

The Web
Hacking
Incidents
Database

2007

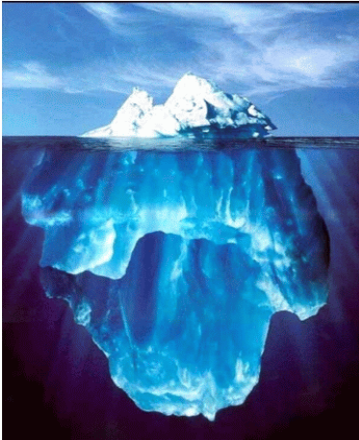
This report was prepared by:
Ofar Shezaf & the Breach Security Labs team

Annual
Report



ABOUT THE WEB HACKING INCIDENTS DATABASE

[The Web Hacking Incident Database](#) (WHID) is a [Web Application Security Consortium](#) project dedicated to maintaining a list of web application-related security incidents. The WHID's purpose is to serve as a community reference for raising awareness of the web application security problem and provide information for statistical analysis of Web security related 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 WHID an incident must be publicly reported, be associated with web application security vulnerabilities and have an identified outcome.

For further information about the Web Hacking Incidents Database refer to <http://www.webappsec.org/projects/whid/>.

RELATED RESEARCH WORK

Many projects such as [Bugtraq](#), [XSSed](#) and the [Web Applications Security Consortium's Statistics Project](#) track vulnerabilities in software or in web sites. However, vulnerabilities present only one dimension of the problem as they tend to be described in technical terms. Real-world incidents 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](#). While zone-h is more comprehensive and includes a large number of incidents, the majority of these are random hacks, something which shadows other types of attack. By excluding random attacks, WHID can provide a better tool for analyzing targeted non-random attacks on web sites.

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 WHID an invaluable resource for making business decisions concerning website security.

ONLY THE TIP OF THE ICEBERG

Since the criteria for inclusion of incidents in the WHID are restricting by definition, the number of incidents that are included is not very large - only 80 incidents made it to the database this year. Therefore the analysis in this document is based on relative percentage rather than on absolute numbers. We also significantly enhanced the database this year, and have not upgraded historical records to the same level, so year-over-year analysis is not yet available.

ABOUT THIS REPORT

The WHID has 237 entries of events occurring from 1999 until 2007. However, the inclusion criteria were changed in 2006 and additional attributes such as incident outcome and type of organization attacked were added in 2007. To date, only incidents for 2007 have been adjusted to the new criteria, so until the historical data is adjusted, year-over-year analysis is not possible. The current report, therefore, focuses on 2007 alone.

For each incident the WHID views attributes from many different angles:

- Attack Method – The technical vulnerability exploited by the attacker to perform the hack.
- Outcome – the real-world result of the attack.
- Country – the country in which the attacked web site (or owning organization) resides.
- Origin – the country from which the attack was launched.
- Vertical – the field of operation of the organization that was attacked.

The analysis in this paper is based on all of the above attributes, apart from origin and country. Information regarding the origin of attacks was too scarce for meaningful analysis. The contributors to the WHID tend to come more from English-speaking countries, presumably, because of the English-language interface of the WHID. This gives a leaning towards incidents in these countries rather than a world status.

In this report we try to cover the following issues:

- The drivers, business or other, behind Web hacking.
- The vulnerabilities hackers exploit.
- The types of organizations attacked most often.

WHAT ARE THE DRIVERS FOR WEB HACKING?

HACKING FOR PROFIT

The first question we confronted was *why do people hack?* It seems that the answers lie in very different areas of the spectrum. On the capitalistic side, an overwhelming number of incidents - more than 40% - are aimed at stealing personal information. Such 'personal records' are easily traded on the internet and therefore are the easiest virtual commodity to exchange for money.

Attack Goal	%
Stealing Sensitive Information	42%
Defacement	23%
Planting Malware	15%
Unknown	8%
Deceit	3%
Blackmail	3%
Link Spam	3%
Worm	1%
Phishing	1%
Information Warfare	1%

