HACKINGPOINT

CHECK POINT™

Advanced Web Hacking

4 day class | Get Certified | Advanced Track

This curriculum continues the Art of Web Hacking series
Learn advanced hacking techniques that compromise web apps, APIs, and associated end-points.
The class focuses on server-side flaws. The vulnerabilities we present usually go undetected by modern scanners.

You will have access to:

- State-of-the-art hacklab with relevant tools and VMs
- Dedicated Kali VM to each attendee
- Scripts and tools are provided during the training, along with student hand-outs.

If you work in the security industry of modern web applications, you will benefit from this class. This is not a beginner class. To gain the maximum value from the topics being explored, attendees should have a strong understanding of the OWASP top 10 issues. The class does not cover all AppSec topics and focuses only on advanced identification and exploitation techniques of vulnerabilities.

Available remotely to Check Point customers and partners
Class size up to 16 students.

Requirement

Bring a laptop with admin/root access

Class Content

- LAB SETUP AND ARCHITECTURE OVERVIEW
- INTRODUCTION TO BURP FEATURES
- ATTACKING AUTHENTICATION AND SSO
  -Token Hijacking attacks
  - Logical Bypass / Boundary Conditions
  - Bypassing 2 Factor Authentication
  - Authentication Bypass using Subdomain Takeover
  - JWT/JWS Token attacks
  - SAML Authorization Bypass
  - OAuth Issues
- PASSWORD RESET ATTACKS
  - Session Poisoning
  - Host Header Validation Bypass
  - Case study of popular password reset fails
- BUSINESS LOGIC FLAWS / AUTHORIZATION FLAWS
- PASSWORD RESET ATTACKS
  - Session Poisoning
  - Host Header Validation Bypass
  - Case study of popular password reset fails
- BUSINESS LOGIC FLAWS / AUTHORIZATION FLAWS
  - Mass Assignment
  - Invite/Promo Code Bypass
  - Replay Attack
  - API Authorisation Bypass
  - HTTP Parameter Pollution (HPP)
- XML EXTERNAL ENTITY (XXE) ATTACK
  - XXE Basics
  - Advanced XXE Exploitation over OOB channels
  - XXE through SAML
  - XXE in File Parsing
- BREAKING CRYPTO
  - Known Plaintext Attack (Faulty Password Reset)
  - Padding Oracle Attack
  - Hash length extension attacks
  - Auth bypass using .NET Machine Key
  - Exploiting padding oracles with fixed IVs
- REMOTE CODE EXECUTION (RCE)
  - Java Serialization Attack
  - Net Serialization Attack
  - PHP Serialization Attack
  - Python serialization attack
  - Server Side Template Injection
  - Exploiting code injection over OOB channel
- SQL INJECTION MASTERCLASS
  - 2nd order injection
  - Out-of-Band exploitation
  - SQLi through crypto
  - OS code exec via PowerShell
  - Advanced topics in SQli
  - Advanced SQLMap Usage and WAF bypass
  - Pentesting GraphQL
- TRICKY FILE UPLOAD
  - Malicious File Extensions
  - Circumventing File validation checks
  - Exploiting hardened web servers
  - SQL injection via File Metadata
- SERVER-SIDE REQUEST FORGERY (SSRF)
  - SSRF to query internal network
  - SSRF to exploit templates and extensions
  - SSRF filter bypass techniques
  - Various Case studies
- ATTACKING THE CLOUD
  - SSRF Exploitation
  - Serverless exploitation
  - Google Dorking in the Cloud Era
  - Cognito misconfiguration to data exfiltration
  - Post Exploitation techniques on Cloud-hosted applications
  - Various Case Studies
- ATTACKING HARDENED CMS
  - Identifying and attacking various CMS
  - Attacking Hardened Wordpress, Joomla, and Sharepoint
- WEB CACHING ATTACKS
- MISCELLANEOUS VULNERABILITIES
  - Unicode Normalization attacks
  - Second order IDOR attack
  - Exploiting misconfigured code control systems
  - HTTP Desync attack
- ATTACK CHAINING N TIER VULNERABILITY CHAINING
- LEADING TO RCE
- VARIOUS CASE STUDIES
  - A Collection of weird and wonderful XSS and CSRF attacks

NotSoSecure part of
claranet cyber security