HP 2012 Cyber Security Risk Report Overview

September 2013

Paras Shah

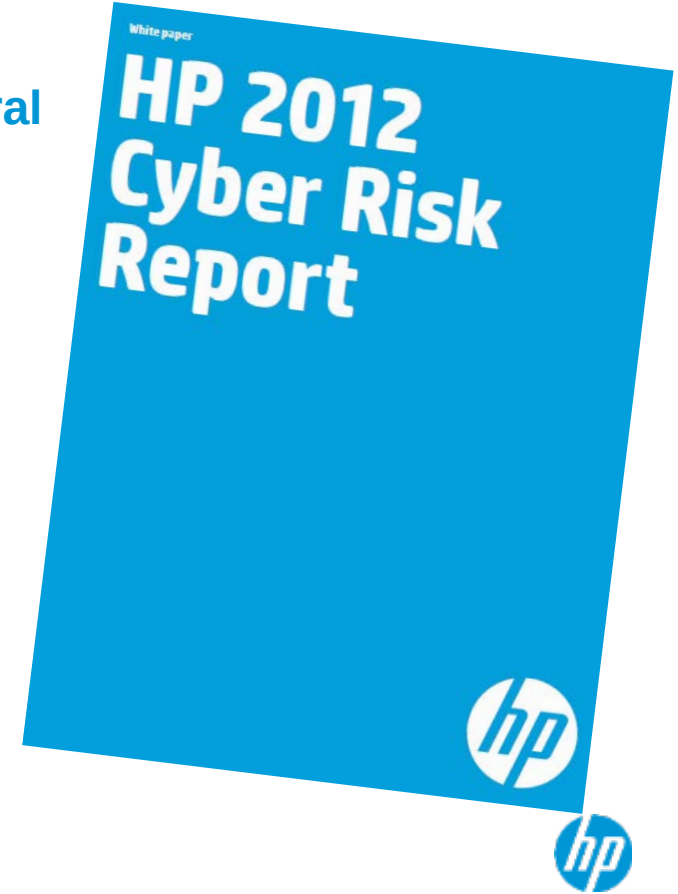
Software Security Assurance - Canada

Background

First published by DVLabs in 2009

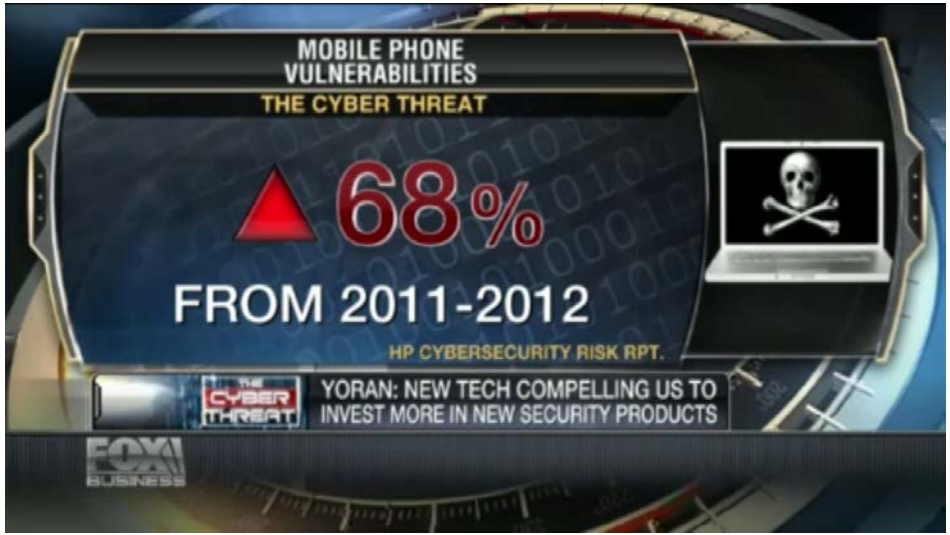
Has since grown to include contribution from several HP groups and third parties including:

- HP Fortify on Demand static and dynamic security testing data
- HP Fortify on Demand penetration testing analysis
- HP Fortify Software Security Research web vulnerability research
- HP DVLabs vulnerability and exploit analysis
- Open Source Vulnerability Database (OSVDB) data
- HP Zero Day Initiative (ZDI) vulnerability data



