FULL STACK WEB ATTACK

by Steven Seeley

TRAINING DESCRIPTION

Full Stack Web Attack is not an entry-level course. It's designed to push you beyond what you thought was possible and set you on the path to develop your own workflow for offensive zero-day web research. Each of the vulnerabilities presented have either been mirrored from real zero-day or are n-day vulnerabilities that have been discovered by the author with a focus on not just exploitation, but also on the discovery. The course material is fully illustrated with detailed slides, workbook, code samples and an answer sheet given out at the end. If you want to learn how to exploit web technologies without client interaction for maximum impact, that is, remote code execution then this is the course for you. Leave your OWASP Top Ten at the door.

TRAINING OUTCOMES

Upon completion of the training course, students should be able to:

- Setup debugging environments for PHP and Java
- Trace code through a debugger
- Discover basic zero-day vulnerabilities
- Chain and exploit web-based vulnerabilities for maximum impact
- Write quality patches and bypass vendor developed patches
- Perform patch differentiation to reveal n-day vulnerabilities
- Write high quality vulnerability reports
- Stay focused for long periods of time to achieve results

ABOUT THE TRAINER

Steven Seeley is a world-renowned security researcher who has over a decade of experience in application security. He has been credited with finding over 1500 high impact security vulnerabilities affecting vendors such as Microsoft, VMWare, Apple, Adobe, Cisco and many others. In 2020, Steven teamed up with Chris Anastasio competing in Pwn2Own Miami - winning the Master of Pwn title. In 2021, Steven reached 12th position on the MSRC top 100 Vulnerability Researchers list.

Buy tickets: https://romhack.io/buy-tickets/

ROMHACK TRAINING

WHAT TO BRING

> x64 host operating system
> 16 Gig RAM minimum
> Virtualization software (VMWare Player, Workstation or Fusion)
> 100 Gig of available hard disk space

WHAT WILL BE PROVIDED

> Access to VMs with laboratories

PARTICIPANT SKILL SET

> An open mind that is ready to focus
> Basic scripting skills with moderate or advanced preferred
> Some exposure to container-based technologies and Unix operating systems
> A strong understanding of various web technologies
> A foundational understanding of common web vulnerabilities

CLASS SYLLABUS

DAY 1

Java Introduction

- Java language fundamentals
- Debugging Java applications

Framework Overview

- Spring MVC
- Struts v1/2

Java Deserialization Primer

- Serializable vs Externalizable
- Unmarshalling vs Deserialization
- Reflection in theory and practice
- Pivot gadgets

JNDI Injection

- RMI and JRMP overview
- Remote class loading
- Exception Handling Deserialization
- Local Object Factory exploitation

Analyzing the Struts Framework

- *Action Mappings*
- *Dynamic Method Invocation*
- *Interceptor Stacks*
- *Case studies:*
    - *Do I even exist? - Analyzing an edge-case RCE vulnerability*

- *Devil in the details - Analyzing a TOCTOU framework vulnerability*

DAY 2

JDBC Injection

- Common drivers and their exploitation primitives
- Exploiting the MySQL Driver via Deserialization
- Discovering your own driver primitives

Authentication Bypasses

- Auditing Servlet Filters
- Auditing Interceptors
- Common authentication bypass patterns

Java deserialization for researchers

- *Building upon Ysoserial*
- *Custom gadget chain creation*
- *Chaining vulnerabilities*

Server-side template injection

- Analyzing and exploiting CVE-2022-XXXXX

Java Bean Validation - Attacking Custom Validators

- Analyzing and exploiting CVE-2022-XXXXX

DAY 3

C# .NET Introduction

- C# Language Fundamentals
- Debugging C# Basic Applications

Architecture and Framework Overview

- IIS Overview
- Application Pools
- ASP.NET

Debugging

- Disabling CLR optimizations
- Debugging with DNSpy
- Program Database Symbols
- Debugging with Visual Studio/dotPeek

Developing Applications in Visual Studio

- Reusing application code
- Compiling Release and Debug builds

Training page: https://romhack.io/full-stack-web-attack/
RomHack Training 2024: https://romhack.io/training/

- Navigating code
- Common project options

DAY 4:

.NET Deserialization Primer

- Unmarshalling VS Deserialization
- Understanding Ysoserial.net
- System.Runtime.Serialization.iFormatter Exploitation
- JavascriptSerializer
- Json.Net
- Json.Net Custom TypeConverters
- Json.Net ISerializationBinder

Analysis of CVE-2023-XXXXX Remote Code Execution

- Discovering the Vulnerability
- Exploitation

Analysis of CVE-2023-XXXXX Elevation of Privilege

- Discovering the Vulnerability
- Exploitation

Analysis of *CVE-2023-XXXXX File Disclosure*

- Vulnerability Discovery

Analysis of *CVE-2023-XXXXX XXE*

- Vulnerability Discovery