About the Web Hacking Incident Database

The Web Hacking Incident Database (WHID) is a project dedicated to maintaining a list of publicly disclosed Web application-related security incidents. The purpose of the WHID is twofold: first, to serve as a tool for raising awareness of Web application security problems, and second, to aid risk-rating methodology processes by providing statistics of real-world Web application security incidents. Unlike other resources covering website security, which focus on the technical aspect of the incident, the WHID focuses on the impact of the attack. To be included in the WHID, an incident must be publicly reported, be associated with Web application security vulnerabilities and have an identified outcome. Trustwave's SpiderLabs (https://www.trustwave.com/spiderLabs-projects.php) is the WHID project sponsor. For further information about the WHID, refer to http://projects.webappsec.org/Web-Hacking-Incident-Database.

Related Research Work

There are numerous community projects such as Bugtraq (http://www.securityfocus.com/bid), XSSed (http://www.xssed.com/) and the Web Applications Security Consortium's (WASC) Statistics Project (http://projects.webappsec.org/Web-Application-Security-Statistics) which track Web application vulnerabilities, however, this represents only one dimension of the standard risk equation (RISK = THREAT x VULNERABILITY x IMPACT). Real-world, Web application breaches, on the other hand, provide us with additional information that enables research into actual trends in the hacking world, such as the types of organizations attacked, the motivation behind the attacks and the sources of the attacks.

Another project that collects information about real-world Web hacking incidents is Zone-H (http://www.zone-h.org/), which serves as the world's largest Web defacement mirror site. While Zone-H includes a large number of incidents, the majority of these are random hacks or crimes of opportunity rather than targeted attacks against a specific organization. By excluding random attacks, the WHID can provide a better tool for analyzing targeted, non-random attacks on websites.

The unique value in tracking targeted Web incidents is that it allows measuring the actual effect of the incidents, transferring research from the technology domain to the business impact domain. In order to manage risk, one needs to understand the potential business impact as opposed to technical failure. This makes the WHID the right tool for making business decisions concerning website security.
Only the Tip of the Iceberg

The criteria for the WHID are restrictive by definition, and the number of incidents that are included is not very large — only 222 incidents were included in the database for 2010. This is merely a sample of the overall Web application compromises that are actually occurring but are not publicly disclosed and/or reported on by media outlets. Therefore, the analysis in this document is based on relative percentage rather than absolute numbers.
Report Summary Findings

An analysis of 75 Web hacking incidents from the second half of 2010 conducted by Trustwave's SpiderLabs team shows the following trends and findings:

- A steep rise in attacks aimed at causing downtime – currently the new no. 1 outcome (up 21% from previous reporting period). This is mainly a result of ideological hacking efforts utilizing distributed denial of service (DDoS) attacks as part of the Anonymous Group versus Anti-Piracy and WikiLeaks events.
- Corresponding to downtime outcomes, denial of service attacks made the largest jump for Attack Methods to no. 1 (up 22% from the previous reporting period).
- Organizations have not properly implemented nor tested anti-automation defenses for their Web application architecture to ensure application availability during denial of service (DoS) attacks.

WHID Top 5 Web Application Risks

<table>
<thead>
<tr>
<th>Application Weakness (Example Attack Method)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Insufficient Anti-Automation (Denial of Service)</td>
</tr>
<tr>
<td>2. Improper Input Handling (SQL Injection)</td>
</tr>
<tr>
<td>3. Improper Output Handling (XSS, Planting of Malware)</td>
</tr>
<tr>
<td>4. Misconfiguration (Improper configuration and detailed error messages)</td>
</tr>
<tr>
<td>5. Insufficient Authentication (Stolen Credentials/Banking Trojans)</td>
</tr>
</tbody>
</table>

This report analyzes the 75 incidents on which information was collected from July to December 2010. For each incident, the WHID views attributes from many different angles:

- **Attack method** — The technical vulnerability exploited by the attacker to perform the hack.
- **Application weakness** — The underlying vulnerability within the application that is exploited.
- **Outcome** — The real-world result of the attack.
- **Vertical** — The field of operation of the organization that was attacked.

The report covers the following issues:

- The drivers, business or other, behind Web hacking.
- The vulnerabilities hackers exploit.
- The attack methods used.
- The types of organizations attacked most often.
What are the Drivers for Web Hacking (Outcome)?
The first question we confronted was: why do people hack? In the second half of 2010, downtime is the new no. 1 outcome, while defacements of websites are no. 2 and leakage of information is no. 3. It is important, however, to note that another major attacker goal is still to compromise websites in order to plant malware code to infect end clients.