Goal is to help enterprises prioritize security resources

HP 2012 Cyber Security Risk Report Coverage



The Register®

USA TODAY

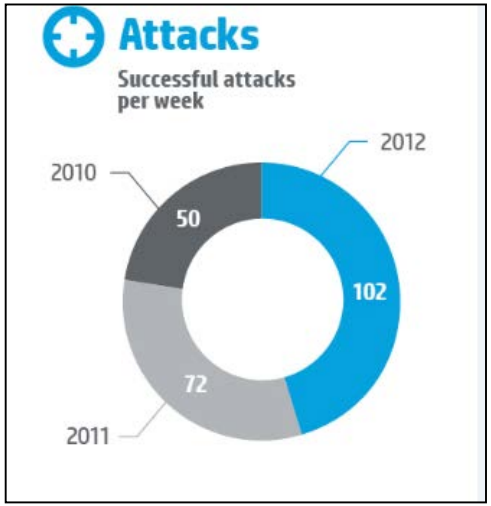
WebProNews

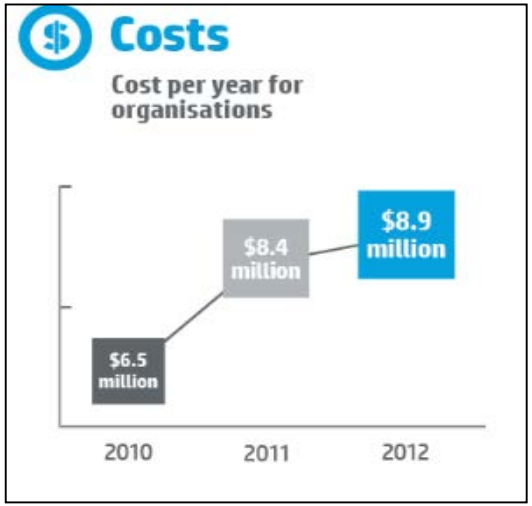
Focus Topics

- Vulnerability Trends
- Web Applications
- Mobile
- Conclusions

Vulnerability Trends

Growing Cost of Cyber-Crime (Ponemon)

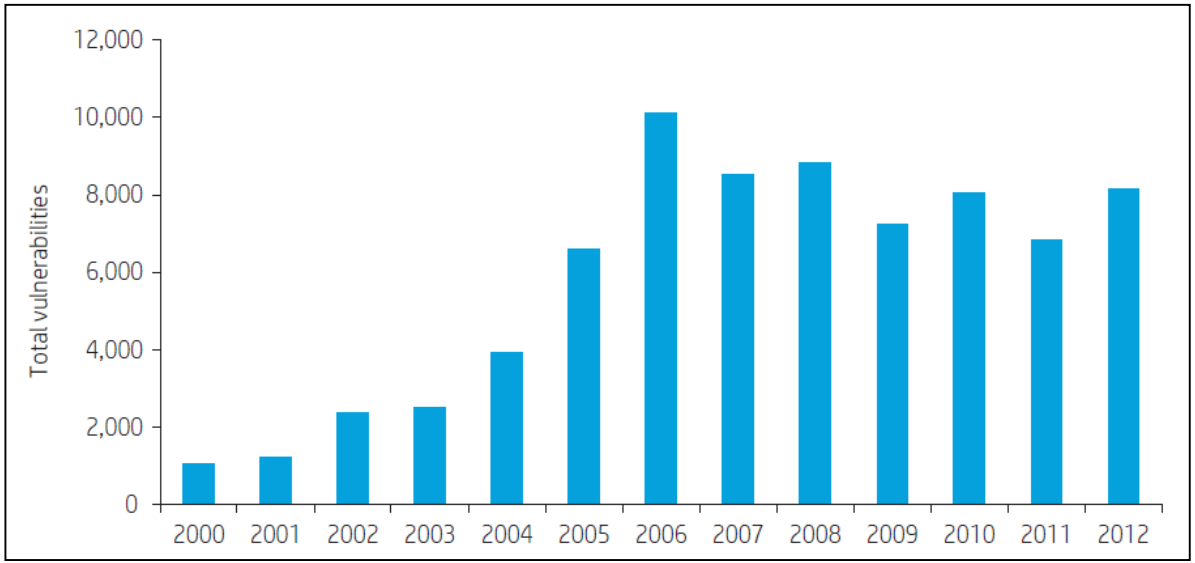




OSVDB Vulnerability Disclosures, 2000-12

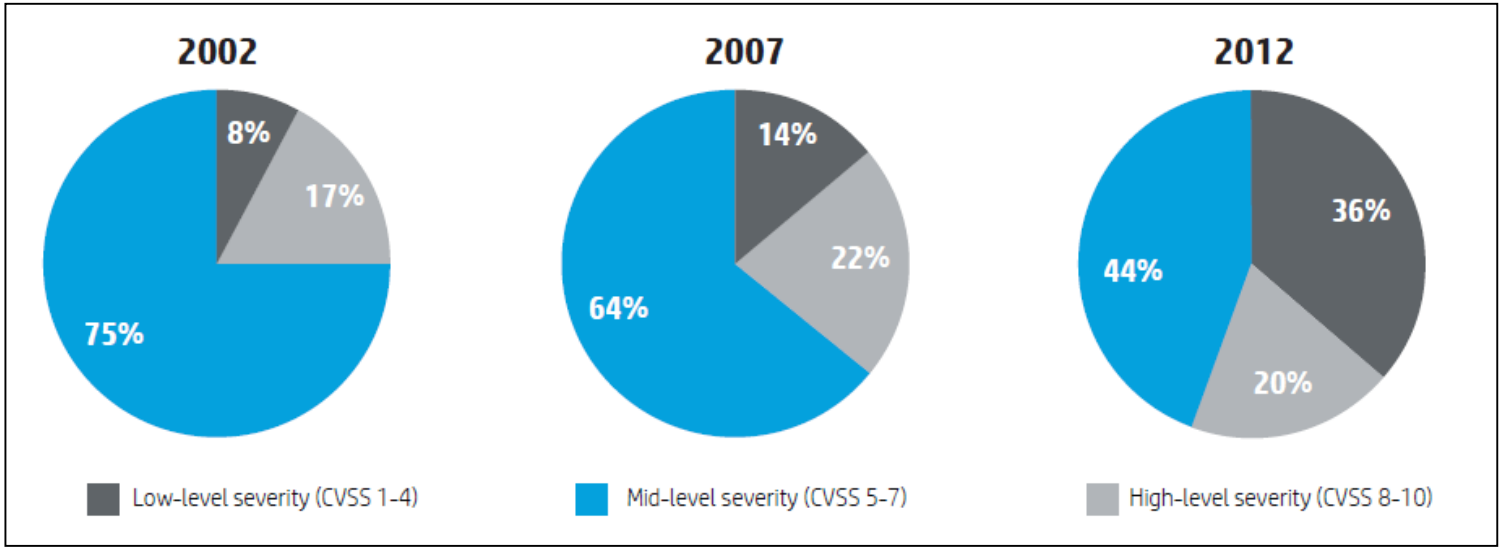
Total vulnerability disclosures grew 19% from 2011-12

