

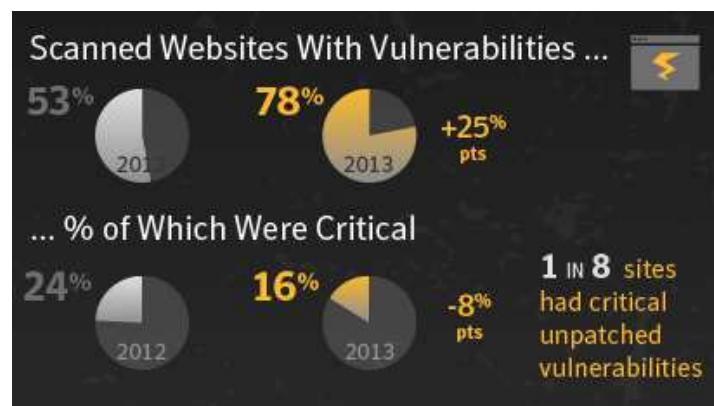


Application Security: To the future and beyond OWASP LATAM TOUR 2014

Fabio Cerullo
OWASP Global Board
CEO @ Cycubix Limited
fcerullo@cycubix.com



Software Threats



Software Threats

Zero-day Vulnerabilities

23 software vulnerabilities were zero-day, 5 of which were for Java

97% of attacks using exploits for vulnerabilities identified as zero-day were Java-based

14 2012 +64% 23 2013

Top-5 zero-day vulnerabilities

Vulnerability	Percentage
Oracle Java SE CVE-2013-1493	54%
Oracle Java Runtime Environment CVE-2013-2423	27%
Oracle Java Runtime Environment CVE-2013-0422	16%
Microsoft Internet Explorer CVE-2013-1347	1%
Microsoft Internet Explorer CVE-2013-3893	<1%

NUMBER OF ATTACKS DETECTED THOUSANDS

NUMBER OF DAYS AFTER VULNERABILITY PUBLICATION

3 Billion Devices Run Java

Computers, Printers, Routers, Cell Phones, BlackBerry, Kindle, Parking Meters, Public Transportation Passes, ATMs, Credit Cards, Home Security Systems, Cable Boxes, TVs...

DAY 0

ORACLE

19 days Total time of exposure for top 5 zero-days

4 days Average time to patch

cycubix Information Security

Software Threats

New Vulnerabilities

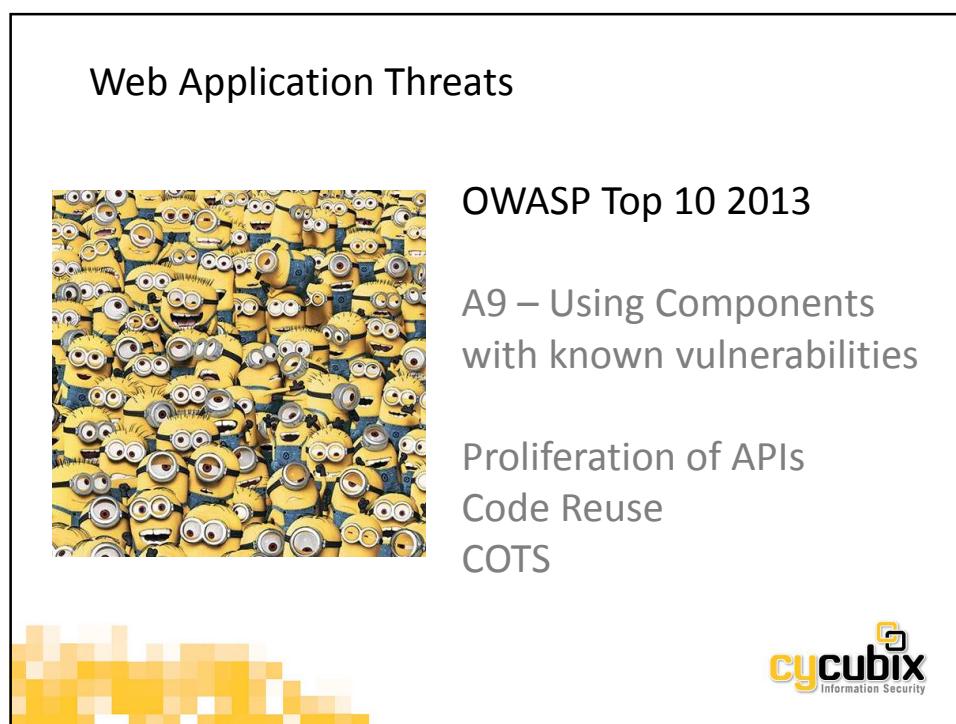
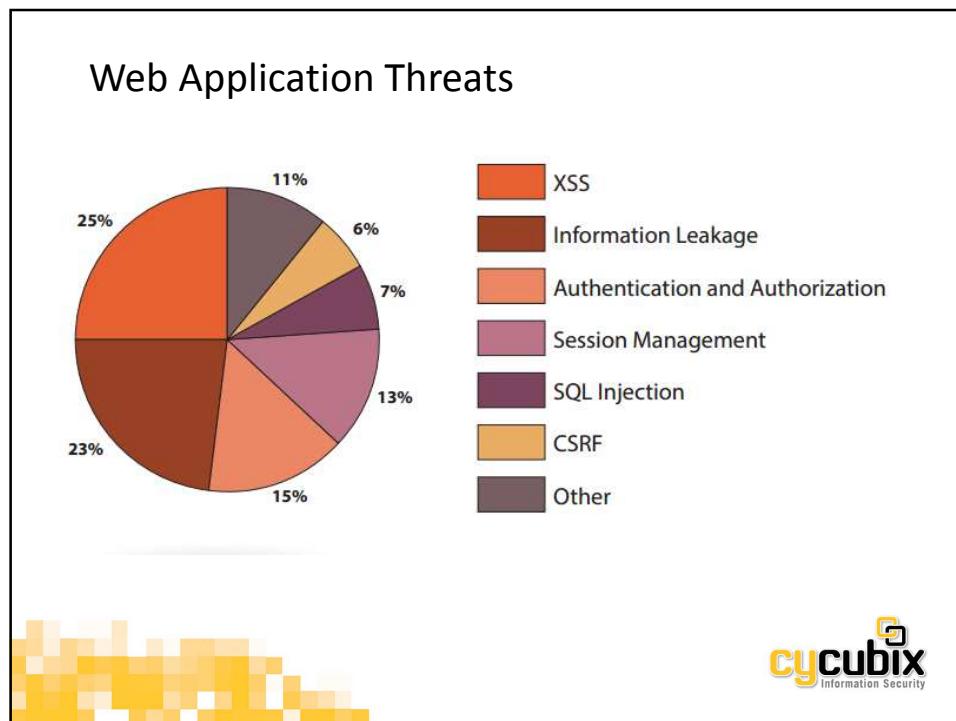
2013 6,787 +28% 2012 5,291

