KOENIG step forward

OffSec | Learning Partner

KOENIG SOLUTIONS · COURSE OUTLINE

Advanced Web Attacks and Exploitation (OSWE) Preparation

Learn to analyse source code and chain vulnerabilities to achieve remote code execution against real-world web applications.

14
MODULES

176
TOPICS

COURSE OVERVIEW

This course covers tools and methodologies for web traffic inspection, source code recovery and vulnerability analysis, then applies them against a series of real applications. It works through case studies including ATutor, ManageEngine Applications Manager, Bassmaster NodeJS, DotNetNuke, ERPNext, openCRX, openITCOCKPIT, Concord and Guacamole Lite, covering issues such as SQL injection, authentication bypass, type juggling, deserialization, XXE, SSRF and prototype pollution. Each case study moves from vulnerability discovery through exploitation to gaining remote code execution. The course closes with a review of the techniques covered and further exercises for continued practice.

WHO THIS COURSE IS FOR

- **Penetration Testers**
- **Security Researchers**
- **Exploit Developers**
- **Application Security Engineers**
- **Red Team Operators**

LEARNING OBJECTIVES

- Apply Burp Suite and Python to inspect and manipulate web traffic
- Recover and analyse source code from compiled .NET and Java applications
- Identify SQL injection flaws and use them for data exfiltration
- Exploit PHP type juggling and authentication bypass vulnerabilities
- Analyse deserialization flaws to achieve remote code execution
- Discover and exploit server-side template injection vulnerabilities
- Assess CORS, CSRF and SSRF weaknesses in web applications
- Exploit prototype pollution to achieve remote code execution

COURSE SYLLABUS

14 Modules, 176 Topics

01

Introduction

ABOUT THE AWAE COURSE

OSWE Exam Attempt

Our Approach · Obtaining Support

OFFENSIVE SECURITY AWAE LABS

General Information · Lab Restrictions · Forewarning and Lab Behavior · Control Panel

Reporting · Backups · About the OSWE Exam · Wrapping Up

02

Tools & Methodologies

WEB TRAFFIC INSPECTION

Burp Suite Proxy · Using Burp Suite with Other Browsers · Burp Suite Scope · Burp Suite Repeater and Comparer · Burp Suite Decoder

Interacting with Web Listeners using Python

SOURCE CODE RECOVERY

Managed .NET Code · Decompiling Java Classes

SOURCE CODE ANALYSIS METHODOLOGY

An Approach to Analysis · Using an IDE · Common HTTP Routing Patterns · Analyzing Source Code for Vulnerabilities

DEBUGGING

Remote Debugging

Wrapping Up

03

ATutor Authentication Bypass and RCE

GETTING STARTED

Setting Up the Environment

Initial Vulnerability Discovery · A Brief Review of Blind SQL Injections

DIGGING DEEPER

When $addslashes Are Not · Improper Use of Parameterization

DATA EXFILTRATION

Comparing HTML Responses · MySQL Version Extraction

Subverting the ATutor Authentication · Authentication Gone Bad · Bypassing File Upload Restrictions

GAINING REMOTE CODE EXECUTION

Escaping the Jail · Disclosing the Web Root · Finding Writable Directories · Bypassing File Extension Filter

Wrapping Up

04

ATutor LMS Type Juggling Vulnerability

TOPICS

Getting Started · PHP Loose and Strict Comparisons · PHP String Conversion to Numbers · Vulnerability Discovery

ATTACKING THE LOOSE COMPARISON

Magic Hashes · ATutor and the Magic E-Mail address

Wrapping Up

05

ManageEngine Applications Manager AMUserResourcesSyncServlet SQL Injection RCE

TOPICS

Getting Started

VULNERABILITY DISCOVERY

Servlet Mappings · Source Code Recovery · Analyzing the Source Code · Enabling Database Logging · Triggering the Vulnerability

HOW HOUDINI ESCAPES

Using CHR and String Concatenation · It Makes Lexical Sense

Blind Bats

ACCESSING THE FILE SYSTEM

Reverse Shell Via Copy To

POSTGRESQL EXTENSIONS

Build Environment · Testing the Extension · Loading the Extension from a Remote Location

UDF Reverse Shell

MORE SHELLS

PostgreSQL Large Objects · Large Object Reverse Shell

Summary

06

Bassmaster NodeJS Arbitrary JavaScript Injection Vulnerability

TOPICS

Getting Started · The Bassmaster Plugin · Vulnerability Discovery · Triggering the Vulnerability · Obtaining a Reverse Shell · Wrapping Up

07

DotNetNuke Cookie Deserialization RCE

SERIALIZATION BASICS

- XmlSerializer Limitations
- Basic XmlSerializer Example
- Expanded XmlSerializer Example
- Watch your Type, Dude

DOTNETNUKE VULNERABILITY ANALYSIS

- Vulnerability Overview
- Manipulation of Assembly Attributes for Debugging
- Debugging DotNetNuke Using dnSpy
- How Did We Get Here?

