



DISA's Application Security and Development STIG: How OWASP Can Help You

Jason Li
Senior Application Security Engineer
jason.li@aspectsecurity.com



AppSec DC
November 12, 2009

The OWASP Foundation
<http://www.owasp.org>

About Me

- Senior Application Security Engineer
 - ▶ Five different organizations
 - ▶ 12 applications validated against ASD STIG this year
 - ▶ CAT I's in almost all of them!



- OWASP Global Projects Committee member
- Star Trek Fan
- Ballroom Dancer

About DISA

- Defense Information Systems Agency
- Part of the Department of Defense
- Administers and protects DoD command and control systems and enterprise infrastructure



About DISA STIGs

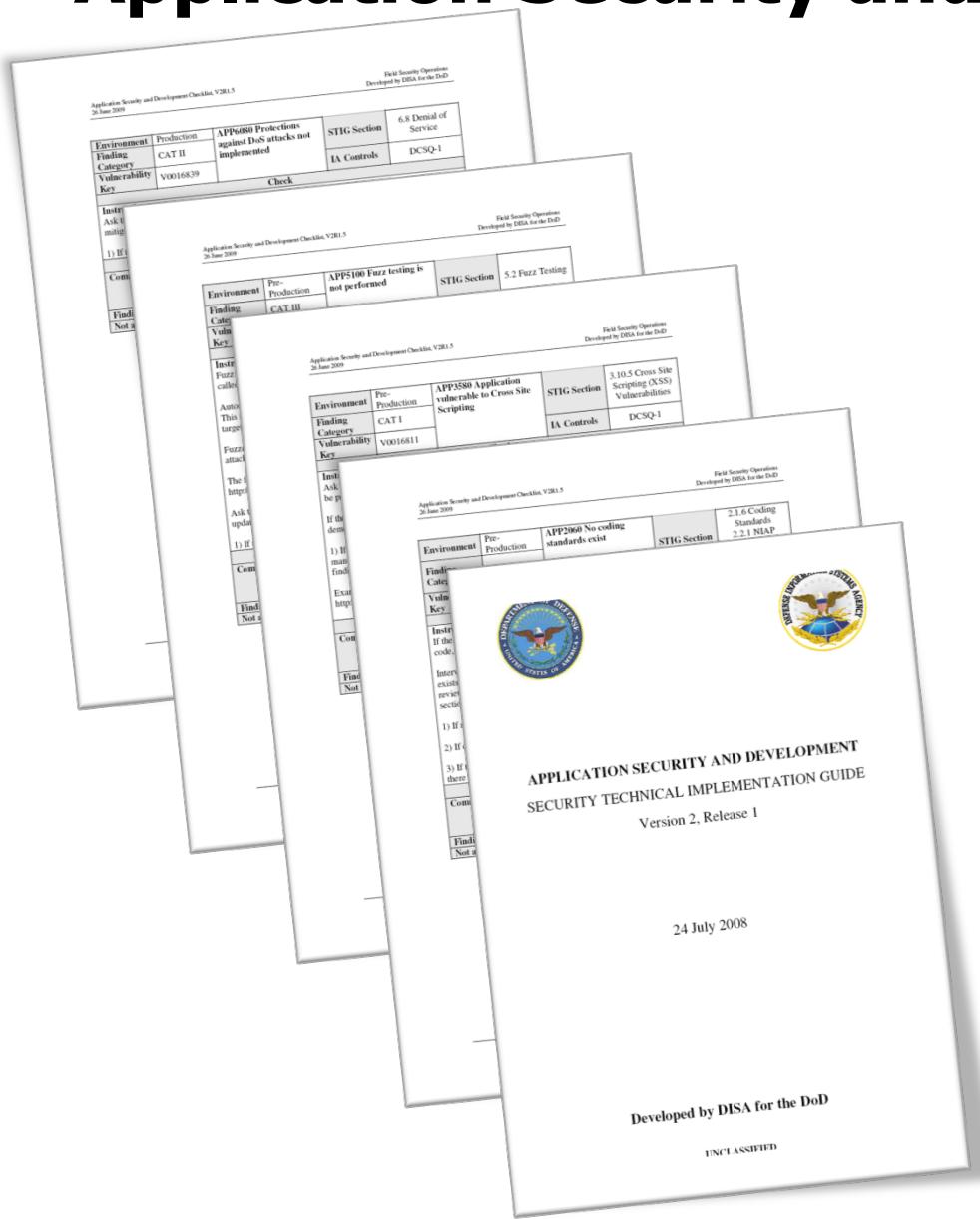
- Offers configuration guides and checklists for:

- ▶ Databases
- ▶ Operating Systems
- ▶ Web Servers
- ▶ Etc...

