Offensive Security

Advanced Web Attacks and Exploitation

v. 1.0

Mati Aharoni
Devon Kearns

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. Atmail Mail Server Appliance Case Study – CVE-2012-2593
- **1.1 Getting Started**
- **1.2 Web Related Attack Vectors**
  - 1.2.1 Impact of XSS Attacks
  - 1.2.2 Types of XSS Attacks
  - 1.2.3 XSS Vulnerability Discovery
- **1.3 Attack Implementation**
  - 1.3.1 Exercise: Atmail - Document Dookie
- **1.4 Stealing Cookies and Hijacking Authenticated Sessions**
  - 1.4.1 Exercise: Atmail – All your Email is Belong to Us
- **1.5 Cross Site Request Forgery 101**
  - 1.5.1 Types of CSRF Attacks
  - 1.5.2 CSRF Vulnerability Discovery
- **1.6 Better Email Snooping Through CSRF**
  - 1.6.1 Exercise: Atmail – All Your Email is Forwarded to Us
- **1.7 Research, Research, Research**
  - 1.7.1 Exercise: Atmail - uid=3000(atmail) groups=3000(atmail)
- **1.8 From XSS to Server Compromise**
  - 1.8.1 The Atmail Attack Plan
- **1.9 Further Reading**

2. X-Cart Shopping Cart Case Study – CVE-2012-2570
- **2.1 Getting Started**
  - 2.1.1 XSS Filter Evasion
  - 2.1.2 Exercise: Revenge of alert("XSS")
- **2.2 Getting the Lay of the Land**
- **2.3 Building the XSS Payload**
- **2.4 Exploiting the XSS Vulnerability**
  - 2.4.2 Exercise: XSS Filter Bypassing
- **2.5 Further Reading**

3. SolarWinds Orion Case Study - CVE-2012-2577
- **3.1 Getting Started**
- **3.2 Web Related Attack Vectors**
- **3.3 View State Stuff**
- **3.4 Attack Implementation**
  - 3.4.1 Exercise: Alert("SNMP Rules, Always")
- **3.5 SolarWinds Orion XSS: Now What?**
  - 3.5.1 Exercise: More Than Meets the Eye
- **3.6 Trying to Add a User**
  - 3.6.1 Exercise: Hopeless Quest
- **3.7 Trying Harder**