Cigital's Top Web Application Security Vulnerabilities Compared to the OWASP Top 10

Joel Scambray, Cigital

Objectives

- Provide another dataset
- Test the “top n” hypothesis
- Discuss & learn
- (etc.)
- (etc.)
- Move infosec to a culture of data…?

Cigital

Our project

- Research performed by Koen Buyens, Senior Consultant
  - Initiated by Sammy Migues, Principal, BSIMM co-author
- Accumulated data from Cigital's Assessment Center (CAC) over >7 years
- Start simple: top n!
- Ask more sophisticated questions later

Cigital

Getting past “go”

Issues

- Data quality (normalization, typos, false positives…)
- Anonymity
- Qualified expertise (data vs security?)

Solutions

- Manual effort (now automated)
- Multi-party review
- Today, security; tomorrow, data science!

Cigital

Assessment Tools & Techniques

Approach

- Dynamic testing
- Web apps
- Authenticated
- Hybrid auto/manual
- IBM AppScan + others

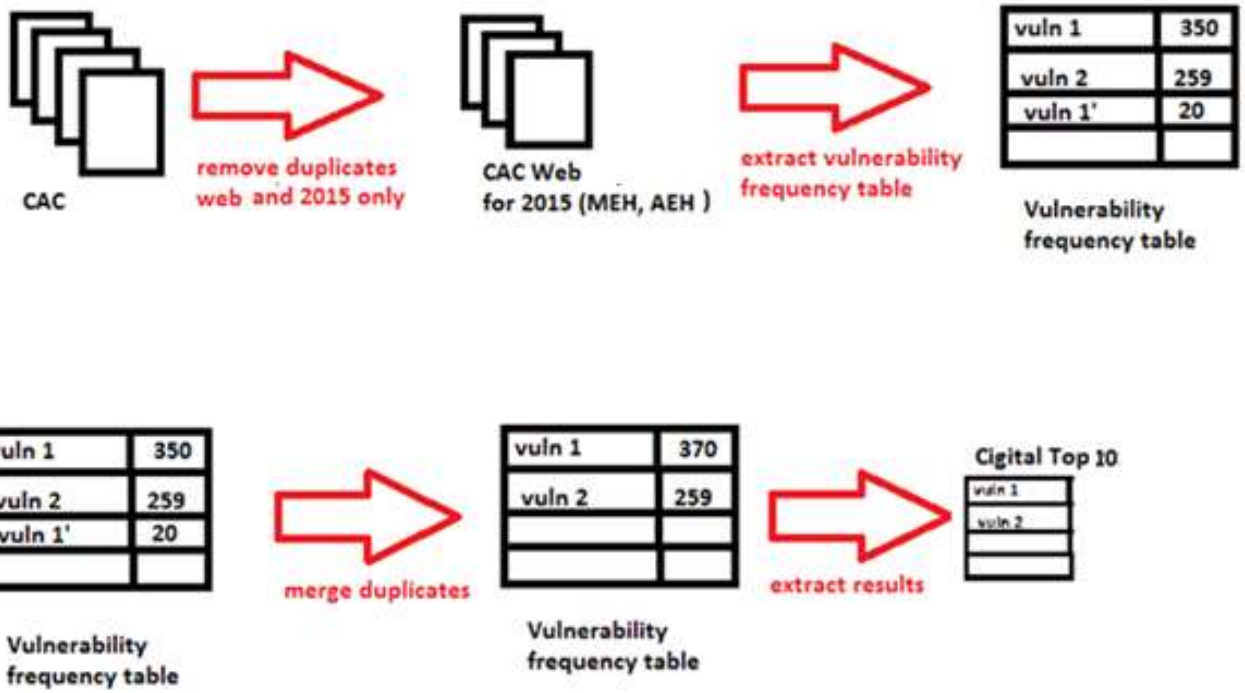
Code review and mobile now avail

Levels of Depth

- ***DSS (Dynamic Security Scan)*** manually crawl the target application and use the outcome to configure **IBM AppScan Standard Edition** with up to **1 user role**, then run an automated scan and manually reduces false-positives to produce a custom-written report.
- ***AEH (Automated Ethical Hack)*** includes the base DSS (above), but with up to **2 user roles**, as well as **some manual business logic testing** for prevalent mistakes (e.g. lack of server-side validation of business logic).
- ***MEH (Manual Ethical Hack)*** includes everything in a standard AEH, plus a **full manual penetration test of the application**, which identifies vulnerabilities that would not be typically identified using more automated approaches, or are related to complex/custom business logic.