- Provides standard “findings” and impact ratings
 - ▶ CAT I, CAT II, CAT III

Information Assurance Support Environment Your One-stop-Shop for Information		
IA News What's New Consent Notice		
Security Technical Implementation Guides		
Security Checklists SRRs STIGs STIG Home Page Whitepapers		
DoD General Purpose STIG, Checklist, and Tool Compilation CD		
Documents	Date	Size
Application Security and Development STIG Version 2, Release 1	July 24, 2008	947KB
Access Control STIG V2R2	Dec 18, 2008	947KB
Application Services STIG V1R1	Jan 17, 2006	298KB
Citrix XenApp Memo	Jul 23, 2009	198KB
Citrix XenApp STIG V1R1	Jul 23, 2009	2070KB
Database STIG V8R1	Sep 19, 2007	557KB
Desktop Application STIG V3R1 .doc/.pdf	Mar 9, 2007	950KB/430KB
Defense Switched Network (DSN) STIG V2R3	Apr 30, 2006	797KB
Directory Services STIG V1R1 .doc/.pdf	Aug 24, 2007	1,719KB/709KB
DISA Instruction Enclave STIG - Currently unavailable	N/A	N/A
Domain Name System (DNS) STIG V4R1	Oct 17, 2007	913KB
Enclave STIG V4R2	Mar 10, 2008	939KB
ERP STIG V1R1	Dec 7, 2006	266KB
ESM STIG V1R1	Jun 5, 2006	1,076KB
ESX Server Memo	Apr 22, 2008	212KB
ESX Server STIG Version 1, Release 1.0	Apr 28, 2008	1,388KB
Instant Messaging STIG Version 1, Release 2 (.pdf)	Feb 15, 2008	1,353KB
Instant Messaging STIG Version 1, Release 2 (.zip)	Feb 15, 2008	4,104 KB
Microsoft Exchange 2003 STIG V1R1 - New! posted Sept 17, 2009	Aug 6, 2009	5,560 KB
Microsoft Exchange 2003 Memo - New! posted Sept 17, 2009	Aug 6, 2009	169 KB
Microsoft Windows Server 2008 Guidance Memo	Jan 21, 2009	166 KB
Network STIG V7R1	Oct 25, 2007	2,059KB

Application Security and Development STIG



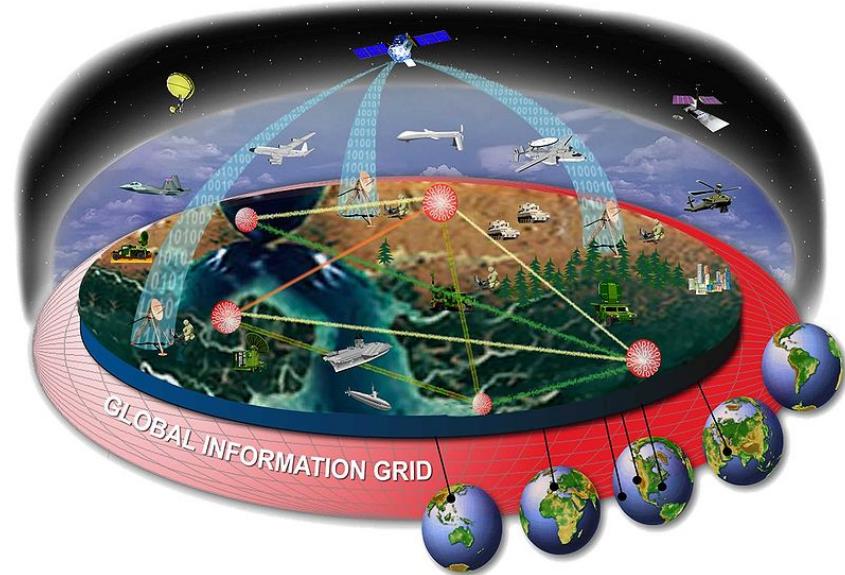
- First draft November 2006; first release July 2008

