Web Application Security Training

asureSECURE™

Penetration Testing Training That Will Reduce Your Security Vulnerabilities

The TVS asureSECURE team are passionate about delivering our Web Application Security Training courses based around the OWASP (Open Web Application Security Project) testing guidelines and verification standard. We offer three training packages that are tailored to meet the needs of both testers and developers.

- Web Penetration Testing 'Expert' Training Course - An Advanced Course
- The Tester Security Training Package - A One-day Introduction
- The Developer Security Training Package - A One-day Introduction

The Web Penetration Testing 'Expert' Course

TVS offers specialist penetration testing training to become an effective web application security expert. TVS has designed a syllabus driven by the latest OWASP testing guidelines and verification standard. Successful asureSECURE Web Penetration Expert (aWPE) certified staff will be able to independently undertake and complete web application penetration tests. The duration of the course is 90 hours. Details of the course content are provided overleaf.

Other Training Packages

The Tester Security Training Package

An initial one-day training course on the Open Web Application Security Project (OWASP) Top-Ten web application security vulnerabilities. This course will ensure testers understand the most critical generic security flaws and how to test for them. Including the OWASP top ten vulnerabilities.

- Injection
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Known Vulnerable Components
- Un-validated Redirects and Forwards

The Developer Security Training Package

An initial one-day training course on the Open Web Application Security Project (OWASP) Top-Ten web application security vulnerabilities. This will ensure developers understand the most critical generic security flaws and how to prevent them in design and coding. This package can be customised depending on the application technology being used such as Java, PHP, .NET etc.

TVS
Test and Verification Solutions

www.TESTANDVERIFICATION.com
security@testandverification.com
@testandverif

Penetration Testing 'Expert' Package

Introduction

- Web technology
- HTTP protocol basics
- Encoding
- Cookies
- Sessions
- Web application proxies and tools

Penetration Testing Process

- Pre-engagement
- Rules of engagement
- Methodologies
- PTES (Penetration Testing Execution Standard)
- OSSTMM (Open Source Security Testing Methodology Manual)
- OWASP testing guide
- Reporting

Information Gathering

- Conduct search engine discovery and reconnaissance for information leakage *(OTG-INFO-001)*
- Fingerprint web server *(OTG-INFO-002)*
- Review webserver metafiles for information leakage *(OTG-INFO-003)*
- Enumerate applications on webserver *(OTG-INFO-004)*
- Review webpage comments and metadata for leakage *(OTG-INFO-005)*
- Identify application entry points *(OTG-INFO-006)*
- Map execution paths through application *(OTG-INFO-007)*
- Fingerprint web application framework *(OTG-INFO-008)*
- Fingerprint web application *(OTG-INFO-009)*
- Map application architecture *(OTG-INFO-010)*

Configuration and Deployment Management Testing

- Test network / infrastructure configuration *(OTG-CONFIG-001)*
- Test application platform configuration *(OTG-CONFIG-002)*
- Test file extensions handling for sensitive information *(OTG-CONFIG-003)*
- Review old, backup and unreferenced files for sensitive information *(OTG-CONFIG-004)*
- Enumerate infrastructure and application admin interfaces *(OTG-CONFIG-005)*
- Test HTTP methods *(OTG-CONFIG-006)*
- Test HTTP strict transport security *(OTG-CONFIG-007)*
- Test RIA cross domain policy *(OTG-CONFIG-008)*

Identity Management Testing

- Test role definitions *(OTG-IDENT-001)*
- Test user registration process *(OTG-IDENT-002)*
- Test account provisioning process *(OTG-IDENT-003)*
- Testing for account enumeration and guessable user account *(OTG-IDENT-004)*
- Testing for weak or unenforced username policy *(OTG-IDENT-005)*

Authentication Testing

- Testing for credentials an encrypted channel *(OTG-AUTHN-001)*
- Testing for default credentials *(OTG-AUTHN-002)*
- Testing for weak lock out mechanism *(OTG-AUTHN-003)*
- Testing for bypassing authentication schema *(OTG-AUTHN-004)*
- Test remember password functionality *(OTG-AUTHN-005)*
- Testing for browser cache weakness *(OTG-AUTHN-006)*
- Testing for weak password policy *(OTG-AUTHN-007)*
- Testing for weak security question/answer *(OTG-AUTHN-008)*
- Testing for weak password change or reset functionalities *(OTG-AUTHN-009)*
- Testing for weaker authentication in alternative channel *(OTG-AUTHN-010)*

Authorization Testing

- Testing directory traversal/file include *(OTG-AUTHZ-001)*
- Testing for bypassing authorization schema *(OTG-AUTHZ-002)*
- Testing for privilege escalation *(OTG-AUTHZ-003)*
- Testing for insecure direct object references *(OTG-AUTHZ-004)*