2010 WHID Entries for Downtime Outcome
**Ideological Hacking**

Ideological hackers use the Internet to convey their message. While traditionally the main goal has been website defacement, this reporting period saw a huge surge in distributed DoS (DDoS) attacks aimed at taking websites offline.

There we two main drivers for these DDoS campaigns: anti-piracy enforcement sites and sites in support of or against WikiLeaks. In both cases, the organizing party behind the DDoS attacks is a group called Anonymous.

At first, Anonymous retaliated against websites that were enforcing anti-piracy/file-sharing laws in an assault labeled “Operation Payback.” Sites attacked and/or knocked offline include:

- Motion Picture Association of America (MPAA) – [www.mpaa.org](http://www.mpaa.org)
- Recording Industry Association of America (RIAA) – [www.riaa.com](http://www.riaa.com)
- Australian Federation Against Copyright Theft (AFACT) – [www.afact.org.au](http://www.afact.org.au)
- US Copyright Office – [www.copyright.gov](http://www.copyright.gov)

**WHID Example**


The second stage of the Anonymous attack was labeled “Operation Avenge Assange” and was a retaliation against any organization that was directly anti-WikiLeaks or negatively affected donation efforts. Sites attacked and/or knocked offline include:

- Amazon – [www.amazon.com](http://www.amazon.com)
- PayPal – [thepaypalblog.com](http://thepaypalblog.com) and [api.paypal.com:443](http://api.paypal.com:443)
- MasterCard – [www.mastercard.com](http://www.mastercard.com)
- Visa – [www.visa.com](http://www.visa.com)

**WHID Example**


**Hacking for Profit**

Professional criminals are continuing to use methods to generate revenue from compromising Web applications. Leakage of information is the no. 2 outcome for this report and is largely comprised of attackers extracting sensitive customer data from ecommerce websites. This data can then be sold on the underground blackmarket for identify theft purposes and fraud.

**WHID Example**

WHID 2010-147: Biggest blog company Skyblog hacked 32,000,000 accounts stolen ([http://datalossdb.org/incidents/2948](http://datalossdb.org/incidents/2948))

Planting of malware is a related outcome and is ranked at no. 4. By adding malicious code to the attacked websites, the attackers convert hacked websites to a primary method of exploiting client’s computers and installing the Banking Trojan software.

**WHID Example**

What Attack Methods do Hackers Use?

Cross-site scripting (XSS) has dominated other vulnerability research projects: XSS is the most common vulnerability found by penetration testers according to the WASC's Statistics Project (http://www.Webappsec.org/projects/statistics/) and is no. 2 in the OWASP Top 10 2010 release. While there is little debate that XSS vulnerabilities are rampant, the WHID focuses instead on monitoring actual security incidents and not vulnerabilities. Incidents are security breaches in which hackers actually exploited a vulnerable website, whereas vulnerabilities only report that a website could be exploited. Actual security breaches are more significant as they indicate both that a vulnerable website is exploitable and that hackers have an interest, financial or other, in exploiting it.

![Figure 2](https://media.blackhat.com/bh-dc-11/Brennan/BlackHat_DC_2011_Brennan_Denial_Service-Slides.pdf)

Figure 2 shows that the new no. 1 attack method is DoS, which makes up 32% of all attack methods. Application DoS attacks cause huge problems for websites, because there are many methods for rendering a Web application inaccessible rather than simply flooding the sites network connection with requests. These attacks often result in downtime for applications. Web applications are relatively fragile and attackers are able to send precise requests that target Web application resources requiring large processing power and thus may more easily consume the site’s available resources.

The main paradigm has shifted away from network bandwidth and now looks at local resources on the Web server platform itself. Traditional network level DoS attacks flood the network connection, while these application layer DoS attacks cause problems with local resources on the Web server or application. The bottom line is that the overall amount of traffic needed to potentially take down a website is much less than is required to flood the network pipe leading to the Web server.

To make these matters even worse, new DoS tools emerged to leverage the concept of “Slow HTTP Requests” against the application layer. Trustwave’s SpiderLabs presented on this concept at a recent Black Hat DC conference - https://media.blackhat.com/bh-dc-11/Brennan/BlackHat_DC_2011_Brennan_Denial_Service-Slides.pdf.
SQL Injection is no. 2 and XSS is no. 3 for known attack methods, which reinforces the vulnerability statistic reports from both WASC and OWASP listing these as top attack methods.

