to analyze the performance of production/distribution enterprises, to expose the trends of online marketing, to analyze the characteristics and explicit/implicit feedback given by clients/customers in a certain public or private sector.

Nowadays, almost every big company uses a business intelligence solution: Microsoft (Microsoft Analysis Services), Oracle (Essbase), SAP, MISConsulting SA (icCube OLAP Server), Panorama Software (Panorama). At the same time, there is next to no information about the security of such systems.

## Brief description of OLAP infocubes and MDX

Consider the example of a table that contains the purchase orders of a company. This table may contain some fields like: order date, country, city, customer name, delivery company, commodity name, commodity amount, cost, etc. Imagine that we need the information about the total cost of all orders form all countries and their distribution over delivery companies.

We will then get a table (matrix) of numbers, where column headers will list delivery companies, row headers will list countries, and order costs will be indicated in cells. This is a two-dimensional data array. It is called a pivot table or a cross-table. If we need the same data plus distribution over years, there will be another dimension, and the data set will become a three-dimensional "cube". Now we understand why it is necessary to use multiple dimensions.

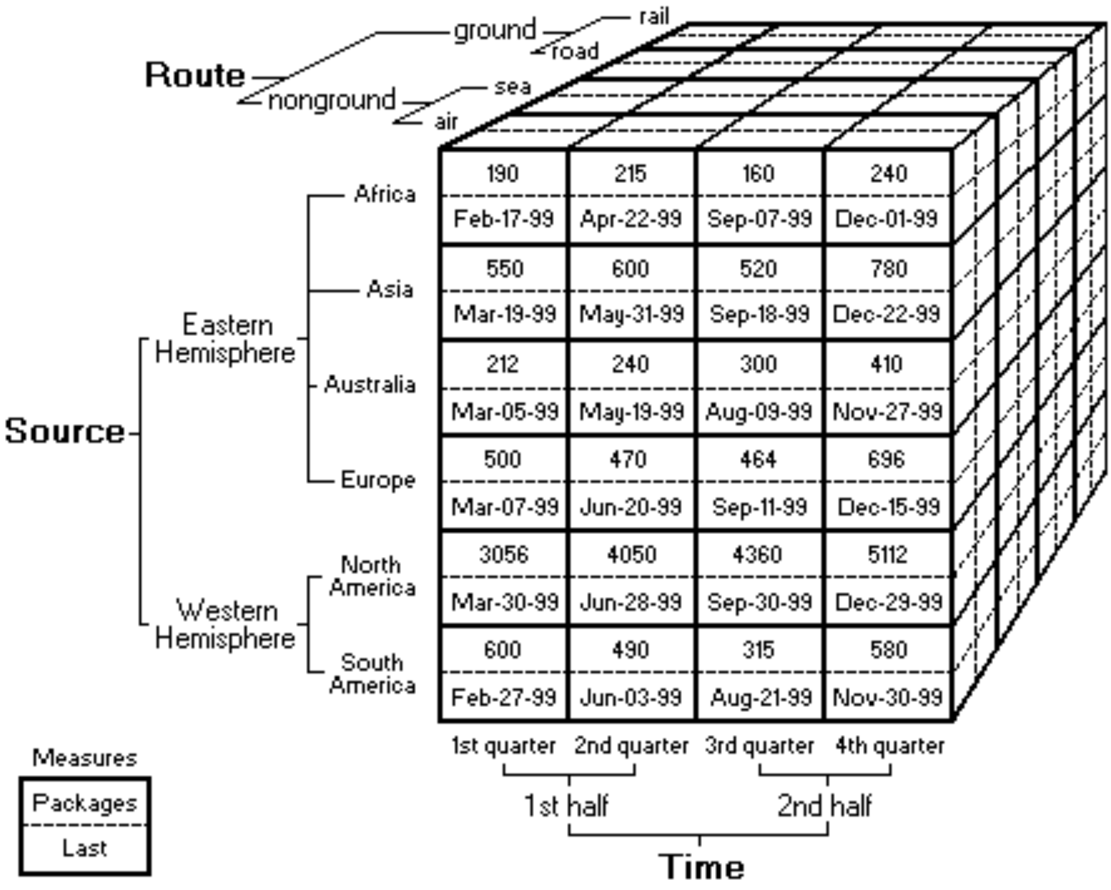
An OLAP cube (also called an infocube) is created by conjunction of tables using "star schema" or "snowflake schema". In the center of the star scheme, there is the fact table, which contains the key facts determining queries.

Dimensions (axes) of the cube are the attributes, and their coordinates are determined by the particular values of the attributes listed in the fact table. For example, if orders were registered for years 2003-2010, the axis of years will contain 8 corresponding points. If orders come from 3 countries, the axis of countries will contain 3 corresponding points, regardless of the number of countries in the reference table. The points of an axis are called "members". The aggregated data is referred to as "measures". Dimensions are better called "axes" to avoid confusion. The set of measures forms another axis: "Measures". It contains as many members (points) as there are measures (aggregated columns) in the fact table.

A figure on the following page shows an example of an OLAP cube which has 3 dimensions: Route, Source and Time, as well as 2 measures: Packages and Last. Every dimension is composed of levels, which, in turn, consist of members. For example, the dimension "Source" contains the level "Eastern Hemisphere", which consists of four members: Africa, Asia, Australia, and Europe.

SQL, the classic query language, is inconvenient for multidimensional data structures. This is why a new language was developed to be used for OLAP queries: MDX. MDX, an acronym for Multidimensional Expressions, is a syntax that supports the definition and manipulation of multidimensional objects and data. MDX is similar in many ways to the Structured Query Language (SQL) syntax, but is not an extension of the SQL language; in fact, some of the functionality that is supplied by MDX can be supplied, although not as efficiently or intuitively, by SQL.

As with an SQL query, each MDX query requires a data request (the SELECT clause), a starting point (the FROM clause), and a filter (the WHERE clause). These and other keywords provide the tools used to extract specific portions of data from a cube for analysis. MDX also supplies a robust set of functions for the manipulation of retrieved data, as well as the ability to extend MDX with user-defined functions.



| | 1st quarter | 2nd quarter | 3rd quarter | 4th quarter |
|---|---|---|---|---|
| Africa | 190<br>Feb-17-99 | 215<br>Apr-22-99 | 160<br>Sep-07-99 | 240<br>Dec-01-99 |
| Asia | 550<br>Mar-19-99 | 600<br>May-31-99 | 520<br>Sep-18-99 | 780<br>Dec-22-99 |
| Australia | 212<br>Mar-05-99 | 240<br>May-19-99 | 300<br>Aug-09-99 | 410<br>Nov-27-99 |
| Europe | 500<br>Mar-07-99 | 470<br>Jun-20-99 | 464<br>Sep-11-99 | 696<br>Dec-15-99 |
| North America | 3056<br>Mar-30-99 | 4050<br>Jun-28-99 | 4360<br>Sep-30-99 | 5112<br>Dec-29-99 |
| South America | 600<br>Feb-27-99 | 490<br>Jun-03-99 | 315<br>Aug-21-99 | 580<br>Nov-30-99 |

An MDX query example:

```
SELECT
   [Measures].[Last] ON COLUMNS,
   { [Time].[1st half].[1st quater], [Time].[2nd half] .[4th quater]} ON ROWS
FROM Test_Cube
WHERE ( [Route].[nonground].[air] )
```

Of course, this is a simple query.  Real MDX queries are much more complex.
MDX supplies a great deal of intrinsic functions, designed to accomplish everything from standard statistical calculation to member traversal in a hierarchy. But, as with any other complex and robust product, there is always the need to extend the functionality of such a product further. To this end, MDX provides the ability to add user-defined function references to MDX statements.

## Attacking OLAP and MDX

There are three basic types of attacks on MDX:

- Unauthorized access to cube data
- Unauthorized modification of cube data
- Attacks on lower level services and OS.

The first type includes the cases where the attacker gets access to the data in a cube (or cubes) that is not designed by the developer for this access level. I.e., using an MDX injection or an attack on mdXML, the attacker gets confidential data from the current cube or other cubes.The second type implies the attacks directed at modifying the data in a cube.

The third type includes attacks on other services and infrastructure as well as direct attacks on the server and the OS where the cube is executed. For example, it can be XXE or remote code execution with an MDX query. Notable attack classes:

- MDX injections
- Attacks which use user-defined MDX functions
- mdXML attacks.

## MDX injections

There are three places in a MDX query where you can usually inject:

- in the WITH section query
- in one of SELECT dimension definitions
- in the WHERE clause.

You can use comments in injections, and in most MDX interpreters, you don’t need to close multiline comment, i.e. you can just type '/*' at the end of your injection string, and the remaining query will be ignored by the MDX system. So, the possibility of injecting in the first dimension of SELECT is equivalent to possibility of writing a fully custom query to the system. I.e., if you have the query:

```
SELECT
{ [Measures].[Salary Paid] }  ON COLUMNS,
{ ([Employee].[Department].[Department].ALLMEMBERS,[Gender].[Gender].ALLMEMBERS)
}
ON ROWS FROM [HR]
WHERE ([Store].[Store].AllMembers)
```

and can inject into the [Salary Paid] part, you can do almost anything. For example, you can modify this query to get login information of employers:

```
SELECT
{ [Measures].[Overtime Paid] }  ON 0,
{ [User name].[User name].ALLMEMBERS } ON 1
FROM [HR] /*[Salary Paid] }  ON COLUMNS,
{ ([Employee].[Department].[Department].ALLMEMBERS,[Gender].[Gender].ALLMEMBERS)
}
ON ROWS FROM [HR]
WHERE ([Store].[Store].AllMembers)
```

## Attacks on UDF

As mentioned earlier, external functions, or user-defined functions, were implemented to increase the flexibility of the language and its capabilities. External functions are the functions developed by the user or a third-party developer, which can receive and return values in MDX syntax. External functions can be called in the same way as normal MDX clauses:

```
MySuperFunction(“hello”,313,37)
```

However, a more formal call procedure also exists. It is necessary if the name of a user-defined function is similar to that of an existing function. This is why external functions are called in this way:

```
«ProgramID»!«FunctionName»(«Argument1», «Argument2», ...)
```

Let’s show some UDF faults on the example of IcCube OLAP server. icCube OLAP Server is quite a popular OLAP solution because it has a free community version, it is cross-platform because it is programmed in Java, and it supports all the basic functions which are necessary to work with multidimensional data: MDX, IDE, web reports etc. There are commercial versions of the system as well.

