IT Certification Guru PVT.LTD

Web Application Penetration Testing

Prerequisite(Ethical Hacking)
Duration(75 Days)

Module:-1 Introduction

- 1.0 what is Web Penetration Testing
- 2.0 what is Web?
- 3.0 Understanding the Depth of Web

Module:-2 Owasp Top 10 Injection

- 1.0 What is owasp top 10 injection
- 2.0 what is Proxy?
- 3.0 What is Interception Proxies
- 4.0 Burp Suite Introduction

Module:-3 Information Gathering

- 1.0 Finding WHOIS and DNS
- 2.0 DNS Harvesting Extracting
- 3.0 A Open source information Gathering
- 4.0 The HTTP Protocols
- 5.0 HTTP Methods Open source information Gathering
- 6.0 HTTP Status codes
- 7.0 HTTP Request and Response
- 8.0 what is HTTPS
- 9.0 HTTP Methods and Verb Tampering
- 10 HTTP Method Testing with Nmap and Metasploit

Module:-4 Web App Basic Test

- 1.0 Web App Cryptography Attacks
- 2.0 Data Encoding
- 3.0 Encoding Schemes, URL Encoding, Unicode Encoding
- 4.0 Bypassing weak cipher
- 5.0 Testing HTTPS
- 6.0 Nmap Scan
- 7.0 Gathering Server Info

Module:-5 Burp Suite In-Depth

- 1.0 Burp Target
- 2.0 Burp Proxy
- 3.0 Burp Intruder
- 4.0 Burp Repeater
- 5.0 Burp Scripting
- 6.0 Spidering Web Application
- 7.0 Analysing Spidering
- 8.0 Burp Fuzzing

Office 21-25/A, First Floor Shreenath Plaza, Dnyaneshwar Paduka Chowk,
Pune, Maharashtra 411005 Mob: +91-7798058777

IT Certification Guru PVT.LTD

Module:-6 Broken Authentication and Session Management

- 1.0 Information Leakage
- 2.0 Directory Browsing
- 3.0 What is Authentication
- 4.0 HTTP Response Splitting
- 5.0 HTTP Basic Authentication
- 6.0 Bypass Authentication prompt
- 7.0 Attacking HTTP Basic Authentication with Nmap and Metasploit
- 8.0 HTTP Digest Authentication
- 9.0 HTTP Set-Cookie with HTTPCookie
- 10 Username Harvesting

Module:-7 Injection Attacks

- 1.0 HTML Injection Basics
- 2.0 HTML Injection in Tag Parameters
- 3.0 session Tracking
- 4.0 session Fixation
- 5.0 Authentication Bypass

Module:-8 Command Injection

- 1.0 Command Injection
- 2.0 Web to Shell on the Server
- 3.0 Web Shell: PHP Meterpreter
- 4.0 Web Shell: Netcat Reverse Connects
- 5.0 Web Shell: Using Python, PHP etc.

Module:-9 LFI and RFI

- 1.0 Remote Basics
- 2.0 RFI to Meterpreter
- 3.0 LFI Basics
- 4.0 LFI with Directory Prepends
- 5.0 Remote Code Execution with LFI and File Upload Vulnerability

Module:-10 Upload attacks

- 1.0 File Upload Vulnerability Basics
- 2.0 Beating Content-Type Check in File Upload
- 3.0 Bypassing Blacklists in File Upload
- 4.0 Bypassing Whitelists using Double Extensions in File Uploads
- 5.0 Null Byte Injection in File Uploads
- 6.0 Exploiting File Uploads to get Meterpreter

Module:-11 Unvalidated Redirects and Forwards

- 1.0 Unvalidated Redirects
- 2.0 Exploitation Open Redirects
- 3.0 Securing Open Redirects

Office 21-25/A, First Floor Shreenath Plaza, Dnyaneshwar Paduka Chowk,
Pune, Maharashtra 411005 Mob: +91-7798058777

IT Certification Guru PVT.LTD

Module:-12 SQL Injection

- 1.0 SQL Injection
- 2.0 SQLi discovering
- 3.0 Error based SQLi
- 4.0 Blind based SQLi
- 5.0 Data Extraction
- 6.0 Sql Tools
- 7.0 SQLmap
- 8.0 sqlmap + ZAP

Module:-13 Client-side Attacks

- 1.0 what is javascript
- 2.0 DOM-based Xss
- 3.0 explotating DOM-xss
- 4.0 Javascript injection
- 5.0 Cross-Site Scripting
- 6.0 Reflective XSS
- 7.0 Stored Xss
- 8.0 XSS tools
- 9.0 XSS Fuzzing
- 10 Xss Exploitation
- 11 Beef tool Stealing Cookies
- 12 Ajax
- 14 Ajax XSS

Module:-14 CSRF attacks

- 1.0 Cross-site Request Forgery
- 2.0 Exploitation CSRF
- 3.0 Login Attack

Module:-15 Web app Tools

- 1.0 What is automation Testing
- 2.0 What is Manual testing
- 3.0 WPScan
- 4.0 W3af
- 5.0 Wordpress testing

Module:-16 Firewall Testing

- 1.0 Web Application Firewall
- 2.0 Wap Options
- 3.0 Mod_security
- 4.0 WAF Detection

Module:-17 Methodology and Reporting

- 1.0 Web Application Penetration testing methods
- 2.0 Reporting and Presenting

Office 21-25/A, First Floor Shreenath Plaza, Dnyaneshwar Paduka Chowk,
Pune, Maharashtra 411005 Mob: +91-7798058777

IT Certification Guru PVT.LTD

Module:-18 Other Attacks

- **1.0 SSI Attacks**
- **2.0 Server-side Template Injection**
- **3.0 IDOR Injection**
- **4.0 LDAP Injection**
- **5.0 XML External Entity**

Module:-19 Platform

- **1.0 Samurai WTF**
- **2.0 bWAPP**
- **3.0 DVWA**
- **4.0 PentesterLab**
- **5.0 Root-me.org**
- **6.0 Owasp-BWA**
- **7.0 Owasp-WebGoat**

Module:-20 what Next?

- **What is Android Penetration Testing?**
- **Hacking using Nethunter**
- **Hacking using Raspberry-PI.**

**Office 21-25/A, First Floor Shreenath Plaza, Dnyaneshwar Paduka Chowk,
Pune, Maharashtra 411005 Mob: +91-7798058777**

IT
Certifications
guru