Web Application Security QA

3-day Hands-On Course

Course Syllabus

AppSec Labs Ltd.

info@appsec-labs.com | https://appsec-labs.com | 10 HaTa'as St., Kfar Saba 44641 Israel | T: +972-9-7485005 | F: +972-9-7730595

Web Application security QA
3-day Hands-on course

Course description

Quality Assurance processes usually verify that the system meets its functional and non-functional requirements, but does verify the security aspects of the product.

This course is designed to teach the QA personnel how to test for major security vulnerabilities and identify security bugs as the last line of defense before the product is delivered to the customer, as part of the standard QA testing.

The objectives of the course are to teach QA personnel about application security vulnerabilities and how to perform security testing in web applications, and by that increasing the amount and quality of test cases that can be performed by the tester.

The course will introduce the tools & methods that should be performed by the auditor in order to efficiently find vulnerabilities and reducing the false positive / false negative rate.

Target audience

Members of the software development team:

- Security testers
- Members of the QA team
- Developers

Prerequisites

Before attending this course, students should be familiar with:

- Basic knowledge of web applications & programming concepts

Course topics

Day 1:

Information gathering

- Application Discovery
- Site Mapping & Web Crawling
- Server & Application Fingerprinting
- Identifying the entry points
- File extensions handling
- Page enumeration and brute forcing
- Comments in code – view source
- Looking for leftovers and backup files
- Admin interfaces
- Robots.txt
- Analysis of error codes
- **LAB – Identify sensitive information and information leakage**

Authentication vulnerabilities

- What is authentication?
- Authentication scenarios
- User enumeration
- Password Exposure
- Account Lockout vs. CAPTCHA
- Bypassing weak CAPTCHA mechanisms
- Guessing passwords - Brute force & Dictionary attacks
- Default users/passwords
- Weak password policy
- Direct page requests
- Parameter modification
- Password reset flaws
- Password change flaws
- Bypass Login with SQL Injection
- **LAB – Test login pages for authentication bypass**

Day 2:

Authorization vulnerabilities

- What is authorization
- Least Privileges Model
- File authorization
- Authorization bypassing
- Path traversal
- Parameter tampering
- Forceful browsing
- Client side validation attacks
- **LAB – Bypass authorization and impersonating**

Business logic attacks

- Business logic attacks
- Flow bypassing
- Replay attacks
- Abuse of functionality
- **LAB - Business logic attacks**

Injections and Input Validation

- What Is considered Input?
- Input Validation Techniques
- Command Injection
- SQL Injection
- Cross side scripting
- Text based injection
- Log injection
- XML injection
- **LAB – Extract sensitive data using injection attacks**

Day 3:

Insecure file handling

- Path traversal
- Canonicalization
- Insecure file extension handling
- Directory listing
- File size
- Uploaded files backdoors
- Path traversal during upload files
- Upload files threats and mitigations
- **LAB – Upload malicious code-files and overwrite system's files**

Session management

- Session management techniques
- Cookie based session management
- Cookie properties
- Cookies - secrets in cookies, cookie tampering
- Exposed session variables
- Important session attributes
- **LAB – Test session management weaknesses**

Browser manipulation attacks

- Cross Site Request Forgery (CSRF)
- Open redirect
- Clickjacking
- Auto complete & Saved passwords
- Sensitive information in Browser's cache
- **LAB – Identify browser manipulation vulnerabilities**

Auditing

- Importance of Logging
- What Should Be Audited
- Sensitive Data
- What Should the Log Include