- 129 requirements covering:

- ▶ Program Management
- ▶ Design & Development
- ▶ Software Configuration Management
- ▶ Testing
- ▶ Deployment

Application Security and Development STIG

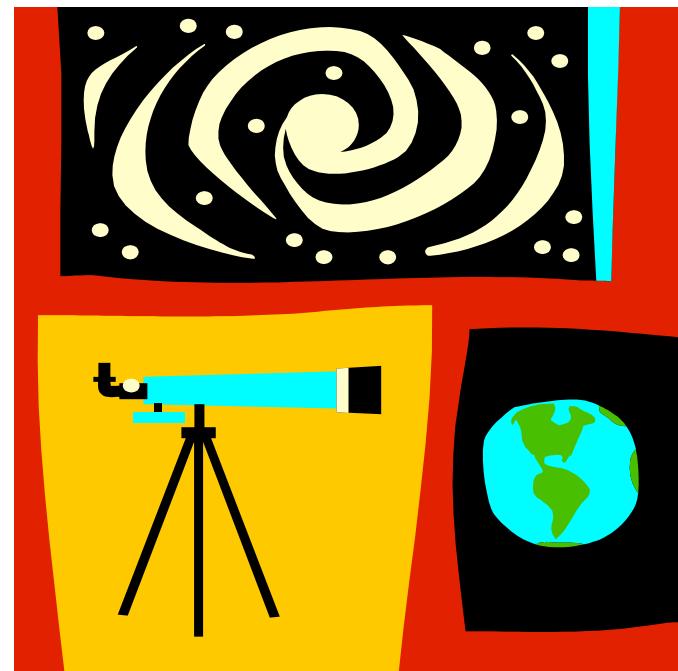
- ASD STIG applies to
“all DoD developed, architected, and administered applications and systems connected to DoD networks”
- Essentially anything plugged into DoD



Application Security and Development STIG

■ Requirements can be extremely broad:

- ▶ e.g. APP3510: The Designer will ensure the application validates all user input
- ▶ e.g. APP3540: The Designer will ensure the application is not vulnerable to SQL Injection



Application Security and Development STIG



■ Requirements can be extremely specific:

- ▶ e.g. APP3390: The Designer will ensure users accounts are locked after three consecutive unsuccessful logon attempts within one hour

Application Security and Development STIG

- Requirements can be esoteric:

- ▶ e.g. APP3150: The Designer will ensure the application uses FIPS 140-2 validated cryptographic modules to implement encryption, key exchange, digital signature, and hash functionality