However, 2012 disclosures remain 19% lower than the peak in 2006



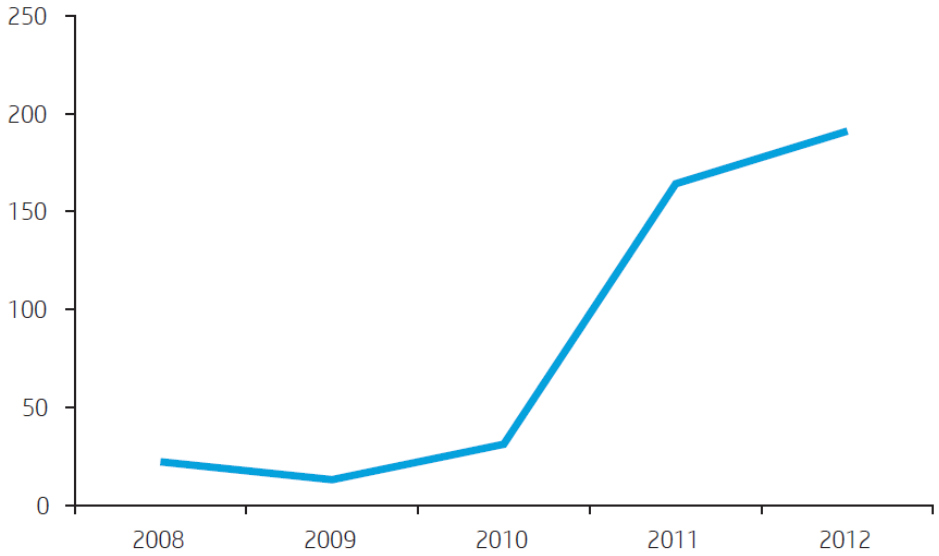
High Risk Vulnerability Disclosure

High risk vulnerabilities have also fluctuated…yet 1 in 5 in 2012 could still be leveraged to compromise a system



Mature technologies introduce continued and evolving risk

SCADA vulnerability disclosures, 2008-12



Vulnerabilities in SCADA systems rose 768% from only 22 in 2008 to 191 in 2012

Key Findings

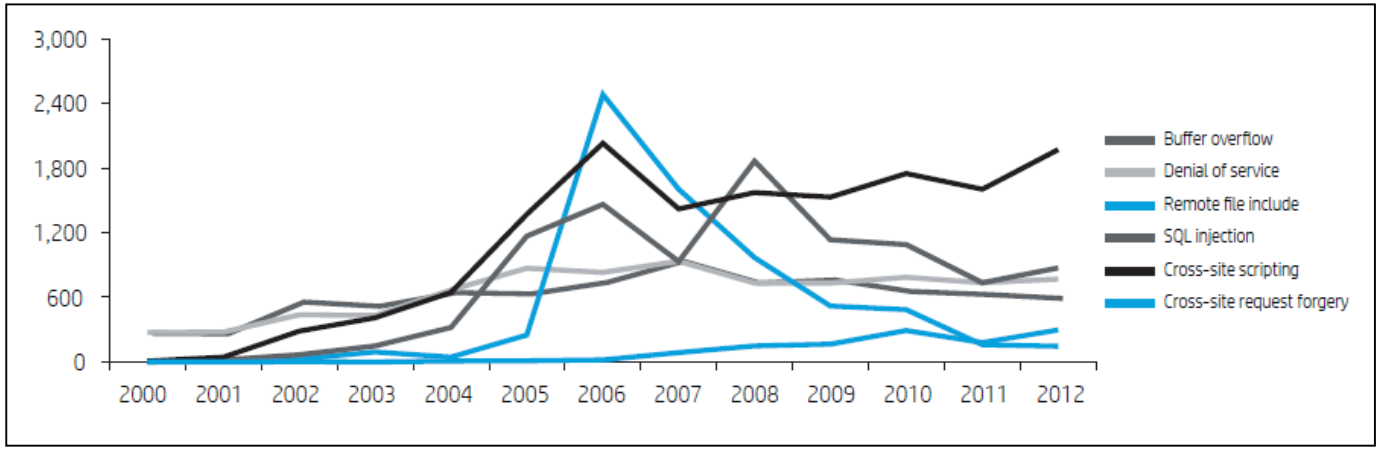
- **Security researchers must develop extensive expertise in specific systems to remain effective.**
- **Researchers receive a better return on investment for severe vulnerabilities that fetch a higher price.**
- **The security war rages on – with no clear victor yet in sight.**