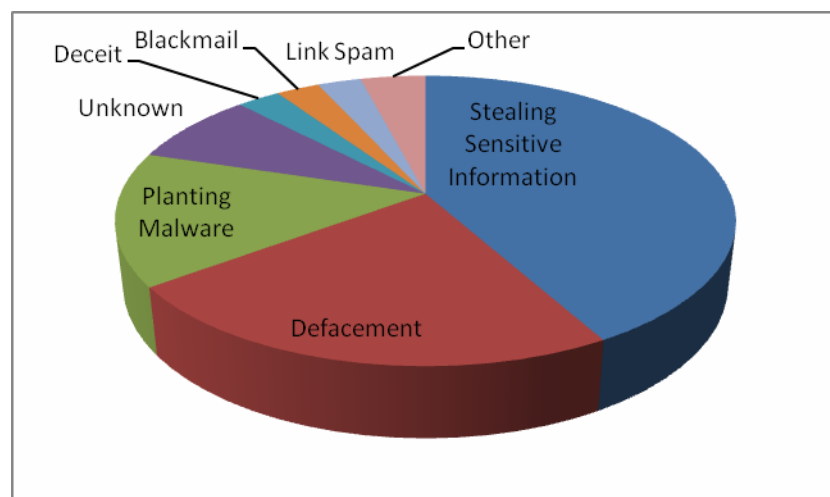


FIGURE 1 - INCIDENT BY OUTCOME

Two other ways in which crooks exploit web sites to gain money are the planting of malware and the adding of link spam to Web pages. The first demonstrates the role of web application hacks in the ever growing client security problem: by adding malicious code to the attacked web sites the attackers convert hacked web sites to a primary method of distributing viruses, Trojans and root kits. They are replacing e-mails as the preferred delivery method.

Link spam, a fast-rising threat, builds on the success of the "grey-hat" comment spam attack by adding links to pages. These links are meant to raise the popularity of the web site they point to and raise their position in search engines. But, unlike comment spam attacks that add links by posting spam comments, Link Spam, the "black-hat" version achieves this by changing pages on the attacked sites directly.

Together with blackmail, deceit and phishing the "for profit" attacks amount to 67% of all reported attacks.

To measure the actual damage caused by incidents we analyzed how many personal records were stolen in each incident. We found that, in the majority of incidents, a few thousand records were stolen.

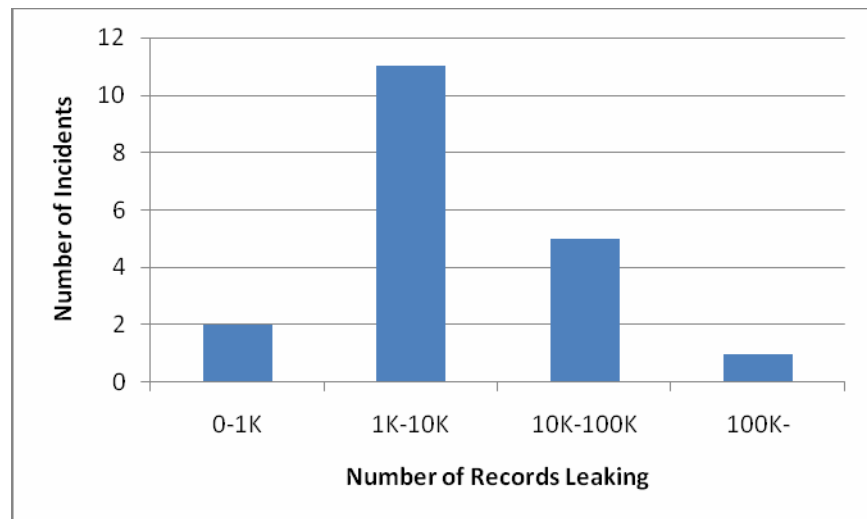


FIGURE 2 - NUMBER OF INCIDENTS BY NUMBER OF RECORDS LEAKING

IDEOLOGICAL HACKING

On the other end of the spectrum, the ideologists use the internet to convey their message using Web hacking. Their main vehicle is defacing web sites. When further analyzing defacement incidents, we found that 50% were of a political nature, targeting political parties, candidates and government departments, often with a very specific message related to a campaign. Others have a cultural aspect, mainly Islamic hackers defacing western web sites.

In order to concentrate on the impact of incidents, the WHID does not include most web site defacements, such as those covered by [zone-h](#), as they are random attacks with relatively low impact. We do, however, include defacement incidents that carry a greater significance. We consider an incident significant mainly based on *who* the victim was and, in some cases, *how* the attack was done. We also require the defacement to be reported publicly and not just by the hacker.

WHAT VULNERABILITIES DO HACKERS USE?

Cross Site Scripting (XSS) has dominated the WHID since its inception. This result is echoed in other research projects: XSS is the most common vulnerability found by pen testers according to the Web Application Security Consortium’s [Statistics Project](#) and tops the OWASP top 10 2007 release.

However, this year we focused our research by monitoring actual security incidents and not vulnerabilities. Incidents are security breaches in which hackers actually exploited a vulnerable web site whereas vulnerabilities only report that a web site could be exploited. Actual security breaches are more significant as they indicate both that a vulnerable web site is exploitable and that hackers have an interest, financial or other, in exploiting it.