Application Security and Development STIG



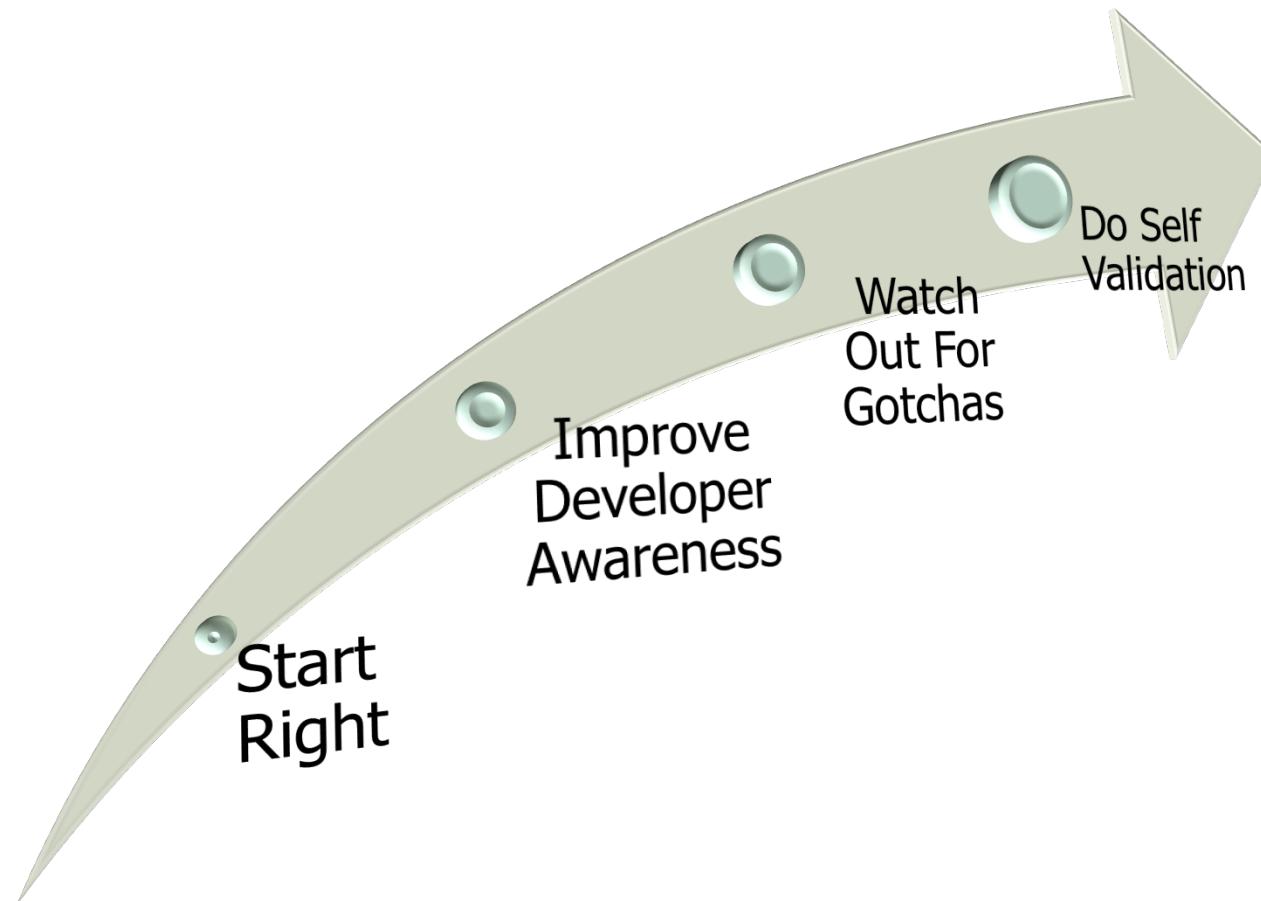
■ Requirements can be expensive:

- ▶ e.g. APP2120: The Program Manager will ensure developers are provided with training on secure design and coding practices on at least an annual basis

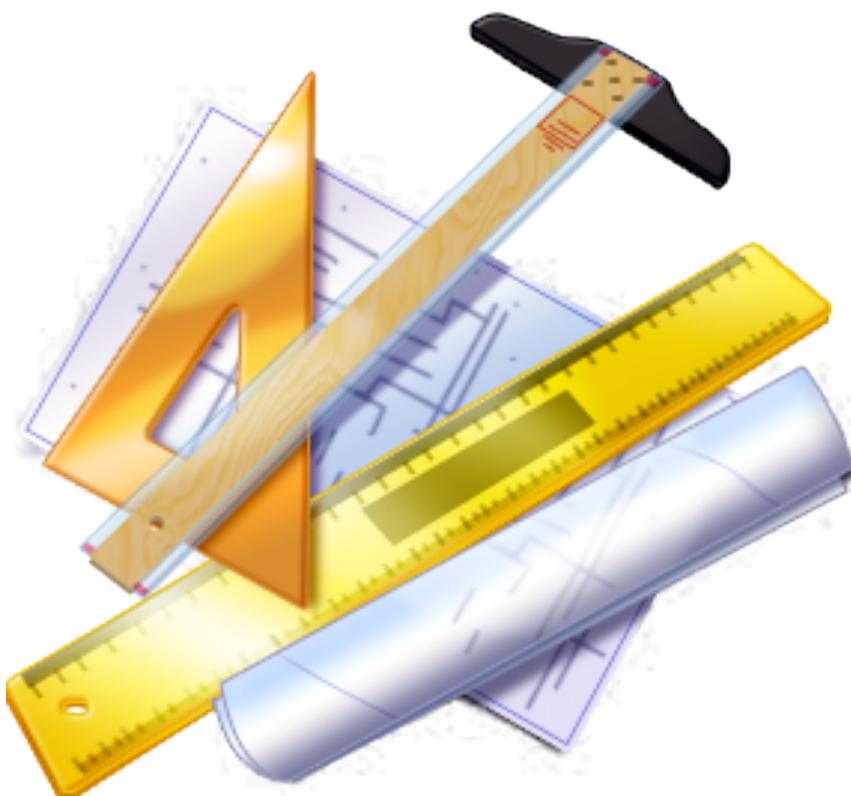
Lost in the Weeds



Roadmap to Success



Start Right



■ Allocate Time

- ▶ Proper allowances in scheduling are key!

