HACKERU
Experience Makes Experts

Web Application Penetration Testing Fundamentals

Index: RT300

40
Hours

Web Application Penetration Testing Fundamentals

Description

The majority of modern organizations use web applications or services on a regular basis. Unfortunately, as this platform has made our lives easier in many ways, it has also opened the door for malicious hackers to come in and exploit multiple vulnerabilities.
This course will teach participants the fundamentals of penetrating web-applications and exploiting a variety of known vulnerabilities. Students will be introduced to many tools and techniques used by attackers and learn how to check for the majority of security vulnerabilities, how to identify security bugs and more. The training is almost entirely geared towards hands-on practitioners and includes a variety of live demonstrations and exercise labs.

Target Audience

The course targets participants with a foundation knowledge in information security and ethical hacking, who wish to enter the world of web-app pen-testing. Primarily:

- Ethical hackers
- Penetration testers
- Red Team members
- Technical cyber security personnel
- Experienced web developers

Prerequisites

- Good knowledge of computer networking and background in information security.
- Basic knowledge in ethical hacking or infrastructure hacking.
- Familiarization with web development (HTML, CSS, JavaScript, etc.) is an advantage.
- CEH provides a solid foundation of preliminary knowledge required for this course.

Objectives

- Understanding how to approach a web application in order to penetrate into the system or exploit it in any other way.
- Practicing various web-app exploitation techniques.
- Learning the hidden and less widely-known ways of overcoming seamingly inpenetrable apps or web functions.
- Learning JavaScript basics in order to perform penetration tests on a broader level, and understanging its influence on security aspects.
- Eventually, participants will be able to test web applications and exploit a broad range of their vulnerabilites.

Course Outline

01

Introduction

6 Hours

The first module will introduce participants to the fundamentals of web application vulnerabilities and hacking techniques, through a thorough understanding of different protocols, and the use of infrastructure tools to attack web servers. This module will deepen the participants' understanding of the connection between the infrastructure and web domains, which is crucial to further grasp the web-app pen-testing arena.

- HTTP basics
- HTTP methods
- HTTP 1.0/1.1/2.0
- HTTP basic authentication
- Attacking basic authentication with Nmap
- Attacking with Metasploit
  - Basic authentication
  - Vulnerability scanning with WMAP
- Session ID
  - Understanding session ID
  - Hijacking session ID
- Overview of server and client attacks
- Case studies of recent vulnerabilities
- Web application pen-testing process – where to
- begin?
- Burp Suite overview
- Application infrastructure
  SSL
  - Configuration
  - Vulnerabilities
    - BEAST
    - BREACH
    - CRIME
    - Heartbleed
    - Poodle
    - and more
- Application misconfigurations
  Brute force directories

02

Attacking Web Applications

20 Hours

The first module will introduce participants to the fundamentals of web application vulnerabilities and hacking techniques, through a thorough understanding of different protocols, and the use of infrastructure tools to attack web servers. This module will deepen the participants' understanding of the connection between the infrastructure and web domains, which is crucial to further grasp the web-app pen-testing arena.

- OWASP Top 10
- Scanning for vulnerabilities:
  - Nessus
  - Nikto
  - Acunetix
- Collecting leaked information from the website
- Web server directory traversal
- Proxies
  - ZAP
  - Finding vulnerabilities with Burp Suite
- Local File Inclusion (LFI)
  - Prepending through directories
  - Remote code execution
  - Null Byte
  - Log poisoning
- URL encoding
- Remote File Inclusion (RFI)
  - Forced extensions
  - RFI to Meterpreter
- SQL database
  - Exercise: build your own database
  - SQL injection
  - Blind SQL injection
- Injecting into LDAP
- Vulnerabilities in the "upload" function
  - Checking content-type
  - Bypassing blacklists
  - Bypassing whitelists
  - Using Null Byte
- Cross-Site Scripting (XSS)
  - Reflected
  - Stored
  - DOM
- Cross Site Request Forgery (CSRF)
  - CSRF basics
  - Trigger tags
  - Multi-Step operation handling
  - Mitigating with tokens
- Unvalidated redirects
- Insecure direct object reference

03

JavaScript (JS) Exploitation

14 Hours

The majority of websites employ Java Script, which is why familiarity with the language is crucial for a better practice of web application security. During this module, students will learn the basics of JavaScript from the (in)security point of view, and understand how to exploit its existing vulnerabilities for web-app attacks.

- Modify HTML with JS
- Hijack form submitting
- Modify forms
- Capturing clicks
- Event listener
- Fetching data
- Extracting CSRF tokens
- XSS
- Sessions – flaws & fixation
- AJAX
- XML and JSON parsing