SSL and TLS protocol renegotiation vulnerabilities were most commonly exploited

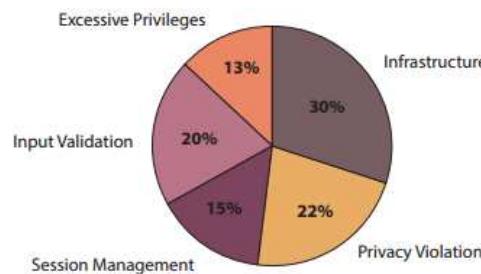



KEEP CALM AND
goto fail;

cycubix Information Security



Mobile Application Threats



2+ Million Apps combined



Mobile Application Threats



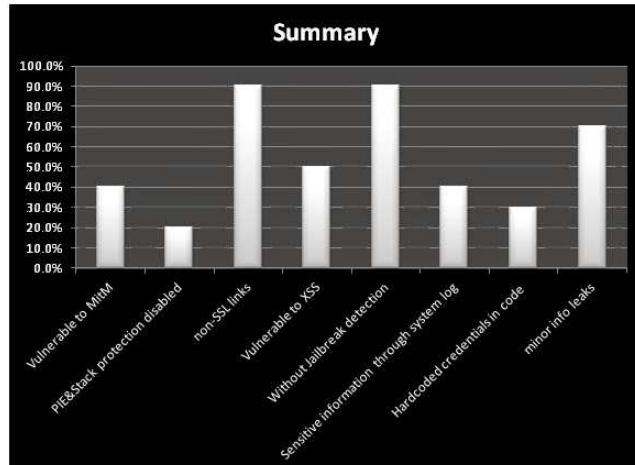
https://docs.google.com/file/d/0B3_TQgTE2uPcMkdBOExKNjh0N28/edit

Android WebView
Exploit, 70% Devices
Vulnerable (Feb
2014)

- Android 4.0-4.2
- Javascript
vulnerability
- Discovered 2012
- Google Glass
- Metasploit



Mobile Application Threats



iOS Mobile Banking Apps

- 40 apps sampled from major financial institutions.
- 90% contain vulnerabilities.
- New vectors of attack.



Mobile Application Threats



Tesla Model S API Authentication Flaws via Mobile App

- 6 chars password
- Token valid for 3 months
- No track of valid tokens
- Caching of token
- Storage of credentials



Embedded systems

[**Toyota Prius “Intelligent” park hack**](#)

[**Hacked Smart Refrigerators sending spam**](#)

[**Nissan Recalls Over 1M Cars for Air Bag Glitch**](#)



Recommendations

Developer Awareness

Risk Based approach

Security Testing & Code Review

Web Application Firewall/SIEM

Stringent Review of 3rd Party Apps/APIs

Mobile App Reverse-Engineering Protection



Thank you

Questions?



Sources:

[Symantec Internet Security Threat Report 2014](#)

[Cenzic Vulnerability Trends Report 2014](#)

[OWASP Mobile Security Project](#)



About Cycubix Limited:

Founded in 2011, Cycubix provides information security goods and services including:

- **Risk Management:** Identification, assessment and mitigation of information security risks. Implementation of risk metrics and supporting management information (e.g. risk dashboards).
- **Application Security:** Technical consultancy in the areas of penetration testing, secure code review and secure application development; assuring that IT application software and infrastructure are designed, implemented, and operated in accordance with applicable security standards and best practices (OWASP, SANS).
- **Security Assurance & Compliance:** Implementation and management of information security policies, processes and projects that adhere to industry standards such as ISO27001, PCI.
- **Security Training:** Delivery of trainings in various information security topics for technical and business audiences.

