HACKING POINT

Advanced Web Hacking

4 day class

Get Certified

Advanced Track

This curriculum continues the Art of Web Hacking series
Learn 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
- A hacking lab for 30 days after completion of the course. 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.

BLACK BELT EDITION
Available remotely to Check Point customers and partners
Class size up to 16 students on-site.

Requirement

Bring a laptop with admin/root access

CLASS CONTENT

Check Point
SOFTWARE TECHNOLOGIES LTD.

Authentication Bypass

Token hijacking attacks
SQL column truncation attack
Logical bypass / Boundary conditions

SAML / OAUTH 2.0 / AUTH-0 / JWT Attacks

JW token brute-force attacks
SAML authentication and authorization bypass XXE through SAML
Advanced XXE exploitation over OOB channels

Password reset attacks

Cookie swap
Host header validation bypass
Case study of popular password reset fails

Breaking Cyrpto

Known plaintext attack (faulty password reset) Path traversal using Padding Oracle
Hash length extension attacks

Business logic flaws / Authorization flaws

Mass assignment
Invite / promo code bypass Replay attack

SQL injection

2nd order injection Out-of-band exploitation SQLi through crypto
NoSQL injection
OS code exec via powershell Advanced topics in SQLi

Remote Code Execution (RCE)

Java serialization attack
Node.js RCE
PHP object injection
RCE through XXE (with blind XXE) RCE through XSLT
Rails remote code execution
Ruby / ERB template injection
Exploiting code injection over OOB channel

Server Side Request forgery (SSRF)

SSRF to query internal networks SSRF to code exec

Unrestricted file upload

Malicious file extensions Circumventing file validation checks Web shells for modern platforms

Miscellaneous Topics

HTTP parameter pollution (HPP) XXE in file parsing
Collection of weird and wonderful XSS and CSRF attacks

Attack Chaining

Combining client-side and server-side attacks to steal internal secrets
B33r 101

In collaboration with
NOT SO SECURE
A Claranet Group Company