Web Applications

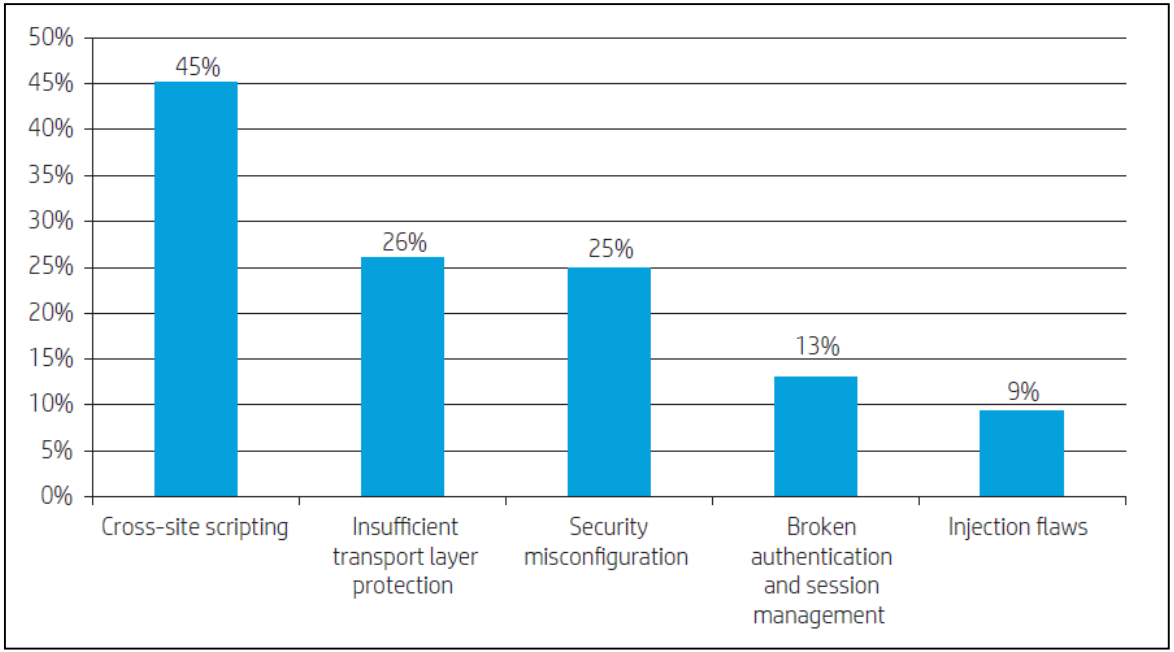
Web applications continue to introduce significant risk to organizations

4 web vulnerability categories made up 40% of 2012 disclosures

SQL Injection, Cross-Site Scripting, Cross-Site Request Forgery, Remote File Includes



