

An overview of

---

# The OWASP Testing Framework

Presented by: Mike Grima



## What is OWASP?

---

- Open Web Application Security Project
- Open source advocacy group -> web security
- Projects dedicated to security on the web



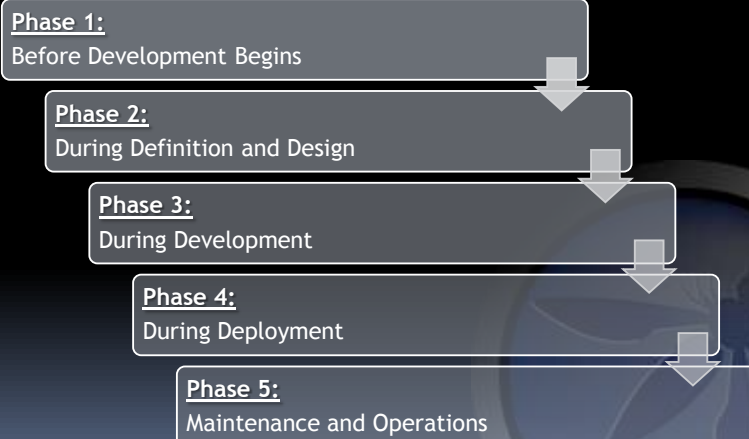
## OWASP Projects

---

- OWASP Top 10
- OWASP Testing Framework (Testing Guide)
  - Methodologies for testing web applications for security holes.
- OWASP CLASP (Comprehensive, Lightweight, Application Security Process)
- OWASP ASVS (Application Security and Verification Process)

## Testing Framework: Phases

---



## Phase 1: Before Development Begins

---

- Documentation (Policy)
- Review and modify existing security policies
- Determine the security needs of the organization
- Ex: ASP.NET Site with SQL Server
  - Windows Authentication vs. SQL Authentication

## Phase 2: During Definition and Design

---

- Determine security requirements of the application
- Review security mechanisms:
  - User Management, Authentication, Authorization, Data Confidentiality, Integrity, Accountability, Session Management, Transport Security, Tiered System Segregation, and Privacy [6].
- Ex: RSA Tokens
  - Use them for Authentication & Authorization

## Phase 3: During Development

---

- Code review
  - Help catch missed security vulnerabilities
- Code walkthroughs
  - Developers and Designers work together
  - Why code was implemented in a specific way.
    - Can it be done better?
- \*End of Phase: Penetration Testing

## Phase 4: During Deployment

---

- Application is “complete” and “shipped out”
- Perform last minute penetration testing
  - After the product has “shipped”
- Configuration Management checks

## Phase 5: Maintenance & Operations

---

- Upkeep the Application
- Review and revise policies
- Application Patching
- Schedule for Penetration Testing
- Perform QA on ALL changes

## Application Testing

---

- Designed with a Black-Box approach
- Black-Box = User has no inside knowledge of the implementation
- 10 Testing Categories
- Black Box, Grey Box, and White Box tests

## Information Gathering

---

- Only passive test
- Electronic Reconnaissance
- Google, Wget, etc.
- Ex: Attacker wants to locate information about login credentials

## Configuration Management

---

- Check for weak server configuration settings
- Look for weak cryptography, server error message output, exposed database settings, directory traversal, etc.
- Popular area for attackers to look

## Authentication Testing

---

- Check login controls
- Check for Dictionary Passwords
- Cryptographic Strength of Authentication methods
- Look for ways to bypass Authentication

## Session Management

---

- Make sure state information is being handled securely.
- Check for Session Hijacking, Session Fixation, CSRF, and generic cookie management

## Authorization Testing

---

- Do users have the correct type of access?
- Check for privilege escalation and anything that can bypass authorization

## Business Logic Testing

---

- Algorithms follow an order. Can you break the application by doing something “out of order”?
- Make test cases which attempt to do something out of order.

## Data Validation Testing

---

- Is user input good?
- Check for XSS, SQL Injection, LDAP injection, Buffer Overflows, command injection, etc.

## Denial of Service Testing

---

- NOT typical “packet flood”
- SQL wildcard attacks, lock user accounts, buffer overflows, and some obscure ones
- Having user input to make a loop counter
  - Infinite Loop?

## Web Services Testing

---

- If you use web services, this must be done
- Very important -> Effects entire infrastructure
- Information gathering (UDDI, WSDL, XML handling: SOAP)
- Perform replay attacks

## AJAX Testing

---

- AJAX is new technology that has profound impacts on the web
- Difficult to test (involve both Client and Server)
- Examining AJAX endpoints, and intercepting and debugging JavaScript code
- Not a lot of info yet -> OWASP AJAX Security Project

## OWASP vs. NIST

---

- NIST SP 800-53A
- Very similar in nature to OWASP Testing Guide
- Both list controls to test, and how to test for them.
- Both also mention how to “rate” security requirements of the application.
  - NIST much more detailed

## OWASP vs. NIST

---

- NIST is designed for generic Information Systems, such as this lab.
- OWASP is dedicated for web applications
- For full organization testing, use both!

# OWASP: You'll say WOW every time!

- Industry Standard
- Free
- Effective
- Detailed
- Step-by-Step
- Familiarity to NIST
- Any Questions?



## Sources:

- Vince ShamWow Pic: <http://just-elle.com/wp-content/uploads/2009/03/vince.jpg>
1. "About The Open Web Application Security Project," [Online document], 2009 February 19, Available at HTTP: [http://www.owasp.org/index.php/About\\_The\\_Open\\_Web\\_Application\\_Security\\_Project](http://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project)
  2. James Walden, "Integrating web application security into the IT curriculum," Proceedings of the 9th ACM SIGITE conference on Information technology education , pp. 187-192, 2008. Available at HTTP: <http://doi.acm.org.navigators-esu.pashe.edu/10.1145/1414558.1414607>
  3. L. Fitcher and R. von Solms, "Guidelines for secure software development," Proceedings of the 2008 annual research conference of the South African Institute of Computer Scientists and Information Technologists on IT research in developing countries: riding the wave of technology , pp. 56-65, 2008. Available at HTTP: <http://doi.acm.org.navigators-esu.pashe.edu/10.1145/1456659.1456667>
  4. Weber, S., Karger, P. A., and Paradkar, "A software flaw taxonomy: aiming tools at security," Proceedings of the 2005 workshop on Software engineering for secure systems—building trustworthy applications , pp. 1-7, 2005. Available at HTTP: <http://doi.acm.org.navigators-esu.pashe.edu/10.1145/1083200.1083209>
  5. "SANS Institute - SANS Top-20 2007 Security Risks (2007 Annual Update)."[Online Document] Available at HTTP: <http://www.sans.org/top20/>
  6. Matteo Meucci, OWASP Testing Guide, v3 ed. , 2008. Available at HTTP: [https://www.owasp.org/images/8/89/OWASP\\_Testing\\_Guide\\_V3.pdf](https://www.owasp.org/images/8/89/OWASP_Testing_Guide_V3.pdf)
  7. NIST Special Publication 800-53A, National Institute of Standards and Technology, July 2008. Available at HTTP: <http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf>
  8. R.Cover, Ed. "Cover Pages: Application Security Standards." [Online Document], 2008 Feb 22, Available at HTTP: <http://xml.coverpages.org/appSecurity.html#owasp>
  9. "Category:OWASP AJAX Security Project," [Online Document], 2008 Feb 24, Available at HTTP: [http://www.owasp.org/index.php/Category:OWASP\\_AJAX\\_Security\\_Project](http://www.owasp.org/index.php/Category:OWASP_AJAX_Security_Project)