NOT SO SECURE
A Claranet Group Company

claranet cyber security

Advanced Web Hacking
2019 Edition

Advanced Web Hacking class talks about a wealth of hacking techniques to compromise web applications, APIs and associated end-points. This class focuses on specific areas of app-sec and on advanced vulnerability identification and exploitation techniques (especially server side flaws). This hands-on class covers neat, new and ridiculous hacks which affected real life products and have found a mention in real bug-bounty programs. In this class vulnerabilities selected are ones that typically go undetected by modern scanners or the exploitation techniques are not so well known.

This training is an action-packed web hacking class exploiting modern web application vulnerabilities such as SSRF, Template Injection, 2nd Order SQLi, Deserialization, Crypto flaws and more. Attacking authentication schemes such as JWT, SAML, OAuth. Learning esoteric Out-of-Band techniques and attack chaining.

Class Outline

Module 1: Attacking Conventional and Modern Authentication Schemes (SAML, JWT. Token Hijacking attacks and more)

Module 2: Password Reset Attacks

Module 3: Business Logic Flaws / Authorization flaws

Module 4: XML External Entity (XXE) Attacks

Module 5: Breaking Crypto

Module 6: Deserialization Attacks on multiple web technologies

Module 7: SQL Injection Attacks

Module 8: Unrestricted File Upload

Module 9: Server-Side Request Forgery (SSRF)

Module 10: Attacking cloud providers

Module 11: Attacking Hardened Content Management System

Module 12: Miscellaneous Topics

Is this class right for you?

If you wonder:

- Are there a ways to effectively exfiltrate data using Out of Band Techniques for certain Vulnerabilities?
- Are there ways to pen test encrypted parameters to find vulnerabilities?
- Are there ways to bypass SSO functionalities?
- Are there ways to find SQL injection vulnerabilities not detected by Automated tools?
- Are there ways to break weak crypto implementations?
- Would there be an effective way to bypass password reset functionalities?
- What are the different things i can do with an SSRF vulnerabilities?
- How can deserialization vulnerabilities be exploited?

Then you have come to the right place. Advanced Web hacking teaches you all of these.

Who Should Attend

- Web Developers , SOC Analysts who wonder types of attacks Penetration Testers use to find flaws in the applications
- Entry/Intermediate level Penetration Testers who want to know; what's next? What are the advanced level attacks through which they can exploit vulnerabilities?
- Network Engineers, Security Architects, enthusiasts who want to stay updated with the latests trends in Web application Hacks
- Any technical person having a basic knowledge of how web applications work

On Completion of this class Attendees will be able to:

Obtain a hands-on introduction to application security vulnerabilities like SQL Injection, XXE, Authentication and authorization flaws on our purposely built vulnerable web applications.

- Identify and perform Out of Band Injections for Vulnerabilities like SQL Injection and XXE to exfiltrate Data
- Learn how to perform Remote Code execution and find Deserialization Vulnerability
- Lastly learn how to attack weak key cryptography and how to fuzz and find vulnerabilities in completely encrypted parameters

What Students Receive

- Students can access our online lab which is purposely riddled with multiple vulnerabilities
- Students will receive demonstrations and hands-on practice of the vulnerabilities to better understand and grasp the issues

- Numerous scripts and tools for advanced attacks
- A PDF copy of all class materials used during the class including instructor slide deck, tool cheat sheets and walkthrough guides
- Access to NotSoSecure's Advanced Web Hacking lab for 30 days after class completion

Prerequisites

The requirement for this class is that you bring your own laptop with at least 4 GB RAM and 20 GB of free disk space and have admin/root access, along with the capability to run Kali Linux Image from Virtual Box. Familiarity with Burp Suite will be beneficial for this class.

Hands-on Training

Advanced Web hacking is an interactive hands-on training class, here is an outline of few of the activities students will carry out:

- Bypassing Custom Authentication
- Attacking JWT to bypass authentication
- Understanding Password reset flaws and exploiting them
- Bypassing the application's Business logic flaws and exploiting them
- Perfoming Out of Band XXE attacks
- Perform Out of Band SQL injection attacks
- Practicing Second order SQL injection
- Identifying and exploiting deserialization vulnerabilities
- Identifying and exploiting vulnerabilites leading to RCE

For more information contact
+44 1223 653193
contact@notsosecure.com