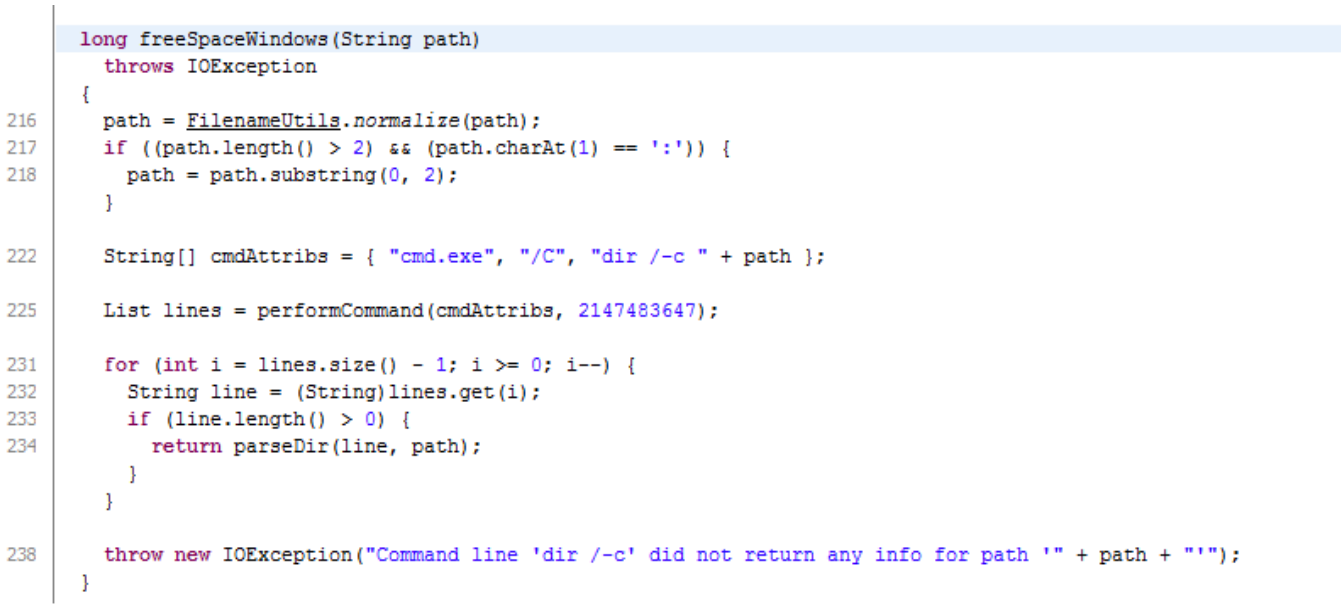
The icCube OLAP Server is written in Java and provides access to static java methods as UDF functions with *J!Method* and *J!Constant* constructions. However, an attempt to execute `System.getProperty("user.dir")` failed because the developers had restricted potentially dangerous Java functions.

But the developer's website said: "if you need Java classes from JAR that are not available with icCube, simply add them to the icCube-install/lib directory". In that directory, a lot of third-party .jar files are available. An evident solution is to try and find some critical static methods in those .jar files.

For instance, the method

**org.apache.commons.io.FileSystemUtils.freeSpaceWindows(String path)**

from the file **commons-io-1.4.jar.**



```
long freeSpaceWindows(String path)
  throws IOException
{
  path = FilenameUtils.normalize(path);
  if ((path.length() > 2) && (path.charAt(1) == ':')) {
    path = path.substring(0, 2);
  }

  String[] cmdAttribs = { "cmd.exe", "/C", "dir /-c " + path };

  List lines = performCommand(cmdAttribs, 2147483647);

  for (int i = lines.size() - 1; i >= 0; i--) {
    String line = (String)lines.get(i);
    if (line.length() > 0) {
      return parseDir(line, path);
    }
  }

  throw new IOException("Command line 'dir /-c' did not return any info for path '" + path + "'");
}
```

The variable *path*, without any filters, goes directly into the parameter that will later be used to call cmd.exe. The method **freeSpaceWindows(String path)** is called by another method **freeSpace(String path)**, which also lacks input parameter checks. It is evidently an OS command injection vulnerability which leads to server-side remote code execution. Exploit code:

```
J!FileSystemUtils.freeSpace("&
calc.exe")
```

## Attacks on mdXML (XML for Analysis)

XML is a very popular data transfer standard. The XML for Analysis (XMLA) standard was developed especially for BI systems. It is based on standards like XML, SOAP, HTTP and allows working with and executing the requests of such languages as MDX, SQL and DMX.

XMLA was developed as the simplest possible standard, so it only contains two SOAP methods:

- Execute
- Discovery

Execute is designed to execute MDX queries and consists of two parameters: Command and Properties. Command specifies the MDX query itself, and Properties specifies the directory name, format and other properties. Discovery allows discovering the structure of multidimensional data. It can help to know the names of cubes, measures, dimensions, members and their properties.

XMLA is based on XML, so it is liable to all attacks typical for XML, like XML External Entities. We will show this attack on the mdXML service of SAP ERP system, which is located at: *http://host:port/sap/bw/xml/soap/xmla*
Let's attempt to read the file c:/passwords.txt from the SAP server, the contents of which are:

My clear text password: secret
Let's use the following request:
POST /sap/bw/xml/soap/xmla HTTP/1.1
Host: 172.16.0.63:8001

```
<!DOCTYPE root [<!ENTITY foo SYSTEM "c:/passwords.txt">]>
 <Execute xmlns="urn:schemas-microsoft-com:xml-analysis">
   <Command>
    <Statement>SELECT Measures."&foo;" ON COLUMNS FROM Sales</Statement>
   </Command>
   </Execute>
```

The external entity will be included in the MDX query. The entity must be enclosed in quotation marks, otherwise a file with special characters or even spaces will be displayed incorrectly. The server will reply with a message about invalid MDX syntax:

```
ERROR_MESSAGE_STATE -e: Invalid MDX command with "My clear text password: secret”
```

SAP Users can install SAP security note 1597066 to prevent form this specific attack.

## Other attacks

Besides direct attacks on MDX and XMLA, this language can be used for various classic attacks. For example, MDX is frequently used to generate reports. The attacker can make use of the fact that the contents of MDX requests are likely to go unfiltered, and use them to transfer XSS, for example.

## Conclusion

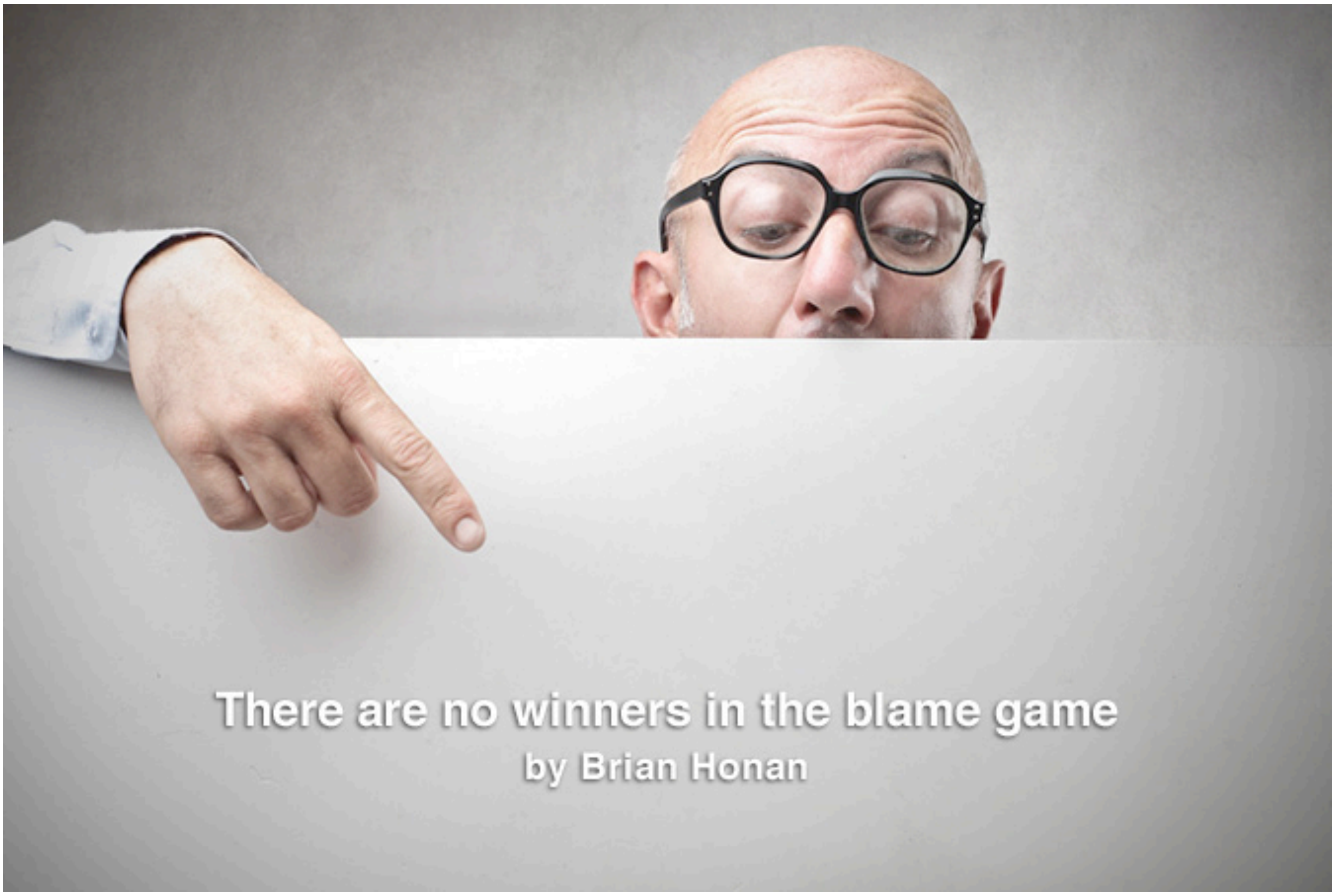
MDX is a very popular language. At this moment, we don’t have an alternative language for multidimensional data requests. It's easy to find hundred of OLAP servers of various companies on the Internet by using search engines. Most of them have a vulnerability that opens a loophole into corporate resources for experienced hackers. If said hackers are successful in attacking Business Intelligence systems, they will kill two birds with one stone: get access to the critical corporate resources and compromise the critical data of the company right away.

The results are reputation risks, loss of information and finances, threats to the further development of any organization. It is yet unclear who or what can prevent cybercriminals from conducting the described attacks.

Dmitry Chastukhin is the director of Pentesting at ERPScan (www.erpscan.com). He works on SAP security, particularly upon web applications and JAVA systems. Dmitry is also a WEB 2.0 and social network security geek and a bug bounty hunter who has found several critical bugs in Yandex, Google, Nokia, Badoo. He is a contributor to the EAS-SEC project.

Alexander Bolshev is a Senior Penetration Tester at ERPScan.

> Visit www.insecuremag.com
> SUBSCRIBE TO (IN)SECURE MAGAZINE



# There are no winners in the blame game

by Brian Honan

Every time a major security breach makes the headlines, a common reaction happens. Even before the details of the breach are known, the information security world gets into a frenzy of speculation as to how the attack happened, who conducted it, and whether the attackers were skilled or not.

Invariably the conversation focuses onto the company that is the victim of the attack, and it often tends to highlight how stupid, negligent or weak its security defenses were. In effect, we blame the victim for being attacked.

While the organization may have been negligent, or their security not up to scratch, we should not forget they are still the victim. How good, or not, the victim's security is is a separate issue for a separate conversation. Foisting blame on the victim on top of having to deal with the incident does not bring much value to the conversation. The blame for the attack should lie squarely on the shoulders of those who conducted it.

Our tendency to blame others for security failings does not stop at the victims of security breaches. Security professionals often berate developers for writing insecure code, when in fact those developers are coding in the way they have been trained. Users are derided, mocked, and blamed for clicking on links, falling for phishing scams, or not following policies, when all they were trying to do was their work.