■ Improve Acquisitions

- ▶ See
[OWASP Secure Software Development Contract Annex](#)

■ Become Aware

- ▶ See
[OWASP Application Security Verification Standard](#)

Improving Developer Awareness

- OWASP Top Ten provides a high level overview
- OWASP Development Guide provides more specific development guidance
- OWASP ESAPI Project provides standard controls



Improving Developer Awareness

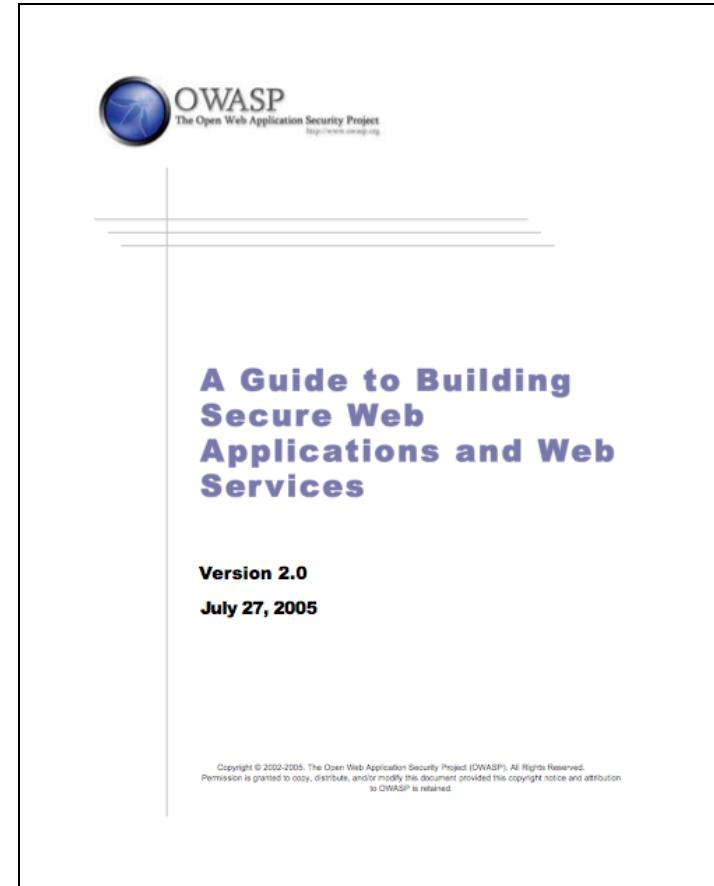
OWASP Top Ten 2007	ASD STIG
A1 – Cross Site Scripting	APP3580
A2 – Injection Flaws	APP3540, APP3570
A3 – Malicious File Execution	APP3740
A4 – Insecure Direct Object Reference	APP3450, APP3480, APP3620
A5 – Cross Site Request Forgery	N/A
A6 – Information Leakage and Improper Error Handling	APP3120, APP3620
A7 – Broken Authentication and Session Management	APP3460, APP3415, APP3420, APP3430
A8 – Insecure Cryptographic Storage	APP3210, APP3340
A9 – Insecure Communications	APP3250, APP3330
A10 – Failure to Restrict URL Access	APP3620

Improving Developer Awareness

OWASP Top Ten 2004	ASD STIG
A1 2004 – Unvalidated Input	APP3510
A2 2004 – Broken Access Control	APP3470, APP3480
<i>A3 2004 = A7 2007</i>	
<i>A4 2004 = A1 2007</i>	
A5 2004 – Buffer Overflow	APP3590
<i>A6 2004 = A2 2007</i>	
<i>A7 2004 = A6 2007</i>	
<i>A8 2004 = A8 2007</i>	
A9 2004 – Application Denial of Service	APP6080
A10 2004 – Insecure Configuration Management	APP3110, APP3290, APP3450, APP3470, APP3480, APP3500, APP6030, APP6040, APP6050, APP6210, APP6240, APP6250, APP6260, APP6260

Improving Developer Awareness

- Use the OWASP Development Guide
- Provides background about key appsec areas



http://www.owasp.org/index.php/Category:OWASP_Guide_Project

OWASP ESAPI Project

- Use standardized security controls
- Standardized library means faster development!

