INFOSECTRAIN

WEB APPLICATION PENETRATION TESTING

ONLINE TRAINING COURSE

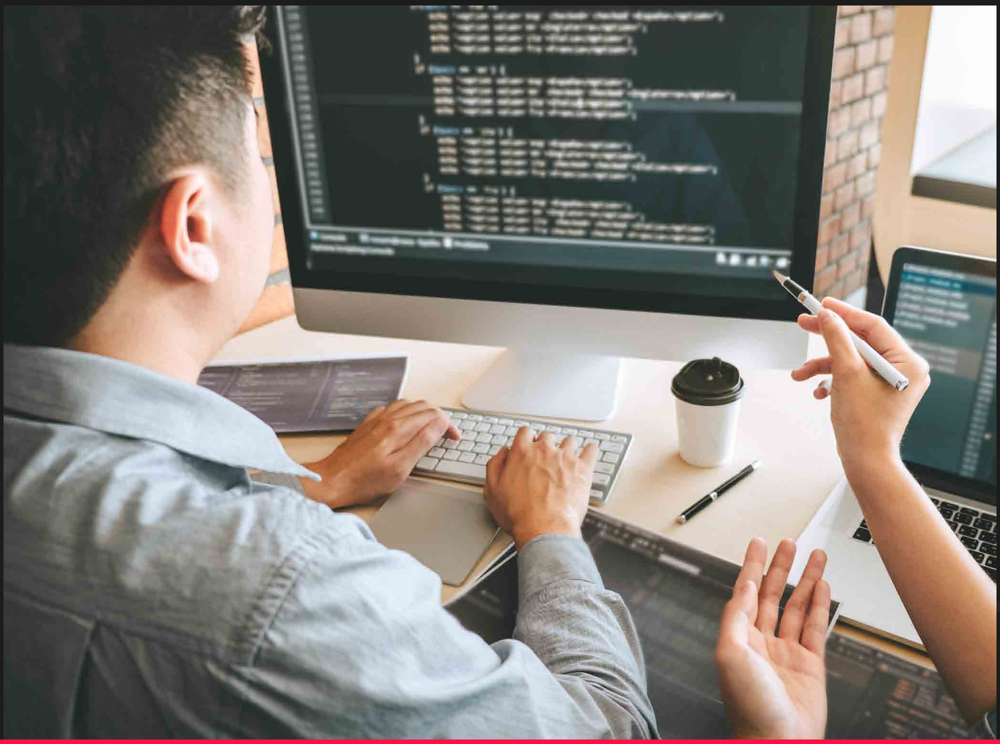
www.infosectrain.com | sales@infosectrain.com

Course Description

Web Application Penetration Testing Training at Infosectrain is designed to teach the details of web app penetration testing in an immersive environment. Our trainers are experts of the industry and they will teach you Web application analysis, information gathering and enumeration to add to your skill. Our Web Application Penetration Testing course will let you have a hands-on penetration testing experience in our cloud-hosted lab environment.You will be provided with an app demonstrating a vulnerability commonly found in a Web or mobile app. which will help you in learning to assess the app and exploit it like an experienced professional.

Thus, during this WAPT course you will learn to:

- Exploit and defend web apps
- Perform static and dynamic analysis of web application by using popular tools
- Find vulnerabilities in source code, and
- Exploit weaknesses in the implementation of web application security



Target Audience

Web Application Penetration Testing Course is beneficial for:

- Penetration testers
- Application developers
- Web administrators
- Security analysts

Pre-Requisite

- Basic understanding of HTML, HTTP and JavaScript.
- Knowledge of PHP code will help although it is not mandatory
- one year in an information security role, or equivalent experience is recommended.

Why Infosec Train?

- Certified & Experienced Instructor
- Flexible Schedule
- Access to the recorded sessions
- Post Training Support
- Tailor Made Training
- 4 hrs/day in Weekend/ Weekday

COURSE CONTENT

- Web Application Assessment
- Authentication vulnerabilities
- Authorization vulnerabilities
- Improper Input Validation & Injection vulnerabilities
- Insecure file handling
- Session & browser manipulation attacks
- Information leak

Course Content

Web Application Assessment

- OWASP Top 10 Vulnerabilities
- Threat Modelling Principle
- Site Mapping & Web Crawling
- Server & Application Fingerprinting
- Identifying the entry points
- Page enumeration and brute forcing
- Looking for leftovers and backup files

Authentication vulnerabilities

- Authentication scenarios
- User enumeration
- Guessing passwords - Brute force & Dictionary attacks
- Default users/passwords
- Weak password policy
- Direct page requests
- Parameter modification
- Password flaws
- Locking out users
- Lack of SSL at login pages
- Bypassing weak CAPTCHA mechanisms
- Login without SSL

Authorization vulnerabilities

- Role-based access control (RBAC)
- Authorization bypassing
- Forceful browsing
- Client-side validation attacks
- Insecure direct object reference

Improper Input Validation & Injection vulnerabilities

- Input validation techniques
- Blacklist VS. Whitelist input validation bypassing
- Encoding attacks
- Directory traversal
- Command injection
- Code injection
- Log injection
- XML injection – XPath Injection | Malicious files | XML Entity
- bomb
- LDAP Injection
- SQL injection
- Common implementation mistakes – authentication
- Bypassing using SQL Injection
- Cross Site Scripting (XSS)
- Reflected VS. Stored XSS
- Special chars – ' & < >, empty

Insecure file handling

- Path traversal
- Canonicalization
- Uploaded files backdoors
- Insecure file extension handling
- Directory listing
- File size
- File type
- Malware upload

Session & browser manipulation attacks

- Session management techniques
- Cookie based session management
- Cookie properties
- Cookies - secrets in cookies, tampering
- Exposed session variables
- Missing Attributes - httpOnly, secure
- Session validity after logoff
- Long session timeout
- Session keep alive - enable/disable
- Session id rotation
- Session Fixation
- Cross Site Request Forgery (CSRF)
  - URL Encoding
- Open redirect

Information leak

- Web Services Assessment
- Web Service Testing
- OWASP Web Service Specific Testing
- Testing WSDL
- Sql Injection to Root
- LFI and RFI]
- OWASP Top 10 Revamp

INFOSECTRAIN

www.infosectrain.com | sales@infosectrain.com