Session Management Testing

- Testing for by-passing session management schema *(OTG-SESS-001)*
- Testing for cookies attributes *(OTG-SESS-002)*
- Testing for session fixation *(OTG-SESS-003)*
- Testing for exposed session variables *(OTG-SESS-004)*
- Testing for cross site request forgery (CSRF) *(OTG-SESS-005)*
- Testing for logout functionality *(OTG-SESS-006)*
- Test session timeout *(OTG-SESS-007)*
- Testing for session puzzling *(OTG-SESS-008)*

Input Validation Testing

- Testing for reflected cross site scripting *(OTG-INPVAL-001)*
- Testing for stored cross site scripting *(OTG-INPVAL-002)*
- Testing for HTTP verb tampering *(OTG-INPVAL-003)*
- Testing for HTTP parameter pollution *(OTG-INPVAL-004)*
- Testing for SQL injection *(OTG-INPVAL-005)*
- Oracle testing
- MySQL testing
- SQL server testing

- Testing Backend Security: PostgreSQL *(from OWASP BSP)*
- MS Access testing
- Testing for NoSQL injection
- Testing for LDAP injection *(OTG-INPVAL-006)*
- Testing for ORM injection *(OTG-INPVAL-007)*
- Testing for XML injection *(OTG-INPVAL-008)*
- Testing for SSI injection *(OTG-INPVAL-009)*
- Testing for XPath injection *(OTG-INPVAL-010)*
- IMAP/SMTP injection *(OTG-INPVAL-011)*
- Testing for code injection *(OTG-INPVAL-012)*
- Testing for local file inclusion
- Testing for remote file inclusion
- Testing for command injection *(OTG-INPVAL-013)*
- Testing for buffer overflow *(OTG-INPVAL-014)*
- Testing for heap overflow
- Testing for stack overflow
- Testing for format string
- Testing for incubated vulnerabilities *(OTG-INPVAL-015)*
- Testing for HTTP splitting/smuggling *(OTG-INPVAL-016)*

Testing for Error Handling

- Analysis of error codes *(OTG-ERR-001)*
- Analysis of stack traces *(OTG-ERR-002)*

Testing for weak Cryptography

- Testing for weak SSL/TLS Ciphers, insufficient transport layer protection *(OTG-CRYPST-001)*
- Testing for padding Oracle *(OTG-CRYPST-002)*
- Testing for sensitive information sent via unencrypted *(OTG-CRYPST-003)*

Business Logic Testing

- Test business logic data validation *(OTG-BUSLOGIC-001)*
- Test ability to forge requests *(OTG-BUSLOGIC-002)*
- Test integrity checks *(OTG-BUSLOGIC-003)*
- Test for process timing *(OTG-BUSLOGIC-004)*
- Test number of times a function can be used limits *(OTG-BUSLOGIC-005)*
- Testing for the circumvention of work flows *(OTG-BUSLOGIC-006)*
- Test defences against application misuse *(OTG-BUSLOGIC-007)*
- Test upload of unexpected file types *(OTG-BUSLOGIC-008)*
- Test upload of malicious files *(OTG-BUSLOGIC-009)*

Client Side Testing

- Testing for DOM-based cross site scripting *(OTG-CLIENT-001)*
- Testing for JavaScript execution *(OTG-CLIENT-002)*
- Testing for HTML injection *(OTG-CLIENT-003)*
- Testing for client-side URL redirect *(OTG-CLIENT-004)*
- Testing for CSS injection *(OTG-CLIENT-005)*
- Testing for client-side resource manipulation *(OTG-CLIENT-006)*
- Test cross origin resource sharing *(OTG-CLIENT-007)*
- Testing for cross-site flashing *(OTG-CLIENT-008)*
- Testing for clickjacking *(OTG-CLIENT-009)*
- Testing WebSockets *(OTG-CLIENT-010)*
- Test Web messaging *(OTG-CLIENT-011)*
- Test local storage *(OTG-CLIENT-012)*

About the Trainer

Arulselvar is a B.Tech Information Technology graduate, working as Security Testing Specialist at Test and Verification Solutions. He is former employee of COMODO Internet Security and Sterling Corporate Communication. He has worked on 50+ Application Penetration testing projects, 15+ Network Penetration testing projects and 10+ Mobile app penetration testing projects.

Arulselvar is a Technical head of NCDRC - National Cyber Defence Research Center to improve Indian cyberspace security. Arulselvar is certified as CEH, ISO 27001 and PCI:DSS lead implementer and has trained more than 300+ corporate staff in Information Security. Arulselvar is experienced in field Information Warfare and Ethical Hacking, and has been a visiting faculty on various Information Security seminars and conferences.

asureSECURE™

security@testandverification.com
http://asuresecure.testandverification.com/