Custom Enterprise Web Application

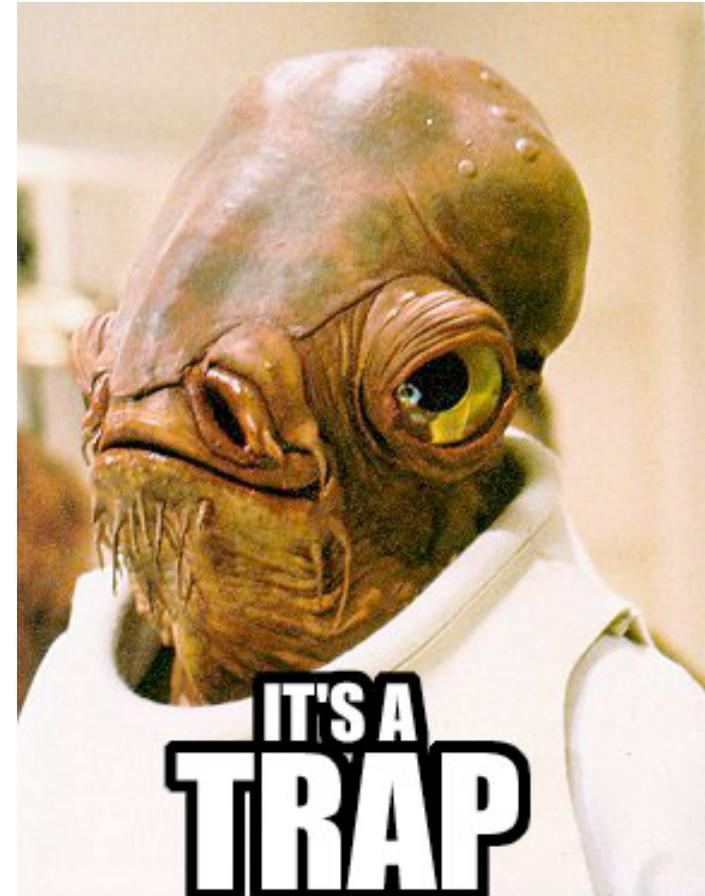
Enterprise Security API



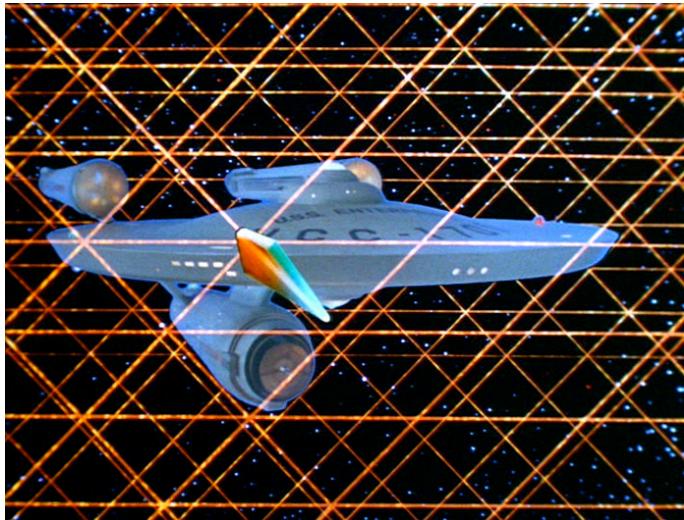
<http://www.owasp.org/index.php/ESAPI>

ASD Gotchas

- APP3010: Label all external links
- APP3270: Identify classification of pages
- APP3440: Include the DoD Logon banner
- APP3530: Set charset in the Content-Header
- APP3320: Enforce DoD password policy



ASD Gotchas (cont.)



