Offensive Security

Advanced Web Attacks and Exploitation

v. 1.0

Mati Aharoni
Devon Kearns
Francesco Ongaro

Course Overview

The days of porous network perimeters are fading fast as services become more resilient and harder to exploit. In order to penetrate today's modern networks, a new approach is required. In order to gain that initial critical foothold in a network, penetration testers must be fluent in the art of exploiting front-facing web applications. Offensive Security's Advanced Web Attacks and Exploitation will take you far beyond the simple basics of SQL injection and bring you deep into the realm of web application penetration testing.

From mind-bending XSS attacks, to exploiting race conditions, to advanced SQL injection attacks, Advanced Web Attacks and Exploitation will broaden your knowledge of web application hacking and help you identify and circumvent various protection mechanisms in use on the web today.

Course Description

Advanced Web Attacks and Exploitation is NOT an entry-level course. The pace or learning is fast and furious - students are expected to have a solid understanding of how to perform basic web application attacks, at a minimum. This class is aimed at penetration testers and security auditors who need to take their web application penetration testing skills to a new level.

It is assumed that the student already has a medium understanding of the underlying protocols and technologies involved in testing web applications such as the HTTP protocol, SSL communications, and the usage of various browser plugins and proxies. A basic familiarity with web based programming languages such as php, javascript and mysql will also prove helpful.

Course Outline

1 Prelude to the Course

1.1 Virtual Lab Composition
1.2 Virtual Lab Setup

2 Cross Site Scripting (XSS)

2.1 Past, Present, and Future of XSS
2.2 Impact of XSS Attacks
2.3 Business Impact and Scoring
  2.3.1 CVSS
  2.3.2 Canonical Classification
2.4 Types of XSS Attacks
  2.4.1 Reflected XSS
  2.4.2 Stored XSS
  2.4.3 Document Object Model (DOM XSS)
2.5 XSS Vulnerability Discovery
2.6 XSS Vulnerability Exploitation
  2.6.1 Signature Based Filters
  2.6.2 Sanitization Routines
  2.6.3 Encoding
  2.6.4 Length Constraints
  2.6.5 Exploiting Different Languages
    2.6.5.1 PHP, ASP, PERL
    2.6.5.2 CGI, BASH, SH, C/C++
    2.6.5.3 ASP.NET
    2.6.5.4 JSP, JSF
    2.6.5.5 PYTHON, RUBY
  2.6.6 XSS in Cascading Style Sheets (CSS)
  2.6.7 Exploiting File Uploads
    2.6.7.1 HTML
    2.6.7.2 SVG
    2.6.7.3 XML
  2.6.8 Technology Specific XSS
    2.6.8.1 Browser Specific
    2.6.8.2 Browser's Plugins
    2.6.8.3 Flash XSS
    2.6.8.4 Java Applet XSS
    2.6.8.5 Web server XSS
  2.6.9 Infrastructure Components and Default Applications XSS
    2.6.10 Cross Zone Injection
    2.6.11 Same Origin Bypass via DNS
2.7 Attack Payloads

2.7.1 Cookie Grabber
2.7.2 Keystroke logger
2.7.3 Port Scanner
2.7.4 Access and Modify the DOM Structure
2.7.5 Circumvent the Same-origin Policy
2.7.6 Other Malicious Actions
2.7.7 Advanced Techniques
2.8 Conclusions
2.9 References and Books
2.10 Table of Examples

3 Cross Site Request Forgery (CSRF)
3.1 History of CSRF
3.2 Impact of CSRF Attacks
3.3 Business Impact and Scoring
3.4 Dynamic of a CSRF Attack
3.5 Common Anti-CSRF Protections
3.6 Types of CSRF Attacks
3.7 CSRF Vulnerability Discovery
3.8 CSRF Vulnerability Exploitation
3.9 Identify Anti-CSRF Protections in Source Code
3.10 Attacks Payloads
3.11 Advanced Techniques
3.11.1 Real Life Example Against Symantec Live Update Administrator
3.11.2 Session Fixation
3.11.3 Cross Site Printing
3.11.4 DNS Pinning
3.12 Conclusions
3.13 References
3.14 Table of Examples

4 Business Logic Issues and Race Conditions
4.1 Code and Business Logic Issues
4.2 PoorLemon's Shopping Cart
4.3 The “smart” Warehouse
4.4 The Mobile Recharging Tool
4.5 Race Conditions
4.6 Conclusions
4.7 Table of Examples

5 SQL Injections

5.1 History of SQL Injection
5.2 Impact of SQLi Attacks
5.3 Business Impact and Scoring
5.3.1 CVSS
5.3.2 Canonical Classification
5.4 Types of SQLi Attacks
5.4.1 First Order Attack
5.4.2 Second Order Attack
5.4.3 Lateral Injection
5.4.4 In-Band or Inbound
5.4.5 Out of Band
5.4.6 Inferential or Inference
5.5 SQL Injection Vulnerability Discovery
5.6 SQL Injection Vulnerability Exploitation
5.6.1 Blind SQL Injection
5.6.1.1 Brute-Force by Direct Match
5.6.1.2 Brute-Force on Single Chars
5.6.1.3 Binsearch (or Bisection) on Single Chars
5.6.1.4 Binsearch with Custom-Balanced Binary Search Tree on Single Chars
5.6.1.5 Search in N Order
5.6.1.6 Mappable SQL Injections
5.7 Advanced Exploitation
5.7.1 Detecting MySQL and its Version
5.7.2 101 ways for SUBSTRING()
5.7.3 LOCATE() Based Inverse Substring
5.8 References
5.9 Table of Examples

6 Command Execution and Code Injection

6.1 History of Command Execution and Code Injection
6.2 Impact of Command Execution and Code Injection Attacks
6.3 Business Impact and Scoring
6.3.1 CVSS
6.3.2 Canonical Classification
6.4 Types of Code Injections
6.4.1 Shell Injection
6.4.2 Dynamic Evaluation
6.5 Code Injection Vulnerability Discovery
6.6 Dynamic Evaluation Vulnerability Discovery
6.7 Command Execution Vulnerability Exploitation
6.8 References
6.9 Table of Examples

7 File System Vulnerabilities

7.1 History of File System Vulnerabilities
7.2 Impact of File System Vulnerabilities
7.3 Business Impact and Scoring
7.3.1 CVSS
7.3.2 Canonical Classification
7.4 Overview of File System Issues
7.4.1 Information Disclosure
7.4.1.1 File Existence
7.4.2 Code and Command Execution
7.4.2.1 Arbitrary File Write
7.4.2.2 Local File Inclusion (LFI)
7.4.2.3 Remote File Inclusion (RFI)
7.5 Discovery
7.6 Exploitation
7.6.1 Information Disclosure
7.6.2 Code Execution
7.7 References
7.8 Table of Examples

8 Configuration and Authentication Issues

8.1 Business Impact and Scoring
8.2 Overview of Configuration and Authentication Issues
8.2.1 Exposed Management Interfaces
8.2.2 Exposed Documentation
8.2.3 Exposed Demo Applications
8.2.4 Exposed Debug Functions
8.2.5 Debug Error Handling
8.2.6 Excessive Information
8.3 References
8.4 Table of Examples

9 Web Services and XML

9.1 History of Web Services and XML Issues
9.2 Business Impact and Scoring
9.3 Overview of Web Services and XML Issues
9.4 References
9.5 Table of Examples