Maslak Mahallesi, Maslak Meydan Sk. No:5. Spring Giz Plaza. Maslak/İstanbul
+90 212 282 7700 - info@bilginc.com

Advanced Web Hacking

Learn via: **Classroom/Virtual**

Duration: **3 Days**

Overview

NotSoSecure is pleased to launch their much awaited advanced Web Hacking course. Much like the Advanced Infrastructure Hacking class, this course talks about a wealth of hacking techniques to compromise web applications, APIs and associated end-points. This three day course will focus on specific areas of app-sec and on advanced vulnerability identification and exploitation techniques (especially server side flaws).

The course allows attendees to practice some neat, new and ridiculous hacks which affected real life products and have found a mention in real bug-bounty programs. The vulnerabilities selected for the course either typically go undetected by modern scanners or the exploitation techniques are not so well known.

Attendees can also benefit from a state-of-art Hacklab and we will be providing 30 days lab access after the course to allow attendees more practice time. This fast-paced course, gives attendees an insight into Advanced Web Hacking, the NotSoSecure team has built a state of the art Hacklab and recreated security vulnerabilities based on real life Pen Tests and real bug bounties seen in the wild.

Prerequisites

Whoever works with or against the security of modern web applications will enjoy and benefit from this course. This is not a beginner class and attendees are expected to have a good prior understanding of the OWASP top 10 issues to gain maximum value from the class. Further to this, the course does not cover all AppSec topics and focuses only on advanced identification and exploitation techniques of the vulnerabilities shown on the right.

This course will be suitable for delegates Interested in the SANS Institute course SEC542: Web App Penetration Testing and Ethical Hacking

What You Will Learn

- Authentication bypass
- Saml / oauth 2.0 / auth-0 / jwt attacks
- Password reset attacks
- Breaking crypto
- Business logic flaws / authorization flaws
- Sql injection
- Remote code execution (rce)
- Server side request forgery (ssrf)
- Unrestricted file upload
- Attack chaining

Outline

AUTHENTICATION BYPASS

- Token Hijacking attacks
- SQL column truncation attack
- 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 CRYPTO

- 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 Serialisation 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 network
- 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
- A Collection of weird and wonderful XSS and CSRF attacks

ATTACK CHAINING

- Combining Client-side and Server-side attacks to
- steal internal secrets
- B33r 101