Management gets blamed for not investing enough money or resources into security. Vendors are blamed for producing and selling products that do not meet our expectations when it comes to protecting our systems. We blame governments for not giving security the attention it should get or not giving the necessary resources to law enforcement to deal with the rise in cybercrime.

It is interesting to note that in all the assigning of blame we very rarely blame ourselves. There is an appropriate saying: “When pointing a finger at someone there are always three of your fingers pointing back at you.” This is something that we in information security need to think about.

Instead of concentrating on the weaknesses of others we should look at our own shortcomings. We never seem to ask why is it that developers have not been trained or made aware on how to code securely? How come users don't understand the risks of clicking on links and attachments or realize that security policies are in place for a reason? Why does senior management not appreciate the risk poor information security poses to the business?

We criticize and berate others for not understanding information security as well as we do, and then wonder why no one will talk to us. We fail to engage with developers, users, and management to proactively understand their requirements. We rarely look at ways to support them so that they can do their jobs in a secure manner.

Blame shames people and makes them less willing to share in the future. Users will be afraid to report potential security breaches as a result of clicking on a link in an email, which will lead to our networks being potentially exposed.

Companies will not be willing to share how they suffered a security breach as they fear the ridicule and negative impact on their image from those who may focus on the inadequacies of their defenses rather than the fact they are a victim. When we don't share our experiences we cannot as an industry learn, and by not learning we will find it more difficult to protect ourselves.

**WE CRITICIZE AND BERATE OTHERS FOR NOT UNDERSTANDING INFORMATION SECURITY AS WELL AS WE DO, AND THEN WONDER WHY NO ONE WILL TALK TO US**

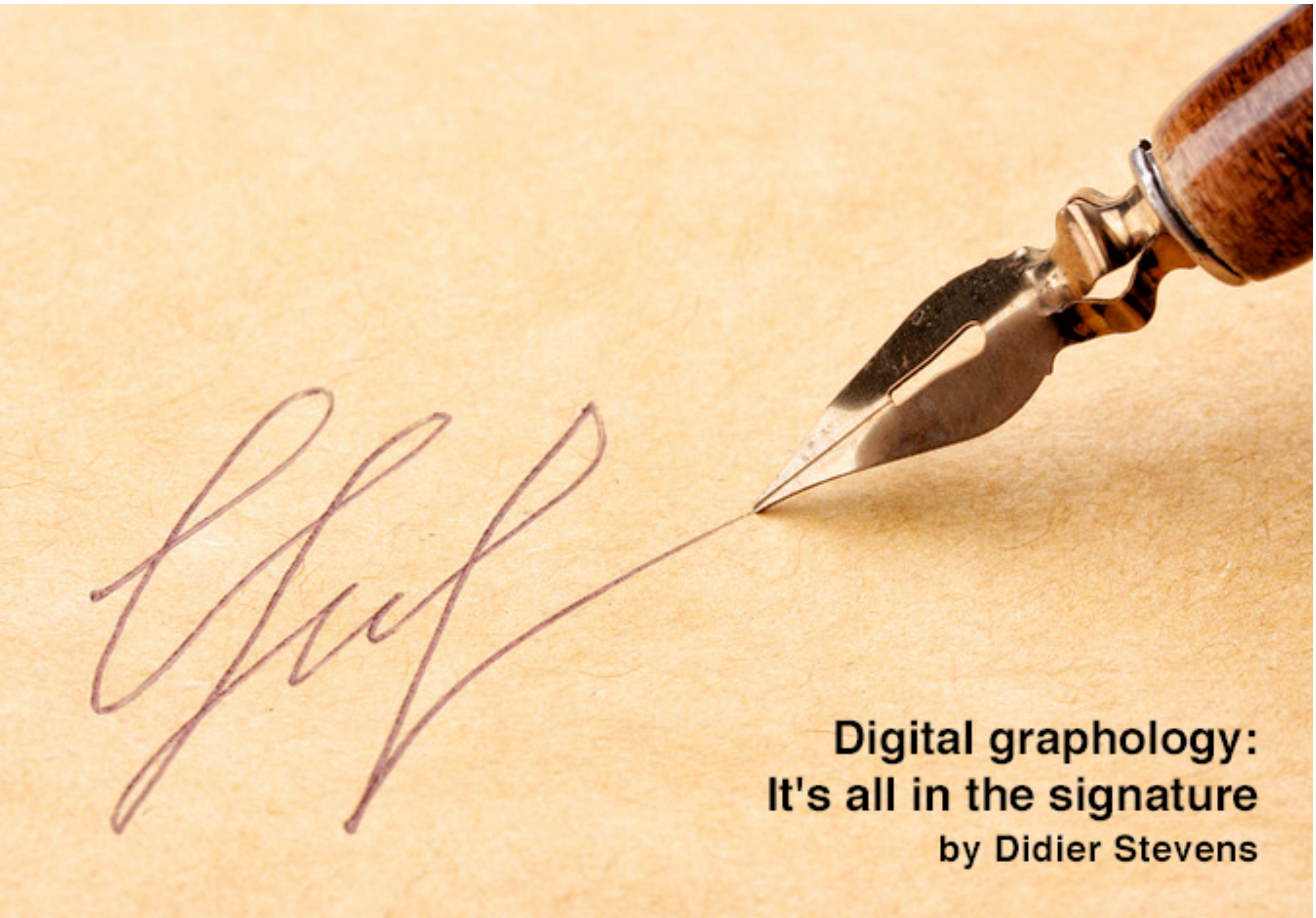
So next time you are dealing with users who do not know how to work in a secure manner, don't blame the users but rather take a step back and try to understand where and how we have failed to enable them to work securely.

When management does not provide the necessary resources to improve information security, let's not blame them for not understanding the issue. Instead let's try to learn how to better present the business case that will get management to approve the investment.

The next time a company's network security is breached remind yourself that they are the victim of a crime. Instead of shaming and blaming the victim, our focus should be on how to stop those responsible for the attacks creating more victims.

In the blame game nobody wins, yet everybody loses. As the famous American novelist John Burroughs said: “You can get discouraged many times, but you are not a failure until you begin to blame somebody else and stop trying.” We have too much at stake in ensuring our systems and networks are secure to fail at what we do. We will be discouraged many times but let's not become failures – let's stop playing the blame game.

Brian Honan (www.bhconsulting.ie) is an independent security consultant based in Dublin, Ireland, and is the founder and head of IRISSCERT which is Ireland's first CERT. He is adjunct lecturer on Information Security in University College Dublin and he sits on the Technical Advisory Board for a number of innovative information security companies. He has addressed a number of major conferences such as RSA Europe, BruCON, IDC and Source Barcelona and numerous others. Brian is author of the book "ISO 27001 in a Windows Environment" and co-author of "The Cloud Security Rules", he regularly contributes to a number of industry recognized publications and is a columnist for Help Net Security (www.net-security.org).



# Digital graphology: It's all in the signature

by Didier Stevens

I'm a big fan of Mark Russinovich's Sysinternal tools. I often use his Listdlls tool to identify active malware that has escaped anti-virus detection on the infected machine. Listdlls is a tool that takes a snapshot of all running processes, and then lists all the executable files (mostly dlls). It has options to check the digital signature and to only list executables without a valid digital signature. This way you can quickly identify malware, working under the assumption that all signed executables are not malicious.

After some time, my need for more features started to grow. For example, I wanted to know about executables with an invalid digital signature. Listdlls would list these executables the same as executables without a digital signature. But such files are more suspicious to me than unsigned files. An invalid signature is often a sign of a modified executable. File infectors will modify executables to include their malicious payload.

I also missed a cryptographic hash in Listdlls' report, like an MD5. A list of MD5s can be quickly checked against blacklists or whitelists, for example with my virustotal-search tool to check these MD5s in VirusTotal's database.

I decided to develop my own free, open source tool with these missing features: ListModules. When ListModules is started, it will take a snapshot of all processes and then analyze all modules (executables like .exe and .dll files) loaded into these processes.

The report is written to a CSV file. Elevate ListModules if you can, because then it will be able to analyze all processes, and not be limited to analysis of the processes of the account that started ListModules. On a 64-bit version of Windows, run the 64-bit version of ListModules. This will prevent WOW (Windows-On-Windows) redirection.

In its first version, ListModules listed all executables with some of their properties (for example the MD5 hash I was missing in Listdlls), followed by some information extracted from the signature, even if the signature was invalid. And for invalid signatures, I included the Windows error code that explained why the signature was considered invalid.

This first version helped me a lot to better analyze running Windows systems and to better understand invalid digital signatures. With each new version, I thought of new file properties that I could add to the report. And with the upsurge in signed malware, I added new signature properties that would help me to identify suspicious signatures.

ListModules became so useful to me, that I started to miss its features in Mark's other digital signature tool Sigcheck. Sigcheck is a Microsoft Sysinternals tool Mark Russinovich developed to check the digital signature of a file. It can check individual files, or all files present in a directory or on a drive. So I developed my own free open source alternative: AnalyzePESig. Essentially, AnalyzePESig can do what Sigcheck does, but it reports the same extensive set of file and signature properties as ListModules. At the time of writing, ListModules and AnalyzePESig have 55 fields in their reports.

## “Discoveries” with my Authenticode Tools

My Authenticode Tools helped me to better understand how digital signatures appear and behave on Windows systems. I propose to share some of my findings here with you.

Some official Microsoft .NET assemblies (DLLs) have no Authenticode signature. You can find them in folders that start with C:\Windows\assembly\NativeImages_... These are .NET executables that are created on your machine with the ngen tool (Native Image Generator) during .NET installations. .NET uses a virtual machine with instructions in the Common Intermediate Language (CIL, formerly called the Microsoft Intermediate Language or MSIL). When assemblies with CIL code are installed on your machine, they are also “compiled” to native machine code that your processor understands (for example x86) with the ngen tool and stored in the native images folders. Since these are DLLs that are generated on your machine, they cannot have an Authenticode signature from Microsoft. Microsoft would need to include a private key to sign these assemblies when they are compiled with ngen, which is a big no-no. Private keys need to be kept secret, they cannot be distributed. To identify .NET assemblies, the report contains fields RVA 15 and CLR Version.

On older Windows systems, I regularly find executables with invalid digital signatures because they are out of their validity period. These would often be from a well-known AV vendor.

Signing certificates have a “shelf-life”: they must not be used after a given date and not before the date they were issued. But you know what happens with digital goods that are past their shelf-life: people still want to use them and change their PC clock to fool the system. A timestamping system was designed to prevent the use of signing certificates after their shelf-life. When an executable is digitally signed, a timestamping service on the Internet can be contacted to produce a counter signature for the signature. This counter signature contains a timestamp from an independent clock and thus guarantees via its signature that the executable was signed with a correct time. I use Verisign's timestamping server when signing my executables.

When a digital signature is signed with a certificate and a counter signature that proves that the certificate was used during its shelf-life, the digital signature remains valid after the shelf-life of the certificate used to produce the signature. But if no counter signature is present, the digital signature becomes invalid after the certificate's shelf-life.

These files I found were signed without a counter signature. To identify such cases, I included the field Countersignature Timestamp. Signed executables were this field is empty, will become invalid after the shelf-life of the certificate.