- APP3390: Lock users after 3 attempts w/in 1 hr
- APP3400: Do not allow automatic timed unlock
- APP3660: Show last and failed login details, including date, time and IP address
- APP3415: Enforce session idle timeout
- APP3420: Include a logout link

Do Self Validation

- ASD Checklist provides a starting point for tests
- Testers are often left unable to thoroughly test
- OWASP Testing Guide provides guidance for testers of web applications:
[http://www.owasp.org/index.php/
Testing_Guide](http://www.owasp.org/index.php/Testing_Guide)



Boldy Go...

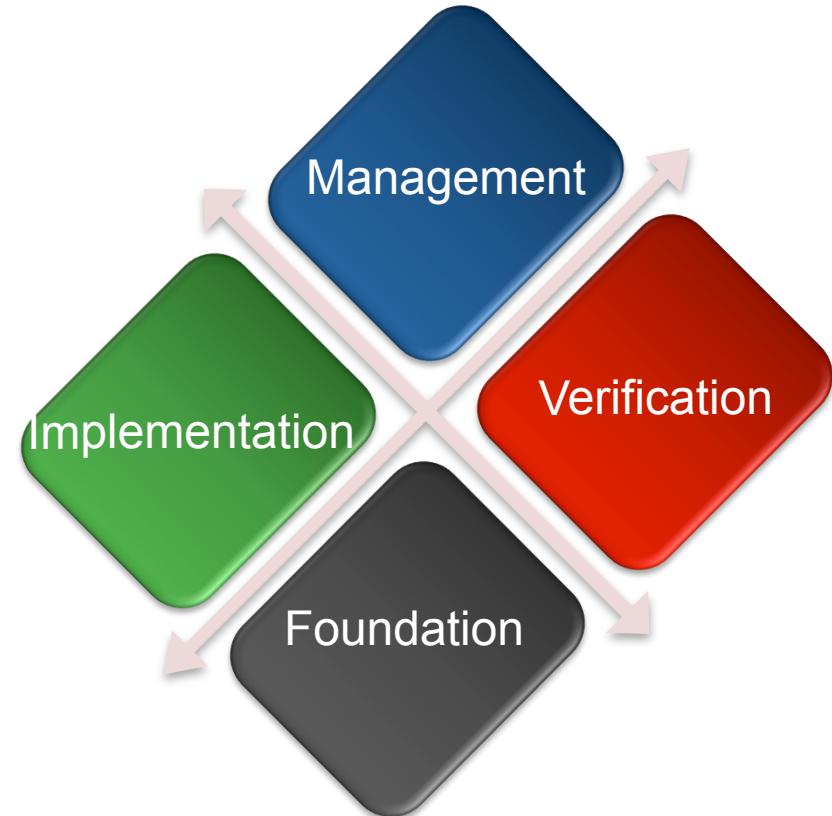
Level	Program Management	Design & Development	Testing
3	<ul style="list-style-type: none">○ Provide Security Awareness Training○ Standardize dev, build, and test platforms	<ul style="list-style-type: none">○ Create Application Threat Model○ Develop Security Logging Policy	<ul style="list-style-type: none">○ Perform Third Party Code Reviews○ Maintain Code Coverage Statistics
2	<ul style="list-style-type: none">○ Add ASD STIG to Contract Language○ Use Common Criteria Validated Products	<ul style="list-style-type: none">○ Enforce All Data Input Specifications○ Use Standardized Security Controls and Libraries	<ul style="list-style-type: none">○ Perform Fuzz Testing○ Use Automated Security Tools
1	<ul style="list-style-type: none">○ Allocate Time in Program Schedule○ Distribute Secure Coding Guidelines	<ul style="list-style-type: none">○ Use SSL with DoD Issued PKI Certificates○ Fix Easy ASD Gotchas	<ul style="list-style-type: none">○ Track Security Flaws○ Create and Perform Security Tests

Summary



- Know the variety of ASD STIG requirements
- Leverage OWASP Projects:
 - ▶ Secure Software Development Contract Annex
 - ▶ Application Security Verification Standards
 - ▶ Top Ten
 - ▶ Development Guide
 - ▶ ESAPI
 - ▶ Testing Guide

Questions?



Contact:

Jason Li

jason.li@aspectsecurity.com

ASPECT)SECURITY
Application Security Specialists