iSecur1ty Web Application Penetration Testing V2.0 syllabus

IS|WAPT v2.0

Course overview

- Introduction to the course & labs Configuration.
- Basics of web application penetration testing.
- Introduction to Web Application Firewalls.
- Client Side Attacks.
- Browsers Security.
- Server Side Attacks.
- Challenges.

Module 1
Intro to the course & Labs Configuration.

- Introduction to the course.
- Labs Configuration.
- Materials and forums support.

Module 2
Basics of web application penetration testing.

- Introduction to Web application penetration testing.
- Basics of web application architectures.
- HTTP protocol basics.
- Proxy and Interception Requests.

Module 3
Introduction to Web Application Firewalls.

- What is WAFs (Web Application Firewalls) ?.
- WAFs Types.
- Fillter , Regulator expression and WAF bypass.

Module 4
Client side attacks

- Cross site scripting vulnerabilities (XSS).
  * Reflected XSS.
  * Stored XSS.
  * DOM XSS.
  * Self-XSS.

- Payloads creating and aggregation

Module 4
Client Side Attacks

- Advanced XSS Exploits using special techniques.
- XSS case stuides.
- XSS exercises solve.

Module 4
Client Side Attacks

- Cross site request forgery vulnerabilities (CSRF).
  * GET and POST CSRF.
  * Token tests.
  * Advanced CSRF with XSS.
  * JSON CSRF.

- CSRF case stuides.

Module 4
Client Side Attacks

- Click Jacking vulnerability.
  * Basics for XFO and Iframe .
  * Frame busting introduction and bypass.
- Reflected file download (New web attack vector).
- Cross site script inclusion (XSSI).

Module 5
Browser Security

- Mime sniffing.
- UXSS.
- Cache.
- XFO.
- HSTS .
- Flash plugin.

Module 6
Server Side Attacks

- Introduction to Server Side Attacks.
- Misconfiguration attacks.
  * Default Credentials.
  * Default Content.
  * Vulnerable web server software.
- Ports and directory.

Module 6
Server Side Attacks

- Attacking authentication.

  -Types :

  * HTML forms-based authentication.
  * Multi-factor authentication.
  * HTTP basic authentication.
- Bad passwords.
- Forgotten password functionality.

Module 6
Server Side Attacks

- Attacking authentication :
  * brute force attack.
  * Forgotten Password Functionality.

Module 6
Server Side Attacks

- SQL Injection Attacks :
  * Fingerprinting the database.
  * Exploiting a basic vulnerability.
  * Bypassing check with SQLi.
  * Using sqlmap.
  * Using SQLi to reconnaissance.
  * SQLi to RCE .

Module 6
Server Side Attacks

- Injecting OS Commands :

  * OS types.

  * commands and split.

  * Finding OS command injection flaws.

- Logic flaws.

Module 6
Server Side Attacks

- File inclusion vulnerabilities :
  * Local file inclusion.
  * Remote file inclusion.
  * Path traversal.
  * Tips to find file inclusion.
  * Tricks to bypass WAF.

Module 6
Server Side Attacks

- HTTP Header Injection.
  * HTTP response splitting (CRLF).
  * Injecting cookies.
  * Delivering other attacks.

Module 6
Server Side Attacks

- XML external entity (XXE) Attacks :
  * Description.
  * Vulnerability.
  * XXE DOS (billion laughs attack).