Attack/Vulnerability Used	%
SQL Injection	20%
Unintentional Information Disclosure	17%
Known Vulnerability	15%
Cross Site Scripting (XSS)	12%
Insufficient Access Control	10%
Credential/Session Prediction	8%
OS Commanding	3%
Misconfiguration	3%
Insufficient Anti-automation	3%
Denial of Service	3%
Redirection	2%
Insufficient Session Expiration	2%
Cross Site Request Forgery (CSRF)	2%

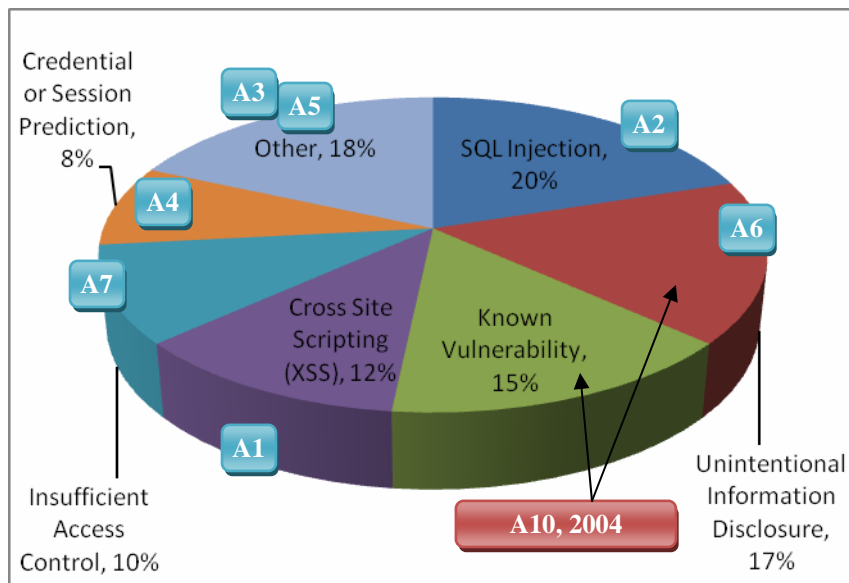


FIGURE 3 - INCIDENT BY ATTACK METHOD
 (“A” LABELS REFER TO THE OWASP TOP 10 POSITION)

When focusing on incidents rather than vulnerabilities, we found that SQL injection attacks top the list with 20% of the incidents. XSS attacks were only 4th with 12%. It seems that while it is easier to find XSS vulnerabilities as the vulnerability is reflected to the client, it is somewhat harder to take advantage of them.

It is interesting to note that nearly one third of the attacks abused operational mistakes rather than programming mistakes. Unintentionally publishing information online seems to be a huge problem which indicates that content management and maintenance procedures are not up to the standards required to maintain a secure site.

Another operational issue high on the list is known vulnerabilities. The broad exploit of known vulnerabilities suggests that regular patching is not performed in many web sites. This may be due to a lack of understanding of the importance of regular patching by system administrators. On the other hand, it might be reluctance to patch due to the operational risk and the time cost of patching, especially given the frequency of security patches in recent years. As a result it might be advisable to explore alternative patching strategies such as virtual patching which employs an external control to patch rather than requiring a software change.

While operational issues, which lost their position on the OWASP top 10, are widely exploited, some top OWASP top 10 vulnerabilities such as Cross Site Request Forgery (CSRF) and malicious file execution are not as widely exploited. Specifically, CSRF vulnerabilities are easy to detect and appear in many web sites are not yet widely exploited.

The table displayed above hides one important factor - the unknown. 29% percent of the incidents reported where reported without specifying the attack method. In many cases we feel that this lack of disclosure, apart from skewing statistics, prevents the fixing of the root cause of the problem. This is most noticeable in malware-planting incidents, in which the focus of the remediation process is removing the malware from the site rather than fixing the vulnerabilities that enabled attackers to gain access in the first place.

But probably the main lesson is that we know too little. With so little information about real-world attacks, threat modeling requires collecting information from many different sources, each providing a partial and perhaps even biased view.

WHICH TYPES OF ORGANIZATIONS ARE ATTACKED MOST OFTEN?

Another aspect we looked into is the type of organizations attackers choose as targets. We found out that the largest category of hacked organizations is government and related organizations. With education in second place, it appears that the non-commercial sector represents the primary target for hackers. Government is a prime target due to ideological reasons while universities are more open than other organizations. These statistics, however, are, to a degree, biased as the public disclosure requirements of government and other public organizations are much broader than those of commercial organizations.