PAYLOAD OPTIONS

- FileSystemUtils PullFile Method
- ObjectDataProvider Class
- Example Use of the ObjectDataProvider Instance
- Serialization of the ObjectDataProvider
- Enter The Dragon (ExpandedWrapper Class)
- Putting It All Together
- Wrapping Up

08

ERPNext Authentication Bypass and Server Side Template Injection

GETTING STARTED

Configuring the SMTP Server · Configuring Remote Debugging · Configuring MariaDB Query Logging

INTRODUCTION TO MVC, METADATA-DRIVEN ARCHITECTURE, AND HTTP ROUTING

Model-View-Controller Introduction · Metadata-driven Design Patterns · HTTP Routing in Frappe

AUTHENTICATION BYPASS DISCOVERY

Discovering the SQL Injection

AUTHENTICATION BYPASS EXPLOITATION

Obtaining Admin User Information · Resetting the Admin Password

SSTI VULNERABILITY DISCOVERY

Introduction to Templating Engines · Discovering The Rendering Function · SSTI Vulnerability Filter Evasion

SSTI VULNERABILITY EXPLOITATION

Finding a Method for Remote Command Execution · Gaining Remote Command Execution

Wrapping Up

09

openCRX Authentication Bypass and Remote Code Execution

TOPICS

- Getting Started

PASSWORD RESET VULNERABILITY DISCOVERY

- When Random Isn't
- Account Determination
- Timing the Reset Request
- Generate Token List
- Automating Resets

openCRX Authentication Bypass and Remote Code Execution (continued)

XML EXTERNAL ENTITY VULNERABILITY DISCOVERY

- Introduction to XML
- XML Parsing
- XML Entities
- Understanding XML External Entity Processing Vulnerabilities
- Finding the Attack Vector
- CDATA
- Updating the XXE Exploit
- Gaining Remote Access to HSQLDB
- Java Language Routines

REMOTE CODE EXECUTION

- Finding the Write Location
- Writing Web Shells
- Wrapping Up

10

openITCOCKPIT XSS and OS Command Injection - Blackbox

TOPICS

Getting Started · Black Box Testing in openITCOCKPIT

APPLICATION DISCOVERY

Building a Sitemap · Targeted Discovery

Intro To DOM-based XSS · XSS Hunting

ADVANCED XSS EXPLOITATION

What We Can and Can't Do · Writing to DOM · Creating the Database · Creating the API · Scraping Content · Dumping the Contents

RCE HUNTING

Discovery · Reading and Understanding the JavaScript · Interacting With the WebSocket Server · Building a Client · Attempting to Inject Commands · Digging Deeper

Wrapping Up

11

Concord Authentication Bypass to RCE

TOPICS

- Getting Started

AUTHENTICATION BYPASS: ROUND ONE - CSRF AND CORS

- Same-Origin Policy (SOP)
- Cross-Origin Resource Sharing (CORS)
- Discovering Unsafe CORS Headers
- SameSite Attribute
- Exploit Permissive CORS and CSRF
- **Authentication Bypass:** Round Two - Insecure Defaults
- Wrapping Up

12

Server Side Request Forgery

TOPICS

Getting Started

INTRODUCTION TO MICROSERVICES

Web Service URL Formats

API DISCOVERY VIA VERB TAMPERING

Initial Enumeration · Advanced Enumeration with Verb Tampering

INTRODUCTION TO SERVER-SIDE REQUEST FORGERY

Server-Side Request Forgery Discovery · Source Code Analysis · Exploiting Blind SSRF in Directus · Port Scanning via Blind SSRF · Subnet Scanning with SSRF · Host Enumeration

Render API Auth Bypass

EXPLOITING HEADLESS CHROME

Using JavaScript to Exfiltrate Data · Stealing Credentials from Kong Admin API · URL to PDF Microservice Source Code Analysis

REMOTE CODE EXECUTION

RCE in Kong Admin API

Wrapping Up

13

Guacamole Lite Prototype Pollution

GETTING STARTED

Understanding the Code · Configuring Remote Debugging

INTRODUCTION TO JAVASCRIPT PROTOTYPE

Prototype Pollution · Blackbox Discovery · Whitebox Discovery

Prototype Pollution Exploitation

EJS

EJS - Proof of Concept · EJS - Remote Code Execution

HANDLEBARS

Handlebars - Proof of Concept · Handlebars - Remote Code Execution

Wrapping Up

14

Conclusion

TOPICS

The Journey So Far · Exercises and Extra Miles · The Road Goes Ever On · Wrapping Up

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training | Live Online Classes (ILO) | Fly-Me-A-Trainer (FMAT) | Flexi (Self-Paced) | 1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com | info@koenig-solutions.com