14-Hacking Web Applications

PLEASE use prebuilt labs

Victim Data: direct interaction Need 2-6 computers online that have the services running and vulnerable

Advanced: Build a data file / artifact that is actionable by the contract holder. There are no instructions for this task. You must figure everything out.
Advanced: capture encrypted packets, using decryption process from capture discussion

Attacker Data: Kali/ Parrot

Objective

The objective of the lab is to perform web application hacking:

- Footprinting a web application using various information-gathering tools
- Performing web spidering, detect load balancers, and identify web server directories
- Performing web application vulnerability scanning
- Performing brute-force and cross-site request forgery (CSRF) attack
- Exploiting parameter tampering and cross-site scripting (XSS) vulnerabilities
- Exploiting WordPress plugin vulnerabilities
- Exploiting remote command execution vulnerability
- Exploiting file upload vulnerability
- Gaining backdoor access via a web shell
- Detecting web application vulnerabilities using various web application security tools

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform web application attacks on the target web application. Recommended labs that will assist you in learning various web application attack techniques include:

1. Footprint the web infrastructure
    1.1. Perform web application reconnaissance
    1.2. Perform web application reconnaissance using WhatWeb
    1.3. Perform web spidering using OWASP ZAP

~~1.4. Detect load balancers using various tools~~

1.5. Identify web server directories

~~1.6. Perform web application vulnerability scanning using Vega~~

1.7. Identify clickjacking vulnerability using iframe

2. Perform web application attacks

2.1. Perform a brute-force attack using Burp Suite*

2.2. Perform parameter tampering using Burp Suite*

2.3. Exploit parameter tampering and XSS vulnerabilities in web applications

2.4. Perform cross-site request forgery (CSRF) attack*

2.5. Enumerate and hack a web application using WPScan and Metasploit

2.6. Exploit a remote command execution vulnerability to compromise a target web server

2.7. Exploit a file upload vulnerability at different security levels

2.8. Gain backdoor access via a web shell using Weevely

*Indicates capture