Which Types of Application Weaknesses are Exploited Most Often?
A new addition to the WHID in 2010 is the inclusion of tracking the underlying application weaknesses, which are exploited by the various attack methods. This is an important addition in that it sheds light upon the missing, misconfigured or broken application program coding practices that allow these attacks to be successful. This is an important metric to track so that developers may identify the root causes of application vulnerabilities and the various methods in which they may be abused. The weaknesses specified are taken from the WASC Threat Classification (http://projects.Webappsec.org/Threat-Classification).
Figure 3 lists the top application weaknesses identified in the second half of 2010. The top application weakness is insufficient anti-automation (at 36%) and is usually exploited during DoS attacks. Availability is a cornerstone of the CIA-triad (confidentiality, integrity and availability). However actually testing Web application defenses against DoS attacks is seldom included as part of a dynamic penetration test/assessment engagement. Unfortunately most organizations assume that their networking infrastructure will protect them from these types of attacks, and as this data shows, this is far from reality.

Improper Input Handling is currently no. 2 (at 23%) while Improper Output Handling came in at no. 3 (at 12%). These weaknesses map directly to the various attack methods listed previously. Here are some examples of this mapping:

- Attack -> Application Weakness
- DoS/Brute Force -> Insufficient Anti-automation
- SQL Injection -> Improper Input Handling
- XSS -> Improper Output Handling

It is important to note that there exists a many-to-one ratio with regards to attacks and weaknesses. There are many different types of attacks, which may leverage the same underlying application weakness. This means that, from a defensive perspective, it is possible to reap a very high mitigation return on investment (ROI) when organizations are able to address the root causes of vulnerabilities.

Which Types of Organizations are Attacked Most Often?

Another aspect we looked into is the types of organizations attackers choose as targets. The largest category of hacked organizations this reporting period are government sites, which remains no. 1 on the list (at 17%). This is mainly attributed to an increase in international “hacktivism,” which may include website defacements or DoS attacks.

Web 2.0 and entertainment sites are tied at no. 2 (at 15%) and political sites hold the no. 3 position (at 6%).
Vertical View: Government, Finance and Retail

Throughout 2010, Government, Finance and Retail verticals faced different, but equally important, outcomes. Attacks against Government agencies resulted in defacement in 26% of attacks, while Retail was most affected by credit card leakage at 27%. It is no surprise that Finance experienced monetary loss in 64% of attacks.

<table>
<thead>
<tr>
<th>Outcome</th>
<th>Attack Method</th>
<th>Application Weakness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government</td>
<td>Defacement (26%)</td>
<td>SQL Injection (24%)</td>
</tr>
<tr>
<td>Finance</td>
<td>Monetary Loss (64%)</td>
<td>Stolen Credentials (36%)</td>
</tr>
<tr>
<td>Retail</td>
<td>Credit Card Leakage (27%)</td>
<td>SQL Injection (27%)</td>
</tr>
</tbody>
</table>

For additional, real-time statistics for the year/vertical market pivot points, visit http://projects.webappsec.org/Web-Hacking-Incident-Database/#RealTimeStatistics.

Summary

The data presented within the report should be used to help organizations prioritize their remediation efforts with regards to Web application security, as these are the risks that are actively being exploited by cybercriminals.

About Trustwave

Trustwave is the leading provider of on-demand and subscription-based information security and payment card industry compliance management solutions to businesses and government entities throughout the world. For organizations faced with today's challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions and patented and award-winning technologies. Trustwave has helped thousands of organizations—ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers—manage compliance and secure their network infrastructure, data communications and critical information assets. Trustwave is headquartered in Chicago with offices throughout North America, South America, Europe, Africa, Asia and Australia.

For more information, visit https://www.trustwave.com.

About Trustwave's SpiderLabs

SpiderLabs is the advanced security team within Trustwave focused on incident response, ethical hacking and application security testing for our premier clients. The team has performed hundreds of forensic investigations, thousands of ethical hacking exercises and hundreds of application security tests globally. In addition, the SpiderLabs Research team provides intelligence through bleeding-edge research and proof of concept tool development to enhance Trustwave's products and services.

For more information, visit https://www.trustwave.com/spiderLabs.php.