Advanced Web Hacking

4 Days (Fast Track available)

BLACK BELT EDITION 2020

Much like our popular Advanced Infrastructure Hacking class, this class talks about a wealth of hacking techniques to compromise web applications, APIs, cloud components and other associated end-points. This class focuses on specific areas of appsec and on advanced vulnerability identification and exploitation techniques (especially server side flaws). The class 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 class either typically go undetected by modern scanners or the exploitation techniques are not so well known.

Note: Attendees will also benefit from a state-of-art Hacklab and we will be providing free 30 days lab access after the class to allow attendees more practice time.

Who Should Attend

- **Web developers**
- **SOC analysts**
- **Intermediate level penetration testers**
- **DevOps engineers, network engineers**
- **Security architects**
- **Security enthusiasts**
- **Anyone who wants to take their skills to the next level**

Delegate Requirements

Students must bring their own laptop and have admin/root access on it. The laptop must have a virtualization software (virtualbox / VMWare) pre installed. A customized version of Kali Linux (ova format) containing custom tools, scripts and VPN scripts for the class will be provided to the students. The laptop should have at least 4 GB RAM and 20 GB of free disk space dedicatedly for the VM. Users are also encouraged to familiarize themselves with Burp Suite https://portswigger.net/burp/communitydownload to gain maximum out of the class.

Key Takeaways

- The latest hacks in the world of web hacking. The class content has been carefully handpicked to focus on some neat, new and ridiculous attacks.
- We provide a custom kali image for this class. The custom kali image has been loaded with a number of plugins and tools (some public and some NotSoPublic) and these aid in quickly identifying and exploiting vulnerabilities discussed during the class.
- The class is taught by a real Pen Tester and the real-world stories shared during the class help attendees in putting things into perspective.

Delegates Receive

Access to a hacking lab not just during the course but for 30 days after the class too. This gives them plenty of time to practice the concepts taught in the class. Numerous scripts and tools will also be provided during the training, along with student handouts.

Our courses also come with detailed answer sheets. That is a step by step walkthrough of how every exercise within the class needs to be solved. These answer sheets are also provided to students at the end of the class.

Course Outline

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

NotSoSecure part of claranet cyber security

For more information:

UK: +44 (0)1223 653 193
US: +1 (628) 200-3053/3052
Email: contact@notsosecure.com
Visit: notsosecure.com

Advanced Web Hacking

4 Days (Fast Track available) (Continued)

BLACK BELT EDITION 2020

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

B33R-101

NotSoSecure part of claranet cyber security

For more information:

UK: +44 (0)1223 653 193
US: +1 (628) 200-3053/3052
Email: contact@notsosecure.com
Visit: notsosecure.com