Web Applications

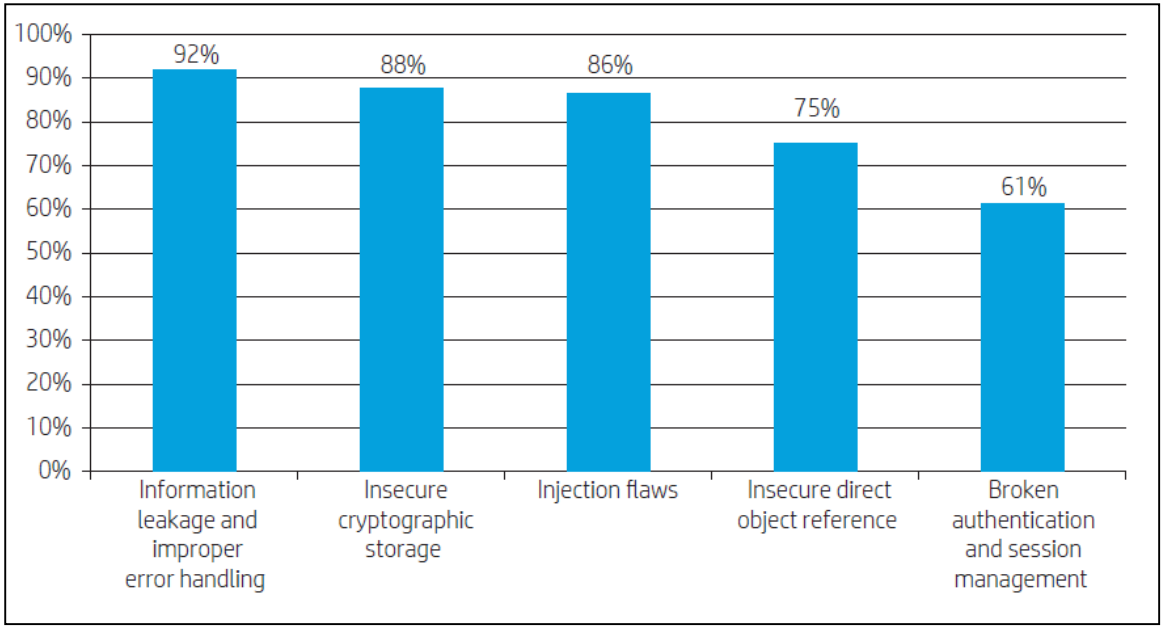


Dynamic Analysis Results

Testing of web applications exactly as an attacker would

No access to code

Web Applications

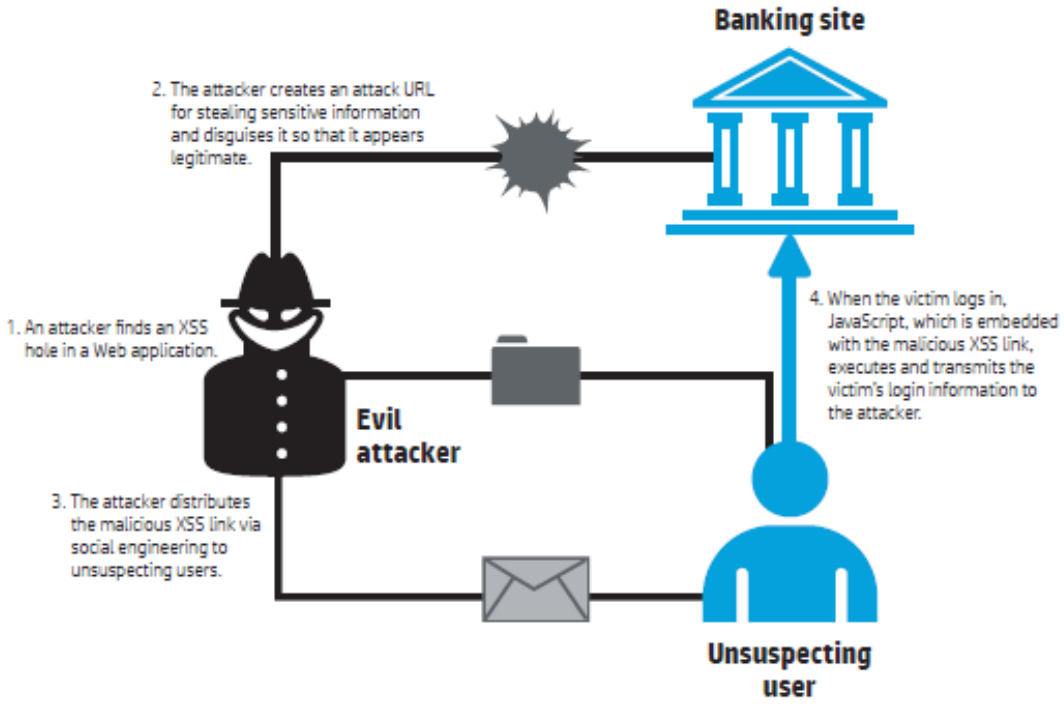


Static Analysis Results

Code level review

No access to the running application

Cross-Site Scripting



Nearly half of tested web applications were vulnerable to XSS in 2012

Cross-Site Scripting accounted for 15% of HP Zero Day Initiative (ZDI) vulnerability submissions in in 20212

Cross-Frame Scripting (XFS)

XFS can lead to click-jacking attacks, etc.

HPSR tested 100,000 URLs for the best XFS mitigation technique

Less than 1% of the sites accurately used the x-frames option header.

Vulnerability first described in 2002.

Web application risk: a case study

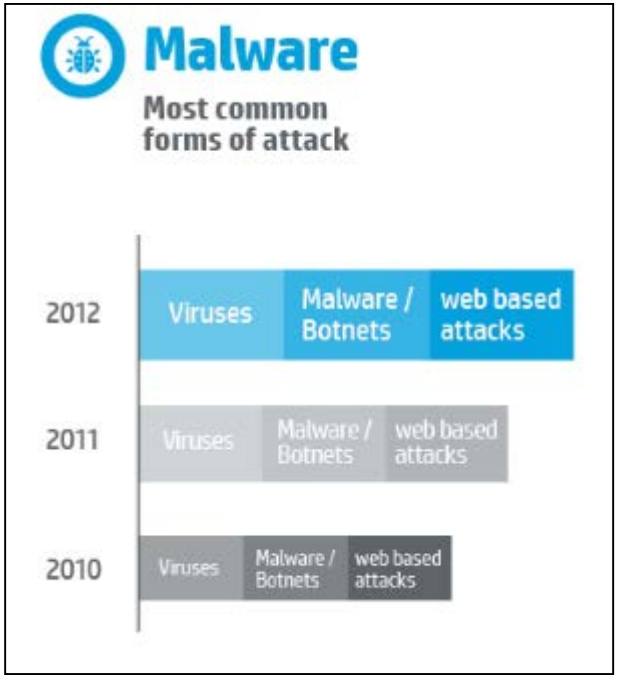
Company profile:

Large (more than 100,000 employees) multinational organization

Application Security program in place

- 54.1 percent of the assessments revealed persistent cookies.
- 48.32 percent of the sites were vulnerable to some form of cross-site scripting.
- 19.57 percent of the sites contained a “mixed-scheme” unencrypted login form where information from an HTTP page was posted to an HTTPS page or vice versa.
- 12.77 percent of the assessments were vulnerable to some form of SQL injection.
- 10.97 percent of the assessments confirmed blind SQL injection vulnerabilities.
- 19.7 percent of sites were vulnerable to logins sent over an unencrypted connection (no SSL).
- 5.26 percent of sites were susceptible to local file inclusion/read vulnerabilities.

Devastating Hacks

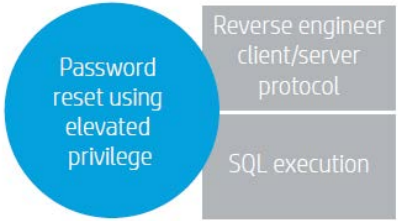


Devastating Hacks – Injection and Improper Input Validation

Industries: petrochemical, food processing, energy, and software

Unsafe file uploads:

Blind SQL Injection: Guided search functionality (a series of checkboxes designed to help consumers narrow down their search criteria) without input validation resulted in the exposure of 35 databases and database system user IDs and password hashes, including the system administrator account.



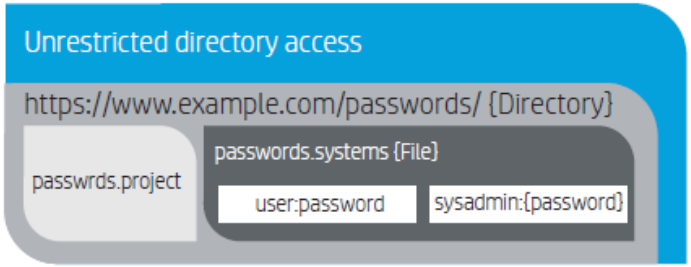
Cleartext SQL: The client was executing SQL statements directly to the back-end SQL server v
administrator-level permissions over HTTP. Via manipulation, privilege escalation and password modification was achieved.

Local file inclusion: Directory traversal and local file inclusion techniques were used to view the contents of the Web server's backup security accounts manager (SAM) file, which allowed the passwords to be cracked.

Devastating Hacks – Security Misconfigurations

Industries: petrochemical and international banking

Failure to restrict access to sensitive directories: In this case, the discov
directory was "https://www.example.com/passwords/".
Normally, this is a low level vulnerability, however…



WebDAV enabled allowing remote write: WebDAV was enabled on a particular Web server in a way that allowed remote application users to interact with the host and write files to arbitrary directories. A custom backdoor executable was written to a directory, then browsed to and executed.

SQL injection and weak input validation controls: A SQL filter was filtering everything but the "OR" operator.

SAP Misconfiguration: The entire credit card database was accessed and dumped to a file. The SAP implementation had poorly configured controls, allowing customer service representatives to run sensitive transactions, including the HR data browser. This capability was used to browse and load the entire contents of the customer credit card data table.

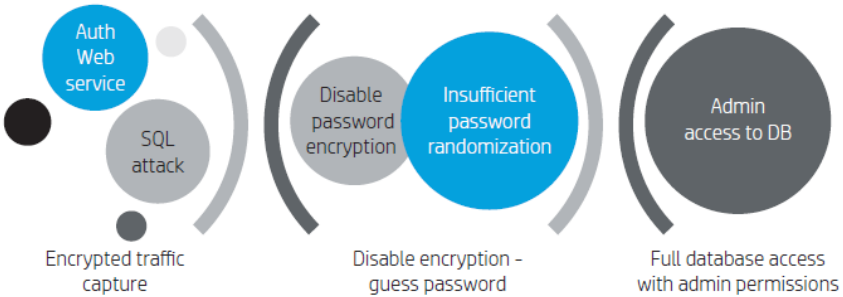
Devastating Hacks - Authentication, Session, Logic and Miscellaneous

Industries: airline, international banking, and energy

Enumeration of airline tickets through mobile QR code Web services: Testers were able to reverse engineer part of the Web service function to create ticket numbers. Fake ticket QR codes for airline flights were then generated.

Web service allowed direct SQL queries: An application allowed connections to its backend database via a Web-based interpreter that was accessible to the Internet without authentication.

