Web Application Hacking (Penetration Testing)

5-day Hands-On 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 Hacking (Penetration Testing)
5-day Hands-On Course

Course Description

Our web sites are under attack on a daily basis and the next security breach is just a matter of time. This intensive hands-on course will teach you how to find those vulnerabilities in your web applications before the bad guys do. The course will introduce the various methods, tools and techniques used by attackers, in order to know how to test for the major security vulnerabilities and how to identify security bugs on real systems, by using live hacking demonstrations and hands-on labs. The objectives of the course are to teach developers and security professionals about the most dangerous vulnerabilities and how to perform security testing, and by that increasing the amount and quality of test cases that can be performed by the auditor.

This course provides intensive hands-on labs using real world applications.

Target Audience

Members of the software development team:

- Security professionals
- Software experts
- Experienced developers

Prerequisites

Before attending this course, students should be familiar with:

- Operating systems concepts, basic knowledge in databases & SQL language
- Programming concepts, with emphasis on web applications (HTML/JS)

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
- Looking for leftovers
- Google hacking
- Analysis of error code
- **LAB – Collect information and reveal application's sensitive data**

Injections and Validations

- Encoding attacks
- Command injection
- Code injection
- LDAP injection
- Log / CRLF injection
- Header injection
- SMTP injection
- XML injection
- XPATH injection
- Input validation techniques
- Blacklist VS. Whitelist input validation bypassing
- **LAB – Exploit improper input validation**

Day 2:

Authentication Vulnerabilities

- What is authentication?
- Supported authentication types - anonymous, basic, digest, forms, Kerberos, client certificate
- Authentication scenarios
- User enumeration
- Guessing passwords - brute force & dictionary attacks
- Direct page requests
- Parameter modification
- Password reset flaws
- Password change flaws
- Bypassing weak CAPTCHA mechanisms
- Common implementation mistakes - authentication bypassing using SQL injection, LDAP injection, XPATH injection
- **LAB – Bypass authentication forms using multiple method**

Authorization Vulnerabilities

- What is authorization?
- Authorization models - DAC/MAC
- RBAC
- Authorization bypassing
- Canonicalization & path traversal
- Parameter tampering
- Forceful browsing
- Rendering based authorization
- Client side validation attacks
- Hardening
- **LAB - Authorization bypassing and impersonation**

Business Logic Vulnerabilities

- Business flow bypass
- Replay attack
- Currency manipulation
- Business logic attack vectors
- Direct access to web services
- **LAB – Exploit business logic vulnerabilities**

Day 3:

SQL Injection Vulnerabilities

- Introduction to SQL command structure
- NoSQL injection – Mongo, ORM
- Database manipulation
- Circumventing authentication
- Retrieving data
- Inserting data
- Deleting data
- Attacking availability
- Local system access
- Discovering vulnerable apps
- Error based
- Blind
- Binary search
- Evasion
- **LAB – Practice SQL injection attacks**

File Handling Attacks

- Path traversal
- Canonicalization
- Uploaded file backdoors
- Insecure file extension handling
- Directory listing
- File size
- File type
- Malware upload
- **LAB – Exploit insecure file handling, upload web shells, deface using upload file mechanism**

Day 4:

Cross Site Scripting (XSS) Vulnerabilities

- Overview of XSS
- XSS Description
- Reflected XSS
- Stored / persistent XSS
- DOM based XSS
- XSS Whitelist VS. Blacklist input validation
- Discovery approaches – Manual VS. Automatic VS. Semi-automatic
- Different XSS scenarios
- XSS input validation evasion
- **LAB – Perform XSS attacks**

Browser Manipulation Techniques

- CSRF (Cross Site Request Forgery)
- Clickjacking
- Open redirects
- HTTP response splitting
- **LAB – Perform actions on-behalf users by CSRF, Test websites for Click jacking**

Day 5:

Cryptography Pitfalls

- Symmetric cryptography
- Asymmetric cryptography
- Hashing
- Digital signing
- PKI / certificate
- SSL protocol
- SSL cipher suite
- Insufficient transport layer protection
- **LAB – Cryptography lab**

Application Denial Of Service (DoS) Vulnerabilities

- Application / OS crash
- CPU starvation
- Memory starvation
- File system starvation
- Resource starvation
- Triggering high network bandwidth
- User level DoS
- Exploiting a specific vulnerability
- Zip bomb
- Over flows
- reDoS
- Parsing errors
- **LAB - Application DoS**

Attacking Client Side Applications

- HTML5 approach
- Client side attacks
- Analyze client side source code
- Insecure storage
- Flash decompile
- Crossdomain.xml
- CORS requests
- **Lab – Client site application hacking**