400 Apps in 40 Days

A discussion of prioritization in application security assessments

Nish Bhalla, Security Compass
Sahba Kazerooni, Security Compass
Introductions

Nish Bhalla
Founder

Direct: 1-888-777-2211 Ext. 101
Mobile: 732-614-1020
E-mail: nish@securitycompass.com
Web: http://www.securitycompass.com

Toronto, Canada | Shrewsbury, USA
Introductions

Sahba Kazerooni
Principal Consultant

Direct: 1-888-777-2211 Ext. 103
Mobile: 732-778-9342
E-mail: sahba@securitycompass.com
Web: http://www.securitycompass.com

Toronto, Canada | Shrewsbury, USA
✓ The focus is on web applications
✓ The approach described here is only ONE approach
✓ Your feedback and participation are encouraged!
The Scenario
“Reduce the risk from all external facing applications”
1700 Domains
40 Days
Resources

1. Just Jim
2. One license for industry-standard web app scanning tool
Challenges

Time
Challenges

Most bang for your buck
Do we care about:

- Static websites? Yes
- Unauthenticated websites? Yes
- Sites that forward to others? Yes
- HTTP vs HTTPS? Yes!
But Wait!

• Some domains are duplicate
• Some are not hosting any applications
• Some are not operated by our organization

➢ Leaves us with 400 domains
Assessment Options
Would you rather know nothing about everything or everything about nothing?
Application Classification

Development Policy 154A – Applies to all applications with Medium or higher Availability:
Ensure that all fatal exceptions are logged to a debugging log to facilitate trouble shooting
Challenges

- 400 apps = 40 days classifying apps
- Coordinating with app owners and admins
- Does anyone know which data and sensitivity levels?
Just Scan Everything?
A Case Study
So we did some of this...
A Lot of this....
Thought about this....
And this....
And came up with this:
Scan the server

- Hidden files and directories
- Information disclosure
- Some known vulnerabilities
- HTTP Config
Scan the app unauth

- XSS (reflective)
- SQL Injection
- Non-SSL forms
- Session management
- Open redirects
Scan the app unauth

- NOT Privilege escalation
- NOT Password complexity (unless obvious)
- NOT Stored XSS
- NOT Business logic flaws
Assess Login forms

- SQL Injection
- User enumeration (if possible)
- Forgot password implementation
Flag sites of interest

- Based on finding count and severity
- Based on systemic issues
The Results
415 Findings
Means we can only do 4 apps

4 apps x 10 findings/app

Estimated 40 findings

Average 10 days per app

Average 10 findings

400 apps

40 days

415 Findings

Thorough Assessment

Unauth. Assessment
SQL Injection: 15
XSS: 35
Remote Command Execution: 2
Arbitrary File Download: 1
Non-SSL Password: 6
Weak Authentication: 19

+ 337 others
Lessons Learned

Can’t rely on automated tools
Lessons Learned

Know your exposures and liabilities
Lessons Learned

Application security policies go a long way
Lessons Learned

No time to investigate – assume the worst
Thank you! Any Questions?