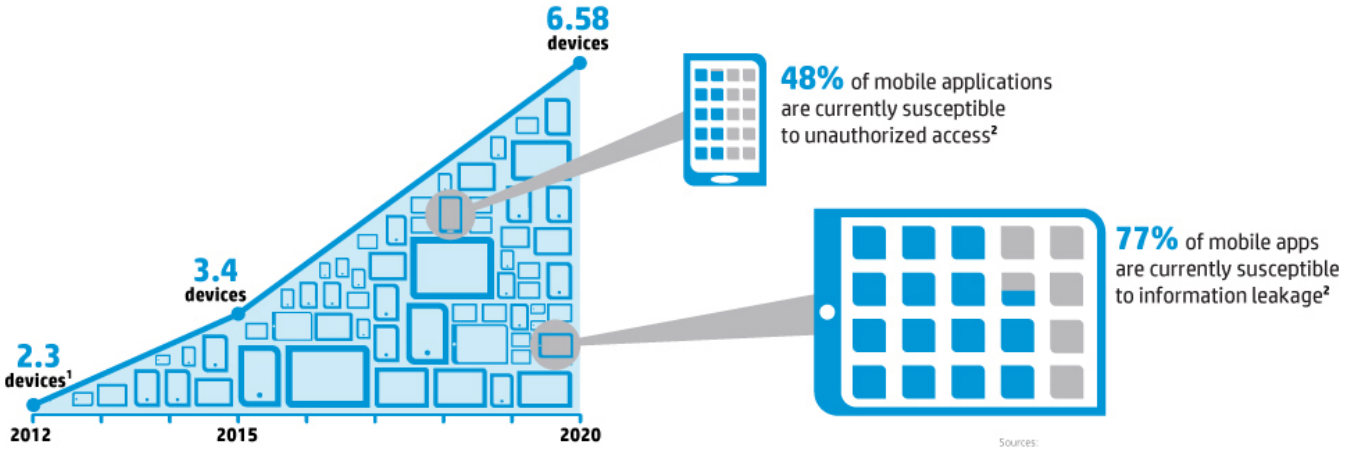
Easily reversible dynamic password generation: Although originally encrypted, SQL Injection was u to turn that flag off for passwords being requested from the db server. The system used dynamic passwords that changed frequently…however, after gathering multiple passwords, a time based pattern emerged and led to easily guessable passwords. Direct access to the database with administrative permissions was confirmed, allowing for complete compromise of the system.



Mobile

Growing number of employee devices a threat to enterprise security

Organizations are at the mercy of mobile applications and their persistent vulnerabilities

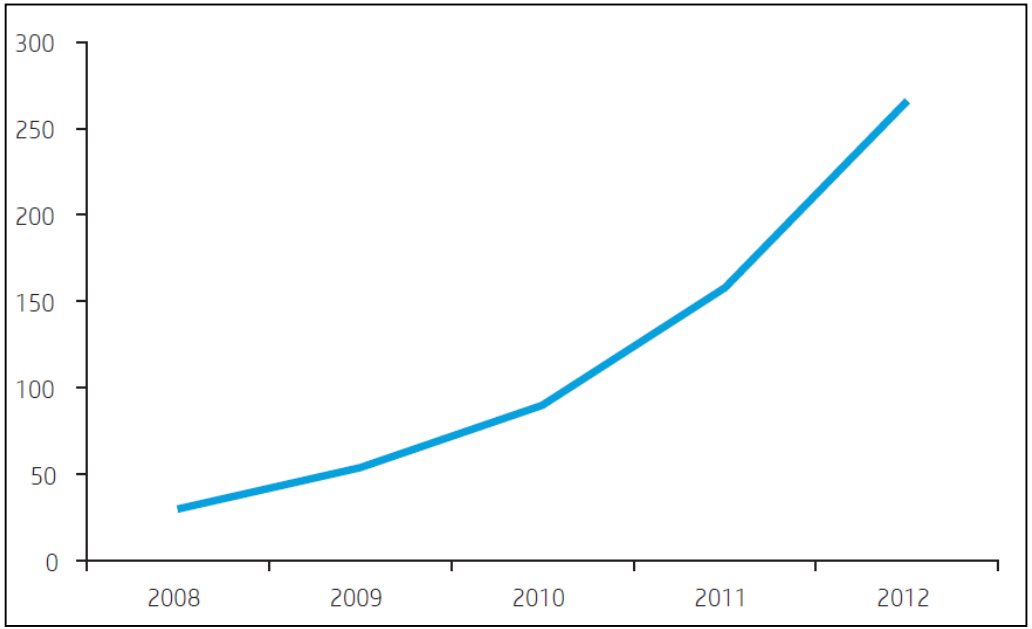


BYOD will only grow, with the number of devices per employee due to bypass 6 by 2020

Sources:
[1]Cisco Internet Business Solutions Group, "Internet of Things," July 2011
[2]HP, "2012 Cyber Risk Report," February 2013

Image Source:
www.enterprise2020.com

Mobile Vulnerabilities



Mobile vulnerabilities rose 68 percent from 158 in 2011 to 266 in 2012

Over the last five years, mobile vulnerability disclosure rose 787 percent

Mobile Vulnerabilities – by the numbers (round 1)

77 percent were vulnerable to Information Leakage

- A lot of this information was simple was simple, such as names, addresses, and phone numbers.
- However, this data also included the current location of the user, and the specific device identifier (aka the UDID).
- Also discovered login information, user credentials, session IDs, tokens, and sensitive company data all being sent over unencrypted network protocols like HTTP.

37.5 percent of the of the applications were susceptible to some form of authorization vulnerability

- This included cleartext passwords, hardcoded passwords, and passwords included as part of the response.
- Much higher percentage than in ‘normal’ applications.

