Web Attacks with Kali Linux

Syllabus

Copyright © 2021 Offensive Security Ltd. All rights reserved.
1. Copyright
2. Introduction to WEB-200
   a. Secrets of Success with WEB-200
      Think Offensively to Improve Defense
      Adapt A Growth Mindset
      Try Harder
      Collect Data and Do Your Research
   b. Introduction to Security Concepts
      The CIA Triad
      Other Security Principles
   c. Getting Started With WEB-200
      The Course Structure
      Lab Overview
      Connecting to the VPN
      Disconnecting from the VPN
      Conclusion
3. Tools
   a. Getting Started
      Accessing The Lab Machines
      About Proxies
   b. Burp Suite
      Burp Suite's Built-In Browser
      Using Burp Suite with Other Browsers
      Proxy
      Intruder
      Repeater
   c. Nmap
      Nmap Scripts
   d. Wordlists
      SecLists Installation
      Choosing a Wordlist
      Building Custom Wordlists
   e. Gobuster
      Installing Gobuster & Basic Usage
      Endpoint Discovery with Gobuster
Go Bust Those Subdomains!

f. Wfuzz
   File Discovery
   Directory Discovery
   Parameter Discovery
   Fuzzing Parameter Values
   Fuzzing POST Data

g. Hakrawler
   Hakrawler Installation
   Hakrawler and the Wayback Machine

h. Shells
   Web Technology
   Choosing the Correct Shell
   Payloads

4. Cross-Site Scripting Introduction and Discovery
   a. Introduction to the Sandbox
      Accessing the Sandbox
      Understanding the Sandbox
   b. JavaScript Basics for Offensive Uses
      Syntax Overview
      Useful APIs
   c. Cross-Site Scripting - Discovery
      Reflected Server XSS
      Stored Server XSS
      Reflected Client XSS
      Stored Client XSS

5. Cross-Site Scripting Exploitation and Case Study
   a. Cross-Site Scripting - Exploitation
      Accessing The Sandbox
      Moving the Payload to an External Resource
      Stealing Session Cookies
      Stealing Local Secrets
      Keylogging
      Stealing Saved Passwords
      Phishing Users
b. Case Study: Shopizer Reflected XSS
   - Getting Started
   - Discovering the Vulnerability
   - Loading Remote Scripts
   - Exploiting Reflected XSS

6. Cross-Origin Attacks
   a. Same-Origin Policy
      - Accessing the CORS Sandbox
      - Introduction to the Same-Origin Policy
   b. SameSite Cookies
   c. Cross-Site Request Forgery (CSRF)
      - Detecting and Preventing CSRF
      - Exploiting CSRF
   d. Case Study: Apache OFBiz
      - Accessing Apache OFBiz
      - Apache OFBiz - Discovery
      - Apache OFBiz - Exploitation
      - Revising the CSRF Payload
   e. Cross-Origin Resource Sharing (CORS)
      - Anatomy of the CORS Request
      - Response Headers
   f. Exploiting Weak CORS Policies
      - Weak CORS Policies - Discovery
      - Trusting Any Origin
      - Improper Domain Allowlist

7. Introduction to SQL
   a. SQL Overview
      - Basic SQL Syntax
      - Manual Database Enumeration
   b. Enumerating MySQL Databases
      - MySQL Specific Functions and Tables
   c. Enumerating Microsoft SQL Server Databases
      - Microsoft SQL Server Specific Functions and Tables
   d. Enumerating PostgreSQL Databases
      - PostgreSQL Specific Functions and Tables
8. SQL Injection
   a. Introduction to SQL Injection
      What is SQL Injection?
   b. Testing for SQL Injection
      String Delimiters
      Closing Out Strings and Functions
      Sorting
      Boundary Testing
      Fuzzing
   c. Exploiting SQL Injection
      Error-based Payloads
      UNION-based Payloads
      Stacked Queries
      Reading and Writing Files
      Remote Code Execution
   d. Database dumping with Automated Tools
      SQLMap
   e. Case Study: Error-based SQLi in Piwigo
      Accessing Piwigo
      Discovering the Vulnerable Parameter
      Exploiting Error-based SQL Injection