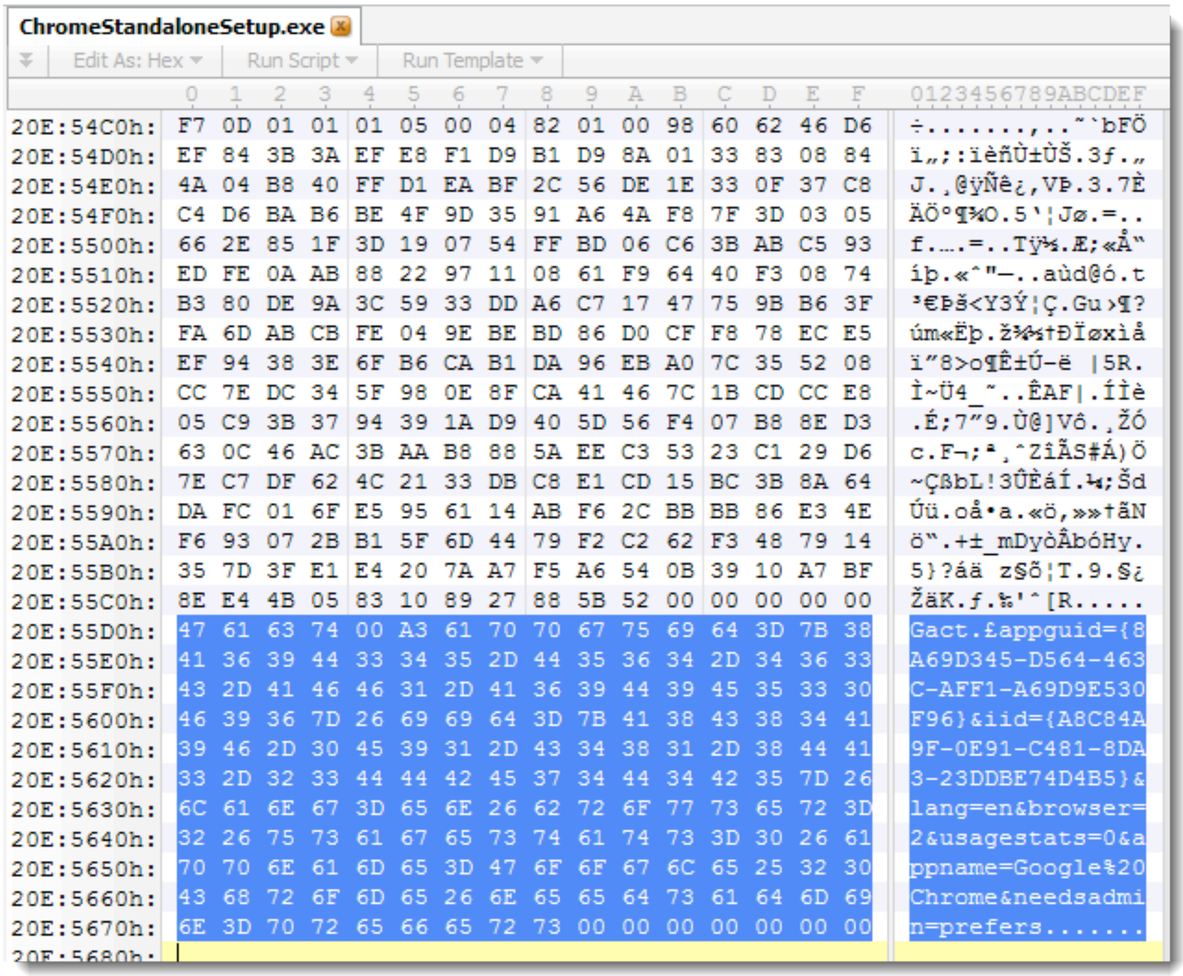
Microsoft prefers to sign executables of the Windows system with catalog files. The signature is not in the executable, but a hash of the executable can be found in a digitally signed catalog file (.cat).

This way, Microsoft does not have to sign individual files. The drawback of this method however, is that you need the catalog file to be able to validate the signature (catalog files are found in C:\Windows\system32\CatRoot\...). If you recover a file from a Windows system, and analyze it on a different Windows version, it is very likely that the necessary catalog file will be missing.

To help with this analysis, I added fields Catalog, Catalogs and Catalog Filename to the reports.

Another peculiarity of the Windows digital signature system I noticed is that signed executables with an invalid signature are reported with a signature timestamp that is equal to the time of checking. But this is not very useful when doing an analysis, because you want to know when the file was actually signed. That is why I extract the timestamp myself from the Authenticode signature (which is a PKCS7 binary data structure).

When a signature is validated, a cryptographic hash (SHA1 by default) of the executable is calculated. But since the signature is included in the file, it has to be excluded from the hash calculation. Data can be added after the signature without invalidating the signature. To detect such data, I included fields like “Bytes after PKCS7 signature”. This helped me to discover setup programs that include instructions for the installer hidden after the digital signature, like this Google Chrome setup program:



```
             0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
20E:54C0h: F7 0D 01 01 01 05 00 04 82 01 00 98 60 62 46 D6  ÷.......‚..˜`bFÖ
20E:54D0h: EF 84 3B 3A EF E8 F1 D9 B1 D9 8A 01 33 83 08 84  ï„;:ïèñÙ±ÙŠ.3ƒ.„
20E:54E0h: 4A 04 B8 40 FF D1 EA BF 2C 56 DE 1E 33 0F 37 C8  J.¸@ÿÑê¿,VÞ.3.7È
20E:54F0h: C4 D6 BA B6 BE 4F 9D 35 91 A6 4A F8 7F 3D 03 05  ÄÖº¶¾O.5‘¦Jø.=..
20E:5500h: 66 2E 85 1F 3D 19 07 54 FF BD 06 C6 3B AB C5 93  f.….=..Tÿ½.Æ;«Å“
20E:5510h: ED FE 0A AB 88 22 97 11 08 61 F9 64 40 F3 08 74  íþ.«ˆ"—..aùd@ó.t
20E:5520h: B3 80 DE 9A 3C 59 33 DD A6 C7 17 47 75 9B B6 3F  ³€Þš<Y3Ý¦Ç.Gu›¶?
20E:5530h: FA 6D AB CB FE 04 9E BE BD 86 D0 CF F8 78 EC E5  úm«Ëþ.ž¾½†ÐÏøxìå
20E:5540h: EF 94 38 3E 6F B6 CA B1 DA 96 EB A0 7C 35 52 08  ï”8>o¶Ê±Ú–ë |5R.
20E:5550h: CC 7E DC 34 5F 98 0E 8F CA 41 46 7C 1B CD CC E8  Ì~Ü4_˜..ÊAF|.ÍÌè
20E:5560h: 05 C9 3B 37 94 39 1A D9 40 5D 56 F4 07 B8 8E D3  .É;7”9.Ù@]Vô.¸ŽÓ
20E:5570h: 63 0C 46 AC 3B AA B8 88 5A EE C3 53 23 C1 29 D6  c.F¬;ª¸ˆZîÃS#Á)Ö
20E:5580h: 7E C7 DF 62 4C 21 33 DB C8 E1 CD 15 BC 3B 8A 64  ~ÇßbL!3ÛÈáÍ.¼;Šd
20E:5590h: DA FC 01 6F E5 95 61 14 AB F6 2C BB BB 86 E3 4E  Úü.oå•a.«ö,»»†ãN
20E:55A0h: F6 93 07 2B B1 5F 6D 44 79 F2 C2 62 F3 48 79 14  ö“.+±_mDyòÂbóHy.
20E:55B0h: 35 7D 3F E1 E4 20 7A A7 F5 A6 54 0B 39 10 A7 BF  5}?áä z§õ¦T.9.§¿
20E:55C0h: 8E E4 4B 05 83 10 89 27 88 5B 52 00 00 00 00 00  ŽäK.ƒ.‰'ˆ[R.....
20E:55D0h: 47 61 63 74 00 A3 61 70 70 67 75 69 64 3D 7B 38  Gact.£appguid={8
20E:55E0h: 41 36 39 44 33 34 35 2D 44 35 36 34 2D 34 36 33  A69D345-D564-463
20E:55F0h: 43 2D 41 46 46 31 2D 41 36 39 44 39 45 35 33 30  C-AFF1-A69D9E530
20E:5600h: 46 39 36 7D 26 69 69 64 3D 7B 41 38 43 38 34 41  F96}&iid={A8C84A
20E:5610h: 39 46 2D 30 45 39 31 2D 43 34 38 31 2D 38 44 41  9F-0E91-C481-8DA
20E:5620h: 33 2D 32 33 44 44 42 45 37 34 44 34 42 35 7D 26  3-23DDBE74D4B5}&
20E:5630h: 6C 61 6E 67 3D 65 6E 26 62 72 6F 77 73 65 72 3D  lang=en&browser=
20E:5640h: 32 26 75 73 61 67 65 73 74 61 74 73 3D 30 26 61  2&usagestats=0&a
20E:5650h: 70 70 6E 61 6D 65 3D 47 6F 6F 67 6C 65 25 32 30  ppname=Google%20
20E:5660h: 43 68 72 6F 6D 65 26 6E 65 65 64 73 61 64 6D 69  Chrome&needsadmi
20E:5670h: 6E 3D 70 72 65 66 65 72 73 00 00 00 00 00 00 00  n=prefers.......
20E:5680h:
```

Since a couple of years, signed malware started to appear. Such malware is often signed with certificates that were stolen from their rightful owner. When this private key theft is discovered, the certificate is revoked by the issuer. But if you are unlucky, you will be the recipient of such malware before the certificate was revoked. To give you a fighting chance to discover this, I included the Subject Name and Thumbprint of the Subject and the Root certificate.

Flame was the first malware found in-the-wild signed with a counterfeited certificate.

Its authors used a novel MD5 collision technique to create this certificate that chained all the way up to Microsoft's root certificate. To achieve this collision, they added data in the Issuer Unique ID field, a field which is normally empty. I added the length of the Issuer Unique ID and Subject Unique ID of each certificate to the report to enable detection of this technique.

## Using my Authenticode Tools

I often use ListModules as a first response tool. I send it to the user with a potentially infected machine, or I use a remote administration tool to run it myself. I have produced versions of my Authenticode Tools with embedded C Runtime (CRT) so that they run on any Windows machine without requiring a runtime installation.

Then I recover the report and filter it with my InteractiveSieve tool. First I hide all signed executables, to better analyze the remaining unsigned files. I search VirusTotal for the MD5s of suspicious files with my virustotal-search.py tool. This method allowed me to identify undetected malware numerous times.

If I find nothing, I review the signed executables. If I still do not find a culprit, I assume the malware is running inside the kernel, or hiding itself from userland applications.

That is the moment when I turn to AnalyzePESig. I recover the harddisk of the suspect machine, and perform a full offline scan with AnalyzePESig. Then I do the same with an online scan, and compare the 2 reports. If I find executables in the offline report, but not in the online report, it is very likely that I found a rootkit or some other type of stealth malware.

On my own machines I use AnalyzePESig in my monthly maintenance. I perform a full scan and compare it to the scan of the previous month.

You can find my Authenticode Tools here - blog.didierstevens.com/programs/authenticode-tools/

Happy hunting!