13.5 were vulnerable to XSS

- Other mobile testing revealed a more consistent 33 percent were susceptible to XSS.
- While a lower percentage than expected, the affected applications were financial and database management applications.

Mobile Vulnerabilities – by the numbers (round 2)

48 percent of the applications were susceptible to unauthorized access vulnerabilities

- These validate the authentication vulnerabilities (37.5 percent) that we encountered in our earlier sample set.
- The numbers show that mobile developers need to concentrate on preventing unauthorized access to mobile applications as much as making them easy for legitimate users to access.

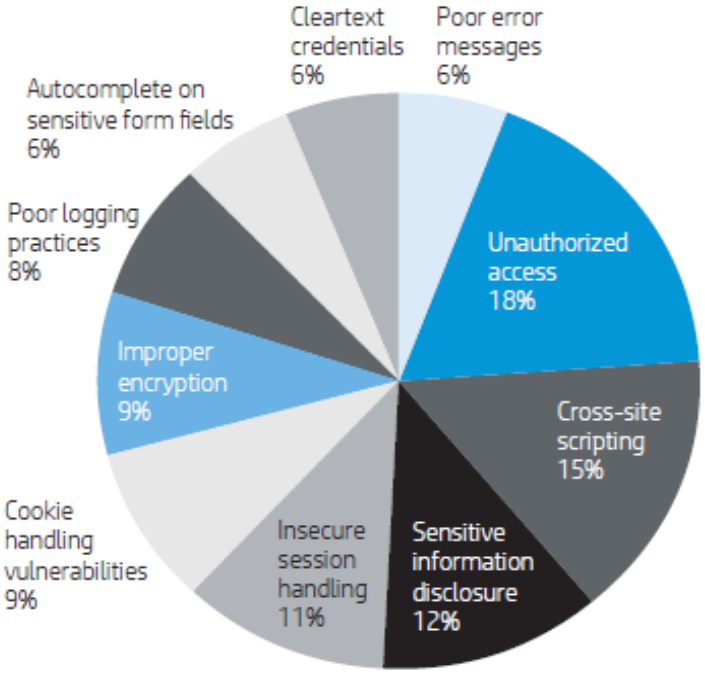
33 percent were susceptible to Cross-Site Scripting

- Consistent with our testing of normal applications.
- The same vulnerabilities that affect normal applications also affect their mobile counterparts.

26 percent of the applications employed improper encryption

- The same encryption standards applied against PCs are not yet being applied to mobile devices.
- In the age of BYOD, that's dangerous.

Mobile Applications – Vulnerability Prevalence



What vulnerabilities were found the most often by number?

Key Findings

- **The rise in usage of mobile devices has also come with a commensurate rise in application risk, especially as businesses try to capitalize on the advantages mobility provides.**

- **When coding mobile applications, developers are not considering the security implications of how they store, transmit and access data.**

- **The same security vulnerabilities that affect regular applications also affect mobile ones.**

Conclusions/Trends

Key Findings

- **While total vulnerability disclosures are on the rise, critical vulnerabilities are on the decline - but still pose a significant threat.**
- **Mobile platforms represent a major growth area for vulnerabilities.**
- **Web applications remain a very popular and viable attack vector.**
- **Developers and organizations alike have been slow to respond to long standing security issues, seriously compounding risk.**
- **Cross-site scripting remains a pervasive problem.**
- **Effective mitigation for cross-frame scripting remains noticeably absent.**
- **Mature technologies introduce continued risk.**

Conclusions/Trends

Mobile vulnerabilities will continue to rise

- The growth in adoption of mobile technology and its intersection with use in the enterprise will continue to introduce considerable risk.
- As BYOD becomes the enterprise norm, and the adoption of mobile devices continues to grow, expect the commensurate rise in mobile application vulnerabilities to continue unabated for the foreseeable future.

Vulnerability weaponization

- Attackers will continue to weaponize vulnerabilities to carry out their malicious agendas.
- Exploit kits will continue to focus on vulnerabilities in prevalent software, often targeting browsers and browser plug-ins, such as Oracle Java and Adobe® Flash.
- Crime organizations, nation states, and hacktivists will continue to use cyber attacks as a method of leveling the playing field against wealthy or powerful targets.

Conclusions/Trends

Web applications will remain vulnerable

- The lack of proper input sanitization in web applications, as well as the information “leaked” by them, shows that developers still have a long way to go to secure their applications properly.
- The high disclosure rate of XSS vulnerabilities coupled with its frequent appearance in testing gives us no reason to expect it to drop in popularity anytime soon.
- In the future, we expect more Injection type vulnerabilities, such as PHP injection, to continue to gain in popularity as the payoff of successful exploitation can be high.

Mature technologies, continued risk

- Attackers will continue to leverage existing and seemingly mature technologies to introduce enterprise risk.
- Securing the enterprise becomes that much harder when even mature technologies remain stubbornly vulnerable.

More Information…

HP Enterprise Security:
hp.com/go/SIRM

HP Security Research:
hp.com/go/HPSR

HP Fortify:
www.hp.com/go/fortify

HP Fortify on Demand:
http://bit.ly/15L7qax