Advanced Web Hacking

Get Certified Today!

Check Point SOFTWARE TECHNOLOGIES LTD

3 DAY CLASS | ADVANCED TRACK

NotSoSecure is excited to launch the Advanced Web Hacking class. Similar to the Advanced Infrastructure Hacking class, this class covers a wealth of hacking techniques that compromise web applications, APIs, and associated end-points. The focus of this course is on specific areas of app-sec, advanced vulnerability identification, and exploitation techniques (especially server side flaws). In the class, attendees will practice some neat, new, and ridiculous hacks which penetrated real clients and are mentioned in bug-bounty programs.

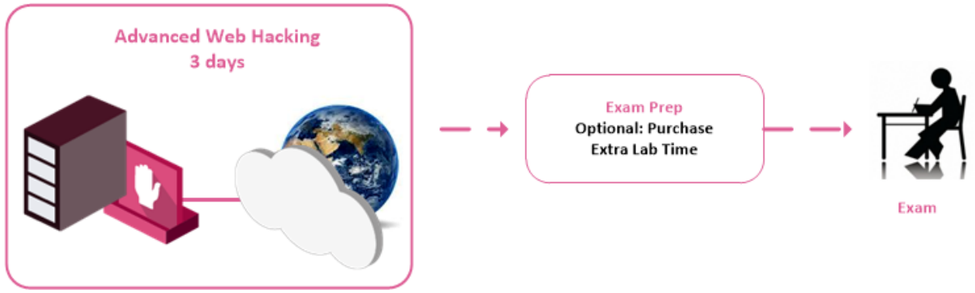
The team has built a state-of-the-art Hacklab and has recreated security vulnerabilities based on real penetration tests and vulnerabilities in the field; vulnerabilities that have gone undetected by modern scanners, or have had less visibility . Attendees will have access to the Hacklab for 30 days after the course.

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.

Requirement: Bring a laptop with admin/root access



BLACK BELT EDITION

Available remotely to Check Point customers and partners

Class size up to 16 students on-site

Authentication Bypass
Token hijacking attacks
Logical bypass / Boundary conditions

SAML / OAUTH 2.0 / AUTH-0 / JWT Attacks
JWT 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
API authorization bypass

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
Ruby/ERB template injection
Exploiting code injection over OOB channels
Ruby / ERB template injection
Exploiting code injection over OOB channel

Server Side Request forgery (SSRF)
SSRF to call internal files
SSRF to query internal networks

Unrestricted file upload
Malicious file extensions
Circumventing file validation checks

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

In collaboration with

NOT SO SECURE
A Claranet Group Company