Didier Stevens (Microsoft MVP Consumer Security, CISSP, GSSP-C, MCSD .NET, MCSE/Security, MCITP Windows Server 2008, RHCT, CCNP Security, OSWP) is an IT Security Consultant currently working at a large Belgian financial corporation. In 2012, Didier founded his own company Didier Stevens Labs. You can find his open source security tools on his IT security related blog at blog.DidierStevens.com.

# Events around the world

## RSA Conference 2013 Europe

www.bit.ly/RSACEU2013

Amsterdam RAI, Amsterdam, The Netherlands

**29 October - 31 October 2013**

## HITBSecConf2013 - Malaysia

conference.hitb.org

InterContinental, Kuala Lumpur, Malaysia

**14 October - 17 October 2013**

## Virus Bulletin 2013

www.virusbtn.com/conference

Maritim Berlin Hotel, Berlin, Germany

**2 October - 4 October 2013**

## Oil & Gas ICS Cyber Security Forum

www.csuae.org

Abu Dhabi, UAE

**7 October - 10 October 2013**

# Security from within: Proactive steps towards protecting corporate assets from attack

by Roy Adar

The abuse of privileged account credentials – which includes administrative accounts, default and hardcoded passwords, application backdoors, and more – continues to be the primary attack vector for almost all targeted cyber attacks.

Regardless of whether attacks are conducted by malicious insiders or outsiders, whether they are politically or financially motivated, or if the attacks are targeted at companies in an attempt to steal sensitive information or intellectual property, attackers are all using the same route to high-value corporate assets.

Once inside the perimeter, attackers will seek a way to escalate privileges as quickly as possible so that they are able to access the assets and applications that really count. With many organizations utilizing cloud service providers, the “perimeter” and potential insiders become even more challenging to control.

Two to three years ago, most organizations that were considering the management of privileged credentials were doing so in order to satisfy compliance requirements in traditionally more regulated industries like banking. Today, businesses are starting to realize that privileged accounts are the first door that attackers knock on, and that the correct management of these credentials is actually more about security than it is about compliance.

Hackers today are guided by collected intelligence, are organized, purposeful, and can be funded and relentless. In order to reach their targets, attackers patiently strive to capture privileged account credentials so that they are able to move undetected throughout an organization with access to almost anything, allowing them to find, gather and exfiltrate sensitive data with relative ease.

The recent stream of high profile breaches has meant that the privileged connection within targeted attacks, such as Advanced Persistent Threats (APTs), has become more widely understood, and not just by IT and security experts. The widespread news coverage about these types of breaches has prompted a broader acceptance of the fact that the abuse of privileged accounts is a major entry point in targeted attacks.

**Privileged account abuse is not just for external attackers.**

However, there is still a disconnect between the knowledge of this privileged connection and businesses taking action to implement systems that can help ensure the effective management of these credentials to protect these valuable accounts.

### The threat of rogue insiders

Privileged account abuse is not just for external attackers. The most recent high profile example of an insider breach is that performed by Edward Snowden. As is common in many organizations, system administrators often have excessive access to information, applications and servers and there is no real segregation of duties. In Snowden's case, he was a systems engineer, systems administrator, senior advisor for the CIA, solutions consultant and telecommunications information systems officer.

This access gave Snowden the ability to view, and ultimately leak, a vast volume of highly sensitive information that he had access to.

It's crucial that employees only have access to information that is essential for their day-to-day jobs, and equally important that these privileges can be revoked in real time in the case of a disgruntled employee or if any suspicious activity takes place on these accounts.

Insider threats don't just come in the form of a malicious or rogue employees - simple human error often plays a major factor in breaches of this type. Furthermore, a common approach by attackers is to go after individual administrators using phishing attacks and social engineering and then impersonate the compromised administrator as they carry out their attack.

If organizations don't have a good grasp on these privileged credentials – which often outnumber the number of employees by three to four times – hackers will have a much easier time taking control of these accounts and credentials to become a "super user", allowing them to anonymously move around a corporate network undetected in order to find their desired assets.

**Insider threats don't just come in the form of a malicious or rogue employees.**

### Application-to-application credentials

In March this year, there was another major example of the malicious abuse of privileged accounts when the computer networks running three major South Korean banks and the country's two largest broadcasters were paralyzed by a cyber attack.

A technical analysis of the attack, which was reportedly attributed to North Korea, showed that the malware deployed was capable of affecting both Windows and Linux machines.

The propagation from Windows to Linux required privileged access, but fortunately for the attackers this was not that difficult as the application stored its privileged access credentials to the Linux environment in plain text within a configuration file, and the hackers used them to propagate their attack to the Linux assets. This attack highlights a well-known problem of application credentials: whenever an application needs to access an asset in the organizational network – be it a database, storage device, or another application – it needs credentials that will enable authentication to authorize the privileged access.

These application-to-application (and often application-to-database) credentials cannot be entered by a human operator in order to gain access, but they need to always be available to the application.

As a result, they can usually be found hard-coded in the application, stored in adjacent configuration files, stored in the application server on which the application relies, or otherwise positioned next to the application that uses them.

By attempting to solve the operational need for providing access between applications, a significant security vulnerability is created. Anyone with activity permissions on the machine that hosts the application - system administrators, application developers, testers or dedicated attackers - can search for and hijack these credentials.

Once accessed, they can be used to impersonate the application and get privileged access to the organizational assets, as was seen in the attack on South Korean banks and broadcasters.

**Best practice steps towards privileged account protection**

In light of the proliferation of these types of attacks, many organizations are looking for proactive steps they can take to better protect themselves from targeted attacks. Protecting privileged accounts is an important part of this, and there are four stages that businesses can follow to ensure better security of these credentials:

1. Understand
2. Control
3. Monitor
4. Respond.

If we look at the first step – understand – this may sound obvious, however research has shown that the majority of organizations underestimate the scope of their privileged account security risk. The Cyber Ark Privileged Account Security & Compliance Survey 2013 found that 86 percent of large organizations either did not know or grossly underestimated the number of privileged accounts within their company, meaning that at least two out of every three privileged accounts in these organizations were either unknown or unmanaged.

**Effective monitoring will help businesses identify irregular or risky activities.**

Understanding therefore includes not only knowing how many accounts there are, but also knowing which of these accounts are protected and properly managed. This means being aware of what people are able to view, what systems they can access, and if there is a real legitimate need for those privileges.

Once businesses discover the number of accounts that they have to contend with, both on-premise and in the cloud, the next step is putting the right processes in place to control these accounts and determining the necessary security policies. Good security policies will provide both strong controls, but on the other hand will align with IT operations procedures and will be as transparent as possible for the IT and operational teams.

An important best practice for controlling privileged access is to ensure session isolation, often enabled by the concept of "jump server" or "privileged account proxy", which creates full isolation between a potentially infected administrator desktop and a sensitive target asset. Controlling privileged accounts and sessions not only helps to improve security processes but is also useful proof that regulatory compliance requirements have been met.

Once organizations have understood the scale of their privileged account problem and have taken steps to isolate and control the use of credentials and access to critical business systems, monitoring the use of these privileged accounts on an on-going basis is a must.

Effective monitoring will help businesses identify irregular or risky activities and will alert them when something goes wrong. As many organizations have central security monitoring or security operation centers (SOC), it is very common to have privileged account activity monitoring integrated for real-time event reporting.

Ultimately, effective monitoring helps businesses to focus on risky activities or abnormal behavior such as accounts being accessed at unusual times of day compared to normal use, and ignore normal activity.

The final step in the processes is having the right tools in place to respond to these issues – whether it's revoking privileges while individual instances are investigated or patching a security hole that has been identified.

Without central controls and continuous monitoring in place, it's difficult for businesses to stop an attacker operating on the network once the perimeter has already been breached and the hacker has been successful in escalating their privileges.

The privileged connection in cyber attacks is well documented and is not going away any time soon – it's inevitable that attackers will look to become the most powerful players in the room as early on in the attack as possible, so that they can access the most valuable information as fast as possible and leave as few traces as possible.

Protection from within is absolutely invaluable, and while there is no silver bullet to secure a company from today's advanced and targeted threats, removing the ability for attackers to hijack and abuse privileged accounts unnoticeably is a crucial proactive step that organizations can take.
Perimeter breaches are inevitable, and security teams should be aware that it's a question of "when" not "if" they will be targeted in an attack - internally or externally.

By understanding, controlling and monitoring activities on all privileged accounts, businesses can be sure that only the right people are accessing critical information and for legitimate purposes, and even if credentials fall into the wrong hands, business can reduce their exposure dramatically by being able to respond faster and lock down paths to their critical information before the attackers get away with it.

---

Roy Adar is the VP of product management at Cyber-Ark (www.cyberark.com).

# HITBSECCONF2013
# MALAYSIA

OCTOBER 14-17 @ INTERCONTINENTAL, KUALA LUMPUR

## TECHNICAL TRAINING SESSIONS

- The Art Of Exploiting Injection Flaws
- iOS Exploitation Techniques
- Diving Into Windows Kernel Internals
- Blackbelt Penetration Testing
- Extreme Web Hacking
- The Android Exploit Lab

Keynote 1:
ANDY ELLIS
(CSO, Akamai)

Keynote 2:
JOE SULLIVAN
(CSO, Facebook)

http://conference.hitb.org

# The five biggest reasons your IT staff is losing sleep

by Troy Gill

Every job has its worst-case scenario, its “code red” condition that we work desperately to avoid.

A massive disaster might fuel emergency workers' nightmares. For stockbrokers, it might be financial collapse. Lawyers might fear losing a high-profile case.

But if you want to peer into the nightmares of network administrators and IT security professionals, you can expect to find one or more of the following trends lurking in the shadows of their minds.

## Hacktivism on the rise

Hacktivism reached new levels in 2011, 2012 and the trend is continuing in 2013. Hacktivists are now posting their targets (often in advance) on open forums as well as the spoils of their crime after the fact. Countless numbers of breaches have been perpetrated and the stolen data that often includes usernames, passwords and the like are being posted on open forums as evidence of their success.

The targets are often chosen due to some perceived wrongdoing on their part. Usually big companies or law enforcement agencies are targeted with the intention of damaging their reputation or disrupting their business, but the individual users / customers are made to suffer along with them.

In August of 2013, The Syrian Electronic Army managed to compromise some major US media outlets including The Washington Post, CNN and Time. The SEA was able to compromise a third party software provider called “Outbrain” which provided a widget that was being used by these media outlets. In previous attacks they have used hacked accounts to broadcast their message and it appears that was the same motivation in this attack. For about a half hour, many readers were being redirected to the SEA website. The attacks were identified, the websites cleaned up and there are no further issues affecting the sites.

## A vast array of web-based threats

We have seen a huge spike in malware being hosted / distributed via web pages in the past several years and they are driven in large part by exploit kits such as Redkit or Blackhole. Both have become available to those wishing to enter the malware distribution market and, as effective as they are, have resulted in a lot of compromised websites.

The compromised website often ends up hosting a malicious JavaScript that redirects visitors to the cybercriminals' malware install. There are a myriad of methods used to drive web users to these compromised sites: emails with malicious links, SEO based search poisoning, click-jacking and posts on social networks, and so on.

### Mobile exploits

Android devices accounted for the majority of smartphone sales worldwide in Q1 of 2013. As the number of people using these devices has grown at a rapid pace, so has the variety and availability of malware targeting them. In fact, various reports have shown that malware targeting Android devices is now somewhere above 90 percent of all mobile device-based malware. While some threats still exist for the Symbian OS, they are on the wane.