Vertical	%
Government Departments	16%
Education	15%
Retail	12%
Media	12%
Service Providers	8%
Security & Law Enforcement	8%
Internet	8%
Technology	5%
Politics	5%
Finance	5%
Sports	3%
Health	3%

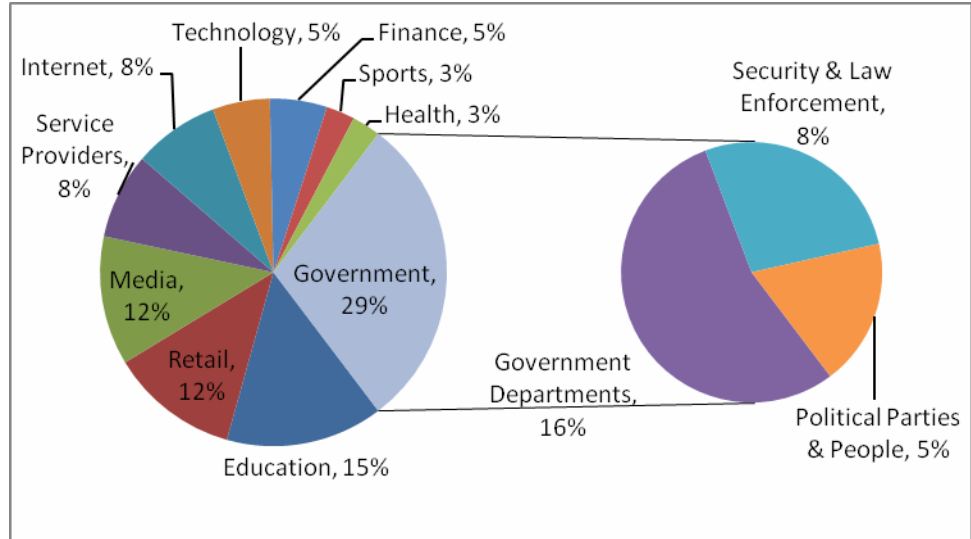


FIGURE 4 - INCIDENT BY ATTACK ORGANIZATION TYPE

On the commercial side, internet-related organizations top the list. This group includes retail shops, comprising mostly e-commerce sites, media companies and pure internet services such as search engines and service providers. It seems that these companies do not compensate for the higher exposure they incur, with the proper security procedures.

Financial institutes, on the other hand, are much lower on the list than one would expect. Two possible explanations are that they have better security measurements in place and that they disclose less.

SUMMARY

While financial gain is certainly a big driver for web hacking, ideological hacking cannot be ignored. Especially government and other non for profit organization suffer from ideological hacking. Internet related organizations, especially hosting providers, are suffering from more and more serious for profit hacking incidents. Financial organizations are either less vulnerable or disclose less.

As far as real-world hacking is concerned we are still at the basics. While researchers are exploring ever more advanced attacks such as CSRF, hackers are still successfully exploiting the most basic application layer vulnerabilities such as SQL injection or information left accidentally in the open.

While we have not seen a staggering increase in the number of reported attacks, we do see a clear and increasing trend upwards. We must also keep in mind that only the tip of the iceberg is reported.

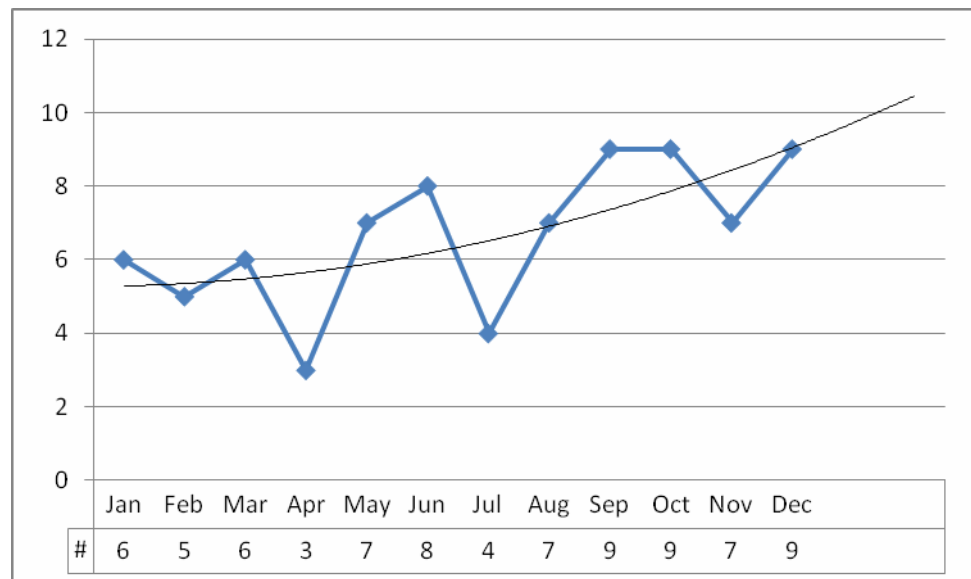


FIGURE 5 - 2007 INCIDENTS PER MONTH