9. Directory Traversal Attacks
   a. Directory Traversal Overview
      Accessing The Lab Machines
   b. Understanding Suggestive Parameters
   c. Relative vs. Absolute Pathing
      Absolute Pathing
      Relative Pathing
   d. Directory Listing
      Parameter Analysis
      Evidence of Directory Listing
   e. Directory Traversal Sandbox
      Directory Traversal - Exploitation
Wordlist/Payload Lists
Fuzzing the Path Parameter

f. Case Study: Home Assistant
   Initial Application Assessment
   Exploitation

g. Wrapping Up

10. XML External Entities
    a. Introduction to XML
       XML Entities
    b. Understanding XML External Entity Processing Vulnerabilities
    c. Testing for XXE
       Retrieving Files
       Error-based Testing
       Out-of-Band Testing
    d. Case Study: Apache OFBiz XXE Vulnerability
       Accessing Apache OFBiz
       Discovery
       Exploitation
       Error-Based Exploitation
       Out-of-Band Exploitation

11. Server-side Template Injection - Discovery and Exploitation
    a. Templating Engines
       Accessing the Template Sandbox
       Introduction to Templating Engines
    b. Twig - Discovery and Exploitation
       Twig - Discovery
       Twig - Exploitation
    c. Apache Freemarker - Discovery and Exploitation
       Freemarker - Discovery
       Freemarker - Exploitation
    d. Pug - Discovery and Exploitation
       Pug - Discovery
       Pug - Exploitation
    e. Jinja - Discovery and Exploitation
       Jinja - Discovery
Web Attacks with Kali Linux

Jinja - Exploitation

f. Mustache and Handlebars - Discovery and Exploitation
   Mustache and Handlebars - Discovery
   Mustache and Handlebars - Exploitation

g. Halo - Case Study
   Accessing Halo
   Halo - Translation and Discovery
   Halo - Exploitation

h. Craft CMS with Sprout Forms - Case Study
   Accessing Craft CMS
   Craft CMS with Sprout Forms - Discovery
   Craft CMS with Sprout Forms - Exploitation

12. Command Injection

   a. Discovery of Command Injection
      Accessing the Command Injection Sandbox
      Familiarizing Ourselves with the Sandbox
      Where is Command Injection Most Common?
      About the Chaining of Commands & System Calls

   b. Dealing with Common Protections
      Typical Input Normalization - Sending Clean Payloads
      Typical Input Sanitization - Blocklisted Strings Bypass
      Blind OS Command Injection Bypass
      Extra Mile

   c. Enumeration & Exploitation
      Enumerating Command Injection Capabilities
      Obtaining a Shell - Netcat
      Obtaining a Shell - Python
      Obtaining a Shell - Node.js
      Obtaining a Shell - PHP
      Obtaining a Shell - Perl
      File Transfer
      Extra Mile I
      Writing a Web Shell
      Extra Mile II

d. Case Study - OpenNetAdmin (ONA)
Accessing OpenNetAdmin
Discovery and Assessment
Exploitation

13. Server-side Request Forgery
   a. Introduction to SSRF
      Interacting with the Vulnerable Server
      Interacting with Back-end Systems and Private IP Ranges
   b. Testing for SSRF
      Accessing the SSRF Sandbox Application
      Discovering SSRF Vulnerabilities
      Calling Home to Kali
   c. Exploiting SSRF
      Retrieving Data
      Instance Metadata in Cloud
      Bypassing Authentication in Microservices
      Alternative URL Schemes
      Extra Mile
   d. Case Study: Group Office
      Accessing Group Office
      Discovering the SSRF Vulnerabilities
      Exploiting the SSRF Vulnerabilities

14. Insecure Direct Object Referencing - targeting Q1 2022
15. Assembling the Pieces - targeting Q1 2022