Malware writers appear to be now focusing their efforts almost exclusively on Android devices, with the total number of malware variants more than doubling over the past year. The attackers' motivation is the same as with nearly all PC malware: profit.

Android's ”open” type policy makes it attractive to developers and gives users easier access to mobile apps, but this is proving to be a double-edged sword. While other mobile operating systems usually limit the permissions that an app developer can ask of users, Android has a more casual approach. Many new malware variants are emerging to take advantage of this approach.

**Many of the malware variants found today are Trojans aimed at stealing personal data, financial data, and misappropriating device resources.**

While the majority of mobile malware we have seen emerge has infected users via malicious app install, the infection vectors are now beginning to look more and more like those used for PC malware. One piece of malware that has been spotted in the wild using one of these classic techniques starts with botnet-based spam messages aiming to entice users into clicking on a link. If the link is followed from an Android device, the user will be directed to a “Flash Player update" (sound familiar?). Once installed, this malware starts making expensive phone calls.

Many of the malware variants found today are Trojans aimed at stealing personal data, financial data, and misappropriating device resources.

The level of complexity of some of these threats is cause for alarm. In fact, there are now multiple forms of mobile malware that is used in tandem with PC malware (such as the Zeus banking Trojan) to defeat two-factor authentication. How does it work? A cybercriminal attempts to log into your bank (Bank A) via an infected PC. Bank A, instead of requiring only the standard username / password combo, also requires a temporary verification code that the user receives via SMS. The SMS is sent to the infected mobile device of the bank account holder and the data is delivered to the attacker to be used to defeat the added security measure.

As the volume of mobile malware rises, and their functionalities and the infection methods used to deliver it are becoming more broad, the availability of such malware is also becoming greater than ever before.

The growing demand for smartphone devices worldwide coupled with the popularity of the Android platform is pretty much a guarantee that these threats will only continue to advance.

Situational awareness is key.

### Advance Persistent Threats

Advanced Persistent Threats (APTs) are attacks targeting either political / governmental or business entities. Unlike the vast majority of attacks that are aimed at getting in and out as quickly as possible for immediate financial gain, APTs are generally more stealthy with a much greater focus on maintaining a presence on the system.

APTs often utilize the same infection vectors as other attacks such as spear phishing emails, web-based drive-by infections, DNS based attacks, infected USB sticks (or other hardware), external hacking.

The initiators of these attacks often combine an array of attack tools and methods to increase their effectiveness. The attacker tends to take a very detailed and patient approach to get from the entry point of the attack to the actual target.

The ultimate goal can vary from data that the attacker exfiltrates from the infected system or, like in Stuxnet's case, the destruction of a very specific target (Iranian nuclear centrifuges).

Another important factor to consider with APTs is that the target entity is not just being targeted by a piece of malware but maybe a dedicated human or a team of them, making the likelihood of success infinitely greater. Perhaps the scariest part of these attacks is that you may never know you were a victim.

Perhaps the scariest part of these attacks is that you may never know you were a victim.

### State sponsored attacks

In recent years state sponsored espionage and intellectual property theft has garnered a great deal of attention - and rightly so. In early 2013, South Korean banks and television broadcasters were the target of a massive cyber-attack that was believed to have been a sponsored by North Korea.

Reports by US security company Mandiant state that the group dubbed “Unit 61398” - believed to be sponsored by the Chinese government -  had stepped up their activity in 2013.

This is just a small part of what's happening on this front, but the most disturbing fact is that attacks like these are happening more and more around the world.

### Conclusion

If your IT staff is looking a little rough around the edges lately, keep in mind that this is the new reality that they’re facing every day.

And keep in mind, there is no silver bullet for any one of these threats. There is no magical charm that will stop hackers from infiltrating your network or prevent data thieves from stealing your information. Instead, it takes layers of security, constantly updated and tested by experienced professionals.

It’s up to your team to identify the threats that pose the greatest risk to your company and your customers and make every effort to mitigate those risks. Situational awareness is key. Nightmares come in different forms for different people. This is what they look like for the men and women who provide your network security.

Troy Gill is the Senior Security Analyst at AppRiver (www.appriver.com).

# How to manage your passwords with KeePass

by Joshua Dionne

Passwords are one of the most troubling aspects of our online-centric culture. There are so many sites that want you to join them to use their service that remembering all those passwords is a pain. Most people will stick to a single “formula” for a password, and add complexity here and there when they need a “more secure” version for a banking site or a business e-mail account.

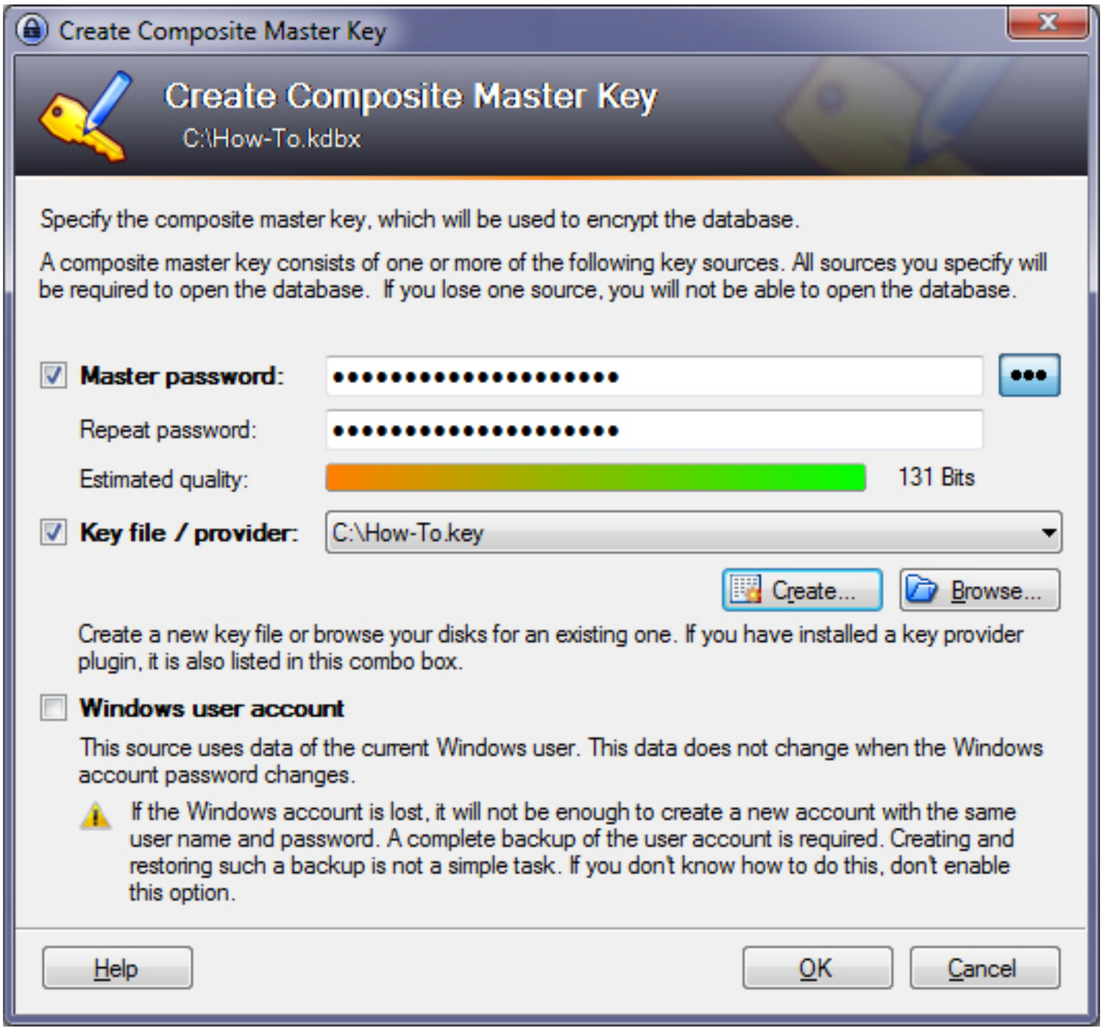
I used to do this, even though I knew it would be advisable to change that habit. None of my passwords ran over 10 characters, though 8-10 is generally thought “secure” against crackers. I had heard about password managers, both online and offline ones, but almost never saw an in-depth “how-to” article for setting one up, wean yourself from your previous habits, and secure it. That’s what I aimed to change with this article.

After extensive reading about the various options, I chose KeePass (www.keepass.info). There are two versions available, and they are both actively developed (in near-parallel), open source projects, with plenty of plugins to add or extend functionality. First, you want to download KeePass; I chose 2.x, since I mostly run Windows, and it can be run in Linux using Mono, if need be.

Installing is a simple affair, creating a database also pretty easy. You can choose the name and location of your database, in Windows 7 it defaults to your Documents folder. You should only have to do the following once.

## Create your database

Here, you will be required to create a master password, and a few other options. I personally use a Master Password, and a Key. Basically, this is like 2-Factor Authentication, without the need for a second physical device. According to the KeePass devs, the keyfile is encrypted with the following algorithm: SHA-256(SHA-256(password), key file contents). You can put the database anywhere, and the keyfile somewhere else, on a USB drive you have with you at all times, which is now required along with the Master Password to open this database. If you choose to create a keyfile (I highly recommend you do), the Entropy Collection screen will come up, and should become familiar soon enough.



Create Composite Master Key

## Create Composite Master Key

C:\How-To.kdbx

Specify the composite master key, which will be used to encrypt the database.

A composite master key consists of one or more of the following key sources. All sources you specify will be required to open the database. If you lose one source, you will not be able to open the database.