Cigital

Methodology



Cigital

Results: The Cigital Top 20 Web Vulns

(CT20W)

1	Verbose server banner	8%
2	Weak SSL ciphers	6%
3	Hidden directory detected	6%
4	Clickjacking (aka UI Redressing)	5%
5	Weak password policy	5%
6	Secure cookie attribute not set	5%
7	Cacheable SSL pages	4%
8	SSL/TLS beast information leakage	4%
9	Username enumeration through password reset	3%
10	Reflected cross-site scripting (XSS)	3%
11	HttpOnly cookie attribute not set	3%
12	Verbose error messages	2%
13	Unencrypted viewstate	2%
14	Cross-site request forgery (CSRF)	2%
15	TLS/SSL not enforced	2%
16	Sensitive information leaked via query string parameter	2%
17	TLS/SSL not enabled	2%
18	Application error	2%
19	No account lockout policy	2%
20	Session identifier set prior to authentication	2%

Cigital

Comparison to OWASP Top 10

OWASP Top 10	Cigital Top 20 Web	Comparable OWASP Ref.
A1-Injection	Verbose server banner	A5-Security Misconfiguration
A2-Broken Authentication and Session Management	Weak SSL ciphers	A6-Sensitive Data Exposure
A3-Cross-Site Scripting (XSS)	Hidden directory detected	A4 Insecure Direct Object References
A4-Insecure Direct Object References	Clickjacking (aka UI Redressing)	(none)
A5-Security Misconfiguration	Weak password policy	A2-Broken Authentication and Session Management
A6-Sensitive Data Exposure	Secure cookie attribute not set	A6-Sensitive Data Exposure
A7-Missing Function Level Access Control	Cacheable SSL pages	A6-Sensitive Data Exposure
A8-Cross-Site Request Forgery (CSRF)	SSL/TLS beast information leakage	A6-Sensitive Data Exposure
A9-Using Components with Known Vulnerabilities	Username enumeration through password reset	A2-Broken Authentication and Session Management
A10-Unvalidated Redirects and Forwards	Reflected cross-site scripting (XSS)	A3-Cross-Site Scripting (XSS)

Cigital

The Next 10

Cigital 10-20	Comparable OWASP Ref.
HttpOnly cookie attribute not set	A6-Sensitive Data Exposure
Verbose error messages	A5-Security Misconfiguration
Unencrypted viewstate	A5-Security Misconfiguration
Cross-site request forgery (CSRF)	A8-Cross-Site Request Forgery (CSRF)
TLS/SSL not enforced	A6-Sensitive Data Exposure
Sensitive information leaked via query string parameter	A6-Sensitive Data Exposure
TLS/SSL not enabled	A6-Sensitive Data Exposure
application error	A5-Security Misconfiguration
No account lockout policy	A2-Broken Authentication and Session Management
Session identifier set prior to authentication	A2-Broken Authentication and Session Management

Cigital

You're going to need a bigger list

- Our 2015 list actually goes to 161 vulns
- Interesting stuff further down the list:
  - Unrestricted file upload #28
  - Client-side validation #63
  - Improper resource shutdown or release #71
  - Unsalted password hashes #156
- Do these matter to you?

Cigital

Observations

- Cigital identifies all 10, but frequencies differ
- A1, A7, A9, and A10 not in Cigital Top 20
- A1 - Injection not in CT20W; #42 >1% frequency
- A4 - Insecure direct object references is less frequent on CT20W (#97)
- Clickjacking on CT20W, but not OWASPT10

Cigital

Analysis

- Frequency deltas not surprising b/c different:
  - Data sources
  - 2015 vs ’13
  - App pool
  - Tools & techniques (code review?)
  - Depth/rigor, etc.
- Clickjacking – OWASP ack’d, https://goo.gl/dP9BzM
- Insecure direct object ref
  - Superset class of instances (e.g. vert/horiz priv escalation)
  - CAC labels instances, not class

Note:
CJ was
submitted…

Cigital

Why is injection so different? (#1 vs 42)

- (see previous)
- OWASPT10 is not pure frequency, but CT20W is
  - OWASPT10-2013 Methodology: https://goo.gl/jUvVji
- OWASPT10 includes dynamic and static, more frequently found?
- Cigital target apps have remediated injection?
  - Wipe out the class through developer training, enforcing re-usable libraries/code, “no ship” gates in the SDLC, high severity rating on found bugs, aggressive fix times, WAFs tuned…
  - Injection’s been around awhile…