☑ **Master password:** ••••••••••••••••••••

Repeat password: ••••••••••••••••••••

Estimated quality: 131 Bits

☑ **Key file / provider:** C:\How-To.key

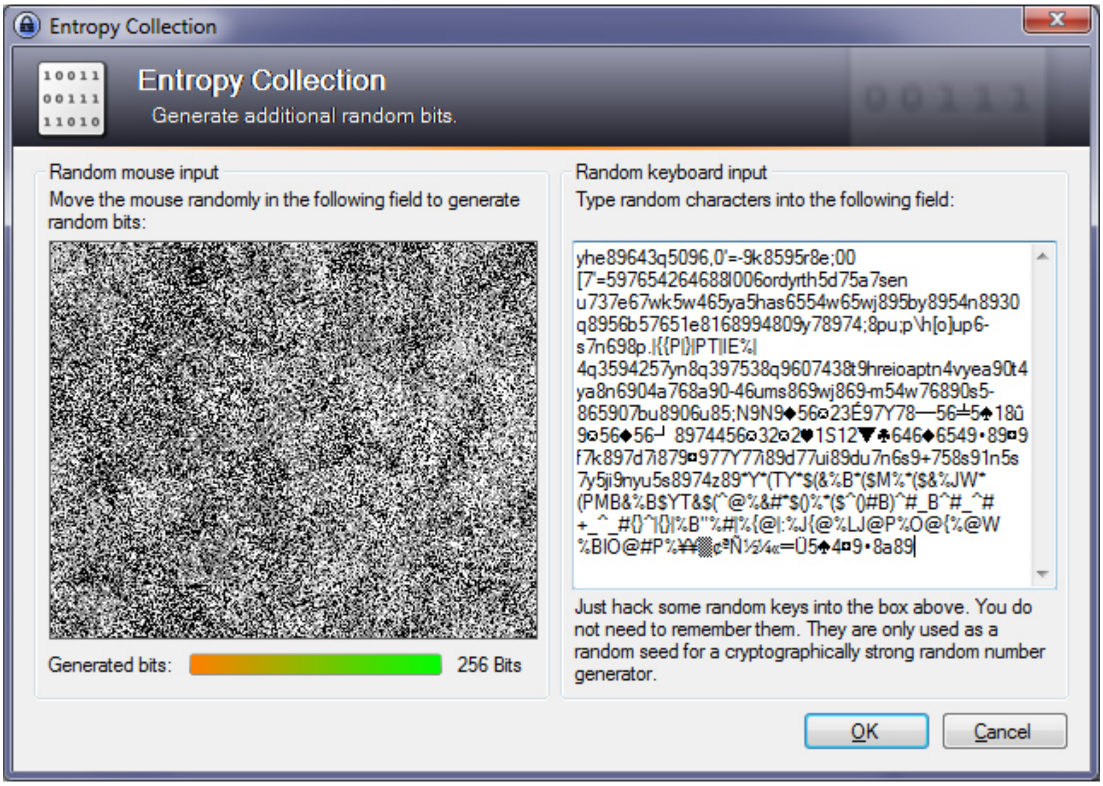
Create a new key file or browse your disks for an existing one. If you have installed a key provider plugin, it is also listed in this combo box.

□ **Windows user account**

This source uses data of the current Windows user. This data does not change when the Windows account password changes.

If the Windows account is lost, it will not be enough to create a new account with the same user name and password. A complete backup of the user account is required. Creating and restoring such a backup is not a simple task. If you don't know how to do this, don't enable this option.

Just follow the directions. Ideally, it should look something like this:



Entropy Collection

## Entropy Collection

Generate additional random bits.

Random mouse input

Move the mouse randomly in the following field to generate random bits:

Generated bits: 256 Bits

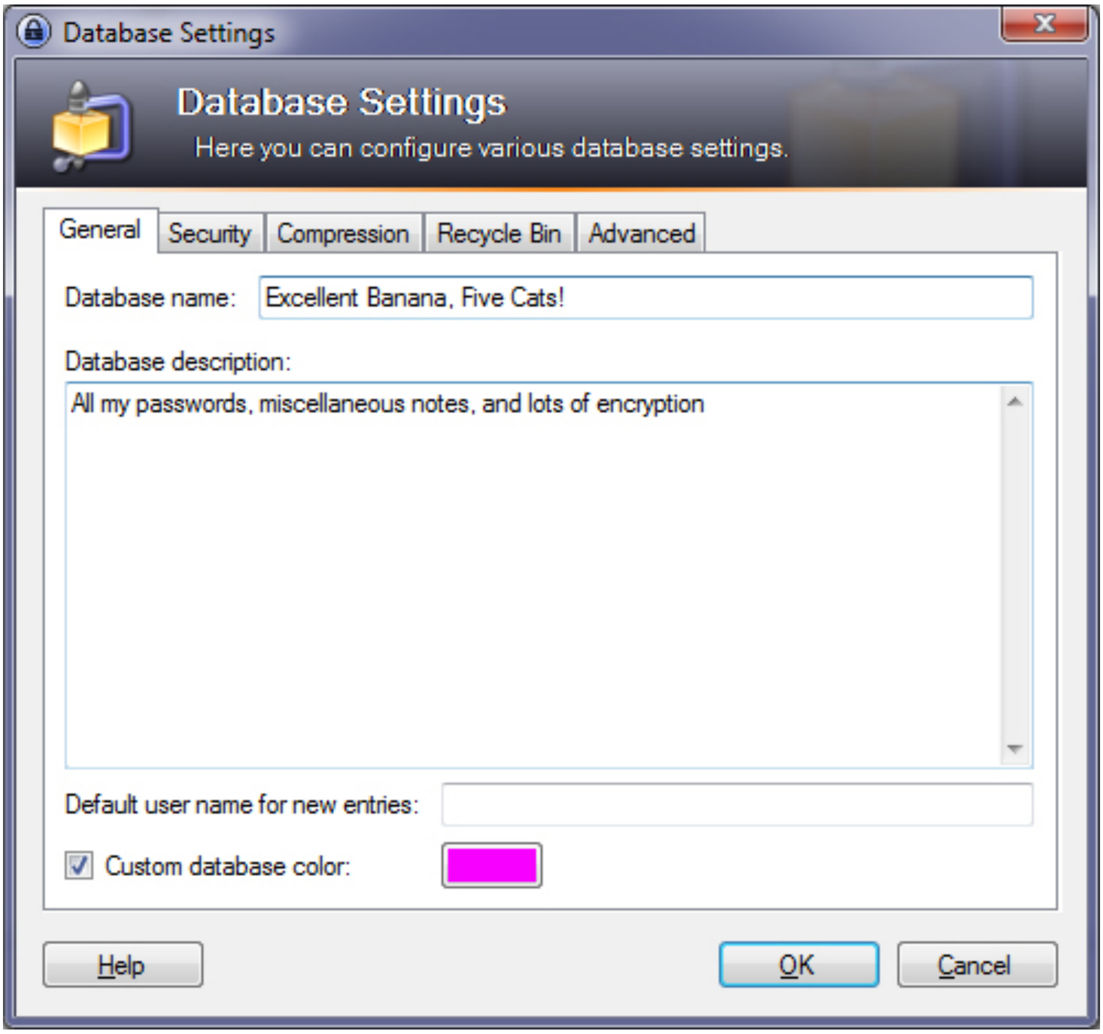
Random keyboard input

Type random characters into the following field:

```
yhe89643q5096,0'=-9k8595r8e;00
[7'=597654264688l006ordyrth5d75a7sen
u737e67wk5w465ya5has6554w65wj895by8954n8930
q8956b57651e8168994809y78974;8pu;p\h[o]up6-
s7n698p.|{{P|}|PT||E%|
4q3594257yn8q397538q9607438t9hreioaptn4vyea90t4
ya8n6904a768a90-46ums869wj869-m54w76890s5-
865907bu8906u85;N9N9◆56☒23É97Y78—56╧5♠18û
9☒56◆56┘ 8974456☒32☒2♥1S12▼♣646◆6549•89¤9
f7k897d7i879¤977Y77i89d77ui89du7n6s9+758s91n5s
7y5ji9nyu5s8974z89*Y*(TY*$(&%B*($M%*($&%JW*
(PMB&%B$YT&$(^@%&#*$()%*($^()#B)^#_B^#_^#
+_^_#{}^|{}|%B"%#|%{@|:%J{@%LJ@P%O@{%@W
%BIO@#P%¥¥▒¢ªÑ½¼«=Ü5♠4¤9•8a89
```

Just hack some random keys into the box above. You do not need to remember them. They are only used as a random seed for a cryptographically strong random number generator.

And now comes the "hard part": a bit of customization and the changing of one option. You can enter whatever you like here; give it a goofy name, describe your database (work, home), change the color of the DB, and so on, before moving on to the Security tab.



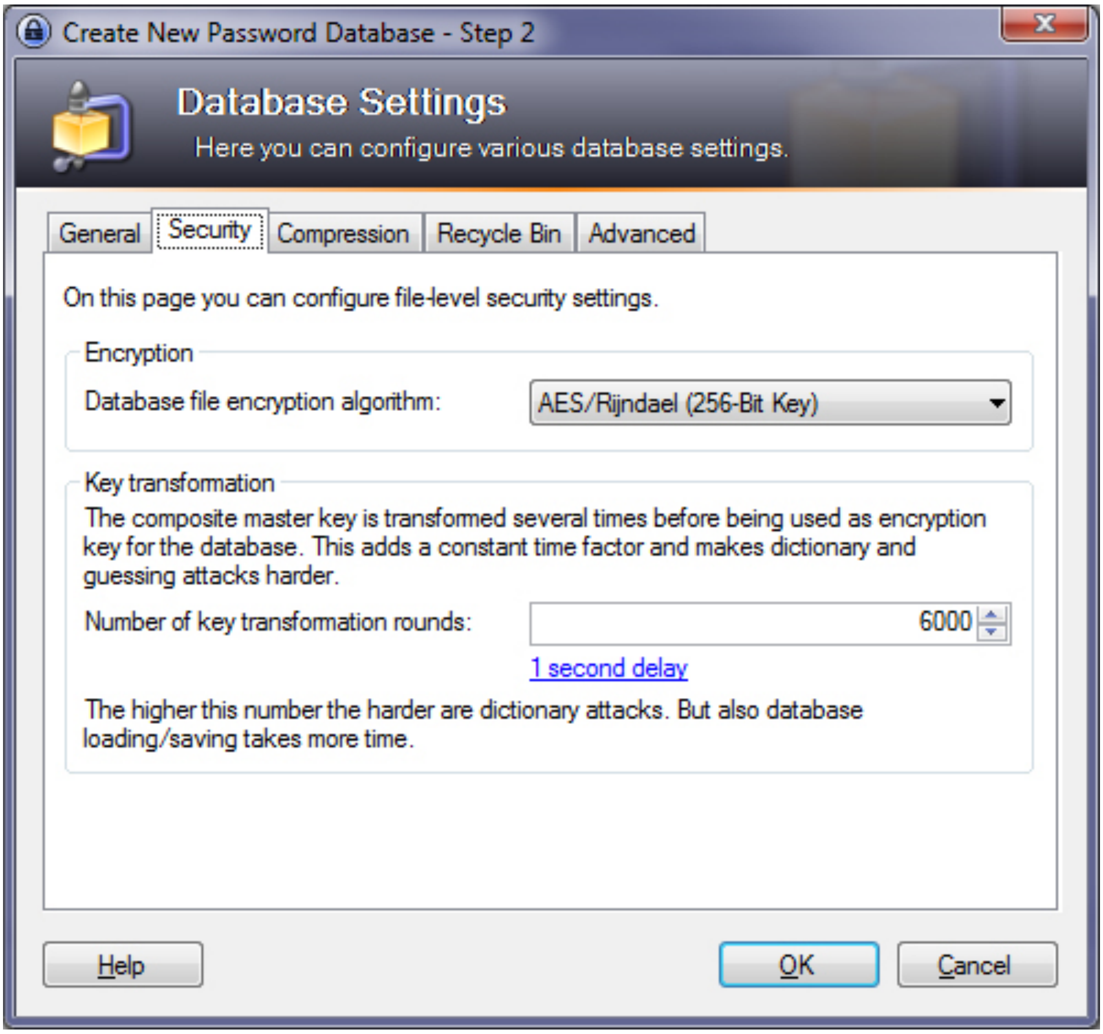
Database name: Excellent Banana, Five Cats!

Database description:

All my passwords, miscellaneous notes, and lots of encryption

Default user name for new entries:

☑ Custom database color: 🟪


Create New Password Database - Step 2
Database Settings
Here you can configure various database settings.
General
Security
Compression
Recycle Bin
Advanced

On this page you can configure file-level security settings.