Cigital

Data evolves

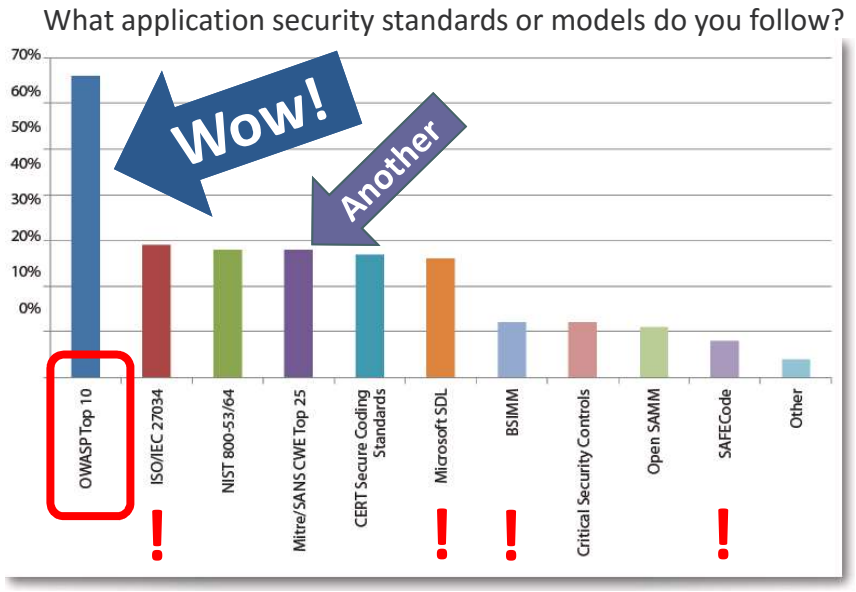
	Feb 2016		Mar 2016		Apr 2016		Jun 2016	
1	Verbose server banner *	8%	Weak SSL Ciphers	7%	DMC Using Regex (or WAF) to Filter Potential XSS	5%	Stored Cross-Site Scripting (XSS)	6%
2	Weak SSL ciphers	6%	Verbose Server Banner *	6%	Weak Password Policy	5%	Clickjacking (aka UI Redressing)	6%
3	Hidden directory detected	6%	Cacheable SSL Pages	5%	Weak Hashing Algorithm	5%	Database Error Pattern Found	4%
4	Clickjacking (aka UI Redressing)	5%	Clickjacking (aka UI Redressing)	5%	Verbose Error Messages	4%	Session Not Invalidated After Logout	4%
5	Weak password policy	5%	Hidden Directory Detected	4%	Clickjacking (aka UI Redressing)	4%	Unrestricted File Upload	4%
6	Secure cookie attribute not set	5%	Secure Cookie Attribute Not Set	4%	Microsoft IIS Missing Host Header Information Leakage	4%	TLS/SSL Not Enforced	4%
7	Cacheable SSL pages	4%	SSL/TLS BEAST	4%	Unprotected Transport of Credentials	4%	Vulnerable Software Version	3%
8	SSL/TLS beast information leakage	4%	Weak Password Policy	4%	Weak SSL Ciphers	3%	Privilege Escalation	3%
9	Username enumeration through password reset	3%	Reflected Cross-Site Scripting (XSS)	3%	Agent Upload Remote Code Execution	3%	Predictable Direct Object References	3%
10	Reflected cross-site scripting (XSS)	3%	HttpOnly Cookie Attribute Not Set	3%	Information Exposure Through an Error Message	3%	Server Path Disclosure Pattern Found	2%
11	HttpOnly cookie attribute not set	3%	Query String Parameter in SSL Request	2%	Help Pages Accessible To Unauthenticated Users	3%	Verbose Server Banner *	2%
12	Verbose error messages	2%	Cross-Site Request Forgery (CSRF)	2%	SQL Injection Lead	3%	F5 BIG-IP Cookie Information Disclosure	2%
13	Unencrypted viewstate	2%	SSL/TLS Client-Initiated Renegotiation	2%	Default Credentials	2%	Vulnerable Server Version	2%
14	Cross-site request forgery (CSRF)	2%	Verbose Error Messages	2%	Autocomplete HTML Attrib Not Disabled for Password Field	2%	Apache HttpOnly Cookie Information Disclosure	2%
15	TLS/SSL not enforced	2%	Username Enumeration through Password Reset	2%	Mail System Does Not Authenticate Trusted Sources	2%	SSL/TLS Client-Initiated Renegotiation	2%
16	Sensitive information leaked via query string parameter	2%	Autocomplete HTML Attrib Not Disabled for Sensitive Fields	2%	Failure to Sanitize Data into a Different Plane	2%	Hidden Directory Detected	1%
17	TLS/SSL not enabled	2%	Application Error	1%	MS12-073: Vulnerabilities in Microsoft IIS Info. Disclos.	2%	Username Enumeration through Forgot Password	1%
18	Application error	2%	No Account Lockout Policy	1%	Broadly Scoped Session Cookie Domain	1%	HTML5 Cross-Origin Resource Sharing	1%
19	No account lockout policy	2%	Excessive Session Timeout Duration	1%	Lack of Binary Obfuscation (Android)	1%	Weak SSL Ciphers	1%
20	Session identifier set prior to authentication	2%	TLS/SSL Not Enforced	1%	Server Path Disclosure Pattern Found	1%	Vertical Privilege Escalation	1%

Note: Incl. mobile, net, etc. ⇨

Cigital

How does this help?

Top n lists are popular…



SANS, https://goo.gl/XqpD1r

…but, reliable?

- Diverse data sources
- Methodology
- Freshness
- Tool/technique fitness
- Review/commentary
- "Keys under streetlamp"

Eg. OWASP Top 10-2013
https://goo.gl/jUvVji

Cigital

Conclusions

- “Top n” lists raise more questions than answer
- Stagnate if not updated periodically
- Sample your own data, compare to existing datasets (eg. CT20W and OWASPT10), adapt, refresh at regular intervals
- Use multiple assessment approaches incl dynamic/pen testing, code review/static analysis, threat modeling, and application-specific assessment methodologies such as mobile or embedded
- …and we’ll keep doing more research!

Cigital

Cigital's Top Web Application Security Vulnerabilities Compared to the OWASP Top 10

Joel Scambray

Cigital, Inc.

jscambray at cigital.com

@joelscam