Encryption

Database file encryption algorithm: AES/Rijndael (256-Bit Key)

Key transformation

The composite master key is transformed several times before being used as encryption key for the database. This adds a constant time factor and makes dictionary and guessing attacks harder.

Number of key transformation rounds: 6000

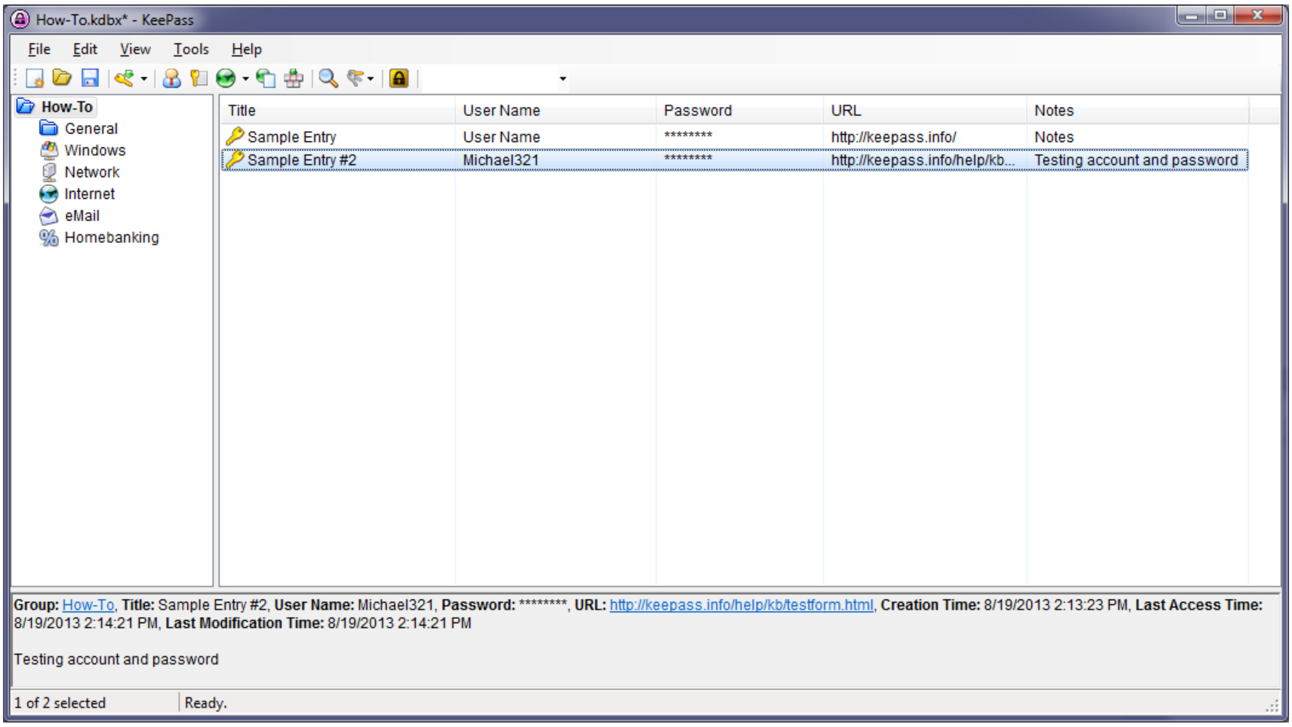
1 second delay

The higher this number the harder are dictionary attacks. But also database loading/saving takes more time.

You will see the Key transformation area has itself set for 6000 rounds of AES-256. The more rounds, the harder to brute force your database. Hit the “1 second delay” button, and let it do its thing.

Depending on your computers’ CPU speed and instruction set, yours may be higher or lower. For this example, I am using a Core i5 3570K, running at 4.2GHz. Yes, that’s 20 million rounds. You can leave that as it is, or make it lower / higher, depending on your needs for different machines. I generally set mine higher, and wait while a P4 516 drags on to decrypt my DB at work. I’ve timed it (unofficially, with stopwatch) at 14.5 seconds as the fastest decryption time.

Below is your new DB, with a few sample entries to get you familiar with using them. Open one and see what options you can edit.



- How-To
  - General
  - Windows
  - Network
  - Internet
  - eMail
  - Homebanking

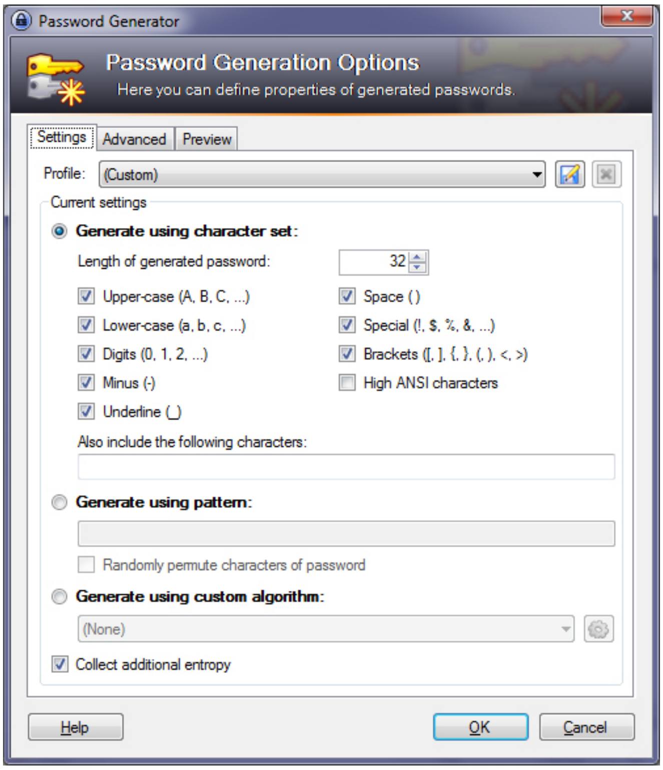
| Title | User Name | Password | URL | Notes |
|---|---|---|---|---|
| Sample Entry | User Name | ******** | http://keepass.info/ | Notes |
| Sample Entry #2 | Michael321 | ******** | http://keepass.info/help/kb... | Testing account and password |

**Group:** How-To, **Title:** Sample Entry #2, **User Name:** Michael321, **Password:** ********, **URL:** http://keepass.info/help/kb/testform.html, **Creation Time:** 8/19/2013 2:13:23 PM, **Last Access Time:** 8/19/2013 2:14:21 PM, **Last Modification Time:** 8/19/2013 2:14:21 PM

Testing account and password

1 of 2 selected | Ready.

Here you can alter all the fields. Right next to the Repeat field is the Password Generator selection.


Password Generator
Password Generation Options
Here you can define properties of generated passwords.
Settings
Advanced
Preview
Help
OK
Cancel

Profile: (Custom)

Current settings

● **Generate using character set:**

Length of generated password: 32

☑ Upper-case (A, B, C, ...)
☑ Space ( )
☑ Lower-case (a, b, c, ...)
☑ Special (!, $, %, &, ...)
☑ Digits (0, 1, 2, ...)
☑ Brackets ([, ], {, }, (, ), <, >)
☑ Minus (-)
☐ High ANSI characters
☑ Underline (_)

Also include the following characters:

○ **Generate using pattern:**

☐ Randomly permute characters of password

○ **Generate using custom algorithm:**

(None)

☑ Collect additional entropy

By default, KeePass supports Auto-Type via key combination Ctrl+Alt+A. In my experience, it works in most browsers; I've tried it in Firefox and IE, though I imagine it works just as well in Safari, Chrome, Opera, etc. You may have to create the association with .kdbx files before this will work properly on some machines, especially with IE. As for migration from using a browser-based password storage solution, I have found you can go two routes: Manually input all that information into new entries, or via some automation. Since I use Firefox as my main browser, all my passwords were stored there (in plain-text!) I used Firefox-to-KeePass Importer (www.keepass.info/plugins.html#ffimport) while Firefox was closed. I left all the options at defaults, and then let it do its thing. It worked well for me, so I imported it into KeePass, with its shiny new and empty database.

And that should be it! After you have installed, configured, imported, and checked everything over again, you should be set to go about business as usual! You can now delve deeper into the password generator for various options, and start upgrading the security of all your passwords!

## PRO TIPS

- While there are versions for other platforms (Android, PocketPC, iOS), all seem to be community contributed builds using some KeePass piece, rather than officially sanctioned and vetted software, so downloader beware!
- Don't forget to check all sites to make sure they login properly.
- Make sure your browser is no longer saving/ auto-typing your passwords after the switch; for most browsers, it's somewhere in their options.
- You can click around in the entropy collection mouse input box, too.
- You can use high ANSI characters/symbols for cryptographic seed generation in the keyboard input area; try ALT+171, ALT+157, and ALT+0172
- Using the built-in rules, you can change your WiFi networks' WPA2 passphrase, and even store it in your database.
- Auto-inserting a password into an entry only works when you use the password generator from within a specific entry. Otherwise it will just create a new entry, with just your newly minted high-entropy password.
- Notes are great for keeping track of when you changed a password, why (data breach?), if you need to use an image to verify ("I used a soccer ball picture"), any restrictions on password length/character choice for an account ("14 characters max length, LAME!!"), or miscellaneous info that doesn't fit anywhere else.
- Making KeePass portable is easy. Download the ZIP version, unzip onto a USB stick, and put your DB/key on the device.
- TFA (Two-Factor Authentication) with the cloud; you can put your database in Dropbox, have the portable KeePass, and your key with you at all times.
- By default, KeePass will clear your clipboard after 12 seconds. You can change this, or disable entirely on the first screen in Tools -> Options
- I mentioned maybe needing to create the association of KDBX files earlier, this is in the Integration tab of Options; there you can change the Auto-type combo, if you so choose, among other options available.
- KeePass will lock automatically if you lock your computer, and will stay that way until you need it. Or, if KeeFox is installed, will remind you that it's locked.
- Favicons for easy identification of accounts (Gmail, Facebook, Amazon, Twitter, etc) are available for your use, just search for "[insert service] icon", download, and click the little key next to the Icon area.
- Using the "Expires" checkbox in an entry can remind you to change passwords at a pre-defined interval (6-, 12-, 18-month) should you decide you need / want to.

Joshua Dionne is an IT security enthusiast from Massachusetts that loves to tinker with technology.

**RSA CONFERENCE**
**EUROPE 2013**
29-31 OCTOBER | AMSTERDAM RAI

# Security in knowledge

Mastering data. Securing the world.

## Intensive information security.
## Essential intelligence in just three days.

Information security today isn't optional. It's business-critical. Over three days, RSA® Conference Europe 2013 imparts the must-know actions to manage growing cyber threats. With 70 sessions spanning 10 hours, attend the educational and networking event that builds your knowledge and furthers your career.

- Leave with actionable solutions
- Build your knowledge and skills
- Develop your professional contacts
- Stay informed, stay ahead

**(IN)SECURE subscribers receive an extra €100 off. Use discount code 56E3HELPND when you register.**

**Register by 27th September to save €300**

Hear how the world's security experts manage challenges like:

- **Bring-Your-Own Device**
- **Cloud security**
- **Mobile and tablets**
- **Big Data**
- **Data breaches**
- **Hacktivism**
- **Cybercrime**
- **Malware threats**

**Find out more at:**
www.rsaconference.com/help