ENCIPHERS

WEB APPLICATION HACKING MASTERCLASS

A Real World Mobile App Hacking Training

By the creators of **Mobexler**

Private & Confidential

ENCIPHERS

Demystifying Security

Having over a decade of experience in penetration testing of web, mobile & cloud, we love to teach what we do. There is no better way to teach hacking than explaining the exploits & vulnerabilities through real life case studies and emulating the same.

What’s so unique about our training?

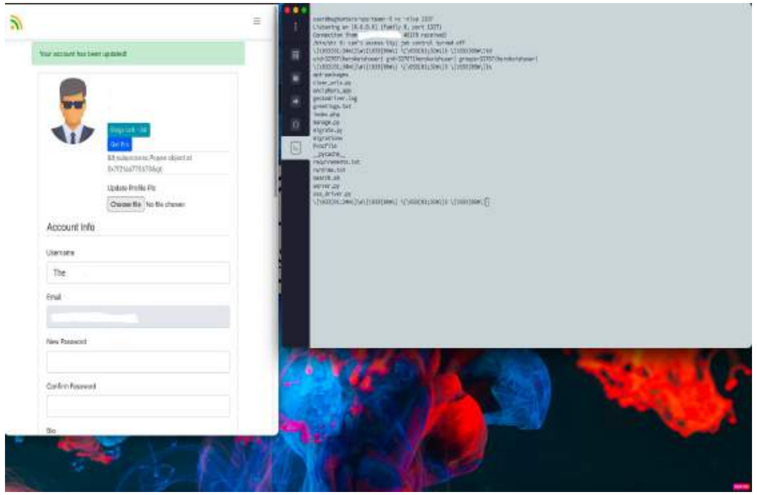
Unlike most of other trainings, we have designed a lab which is as real world as it can get. We have literally created a fake company with several assets to hack, all on the internet. These assets have vulnerabilities which have been previously discovered.

Web Application Testing Masterclass

- A **fully hands on training** designed to teach the skills required for penetration testing of web applications. With tons of real world vulnerabilities, simulated through a state-of-art lab environment, attendees will get to experience how to find & exploit vulnerabilities, hidden deep in the cute looking web apps.

- From **cross site scripting, insecure direct object reference to remote code execution. The training takes on an exciting journey of hacks and exploits.**

- All the theory is followed by some **hands-on challenges, to be solved on the lab environment (no virtual machine setup), and a platform to compete in CTF like fashion, but instead of definite flags to find, you have to actually hack the apps.**



Your account has been updated!

Update Profile Pic

Choose file No file chosen

Account Info

Username

The

Email

[redacted]

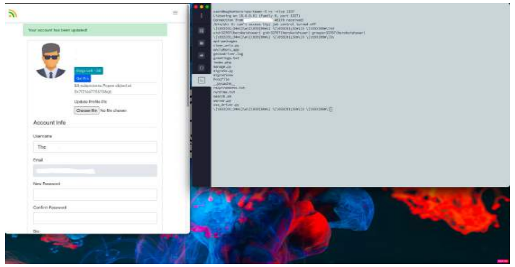
New Password

Confirm Password

Bio

```
[illegible]
Listening on [0.0.0.0] (family 0, port 1337)
Connection from [redacted] received!
/bin/sh: 0: can't access tty; job control turned off
[illegible]
manage.py
migrate.py
migrations
Procfile
__pycache__
requirements.txt
runtime.txt
server.py
[illegible]
```

Training Assets & Apps



Training Lab Application(s): Modern Web App, APIs, Servers, Domains

VantagePoint: A invite only platform to solve the training challenges & compete for leaderboard

Chat Platform: A dedicated chat platform for active discussion & queries on the topic

Course Abstract

Web applications grow in complexity every day and it is extremely difficult to manage them from a security perspective. This training is designed to teach different types of vulnerabilities in web applications and the techniques used to find and exploit them.’

This real-time immersive virtual-lead training uses a combination of lectures, real-world experiences, and awesome hands-on exercises to teach you the skill set required for findings and exploiting vulnerabilities in modern web applications/APIs.

At the end of the training, the attendees will be able to:

- Perform full penetration test of web apps
- Understand the concept behind web app vulnerabilities and how to find & exploit them
- Experience of how real-world web application vulnerabilities are discovered and exploited

Unique Features Of Training

➔ **Access to lab environment:** All the training participants will be given a complimentary access to the lab environment for practicing the skills, for one month.

➔ **Dedicated Chat Platform:** Attendees will have access to a dedicated chat platform (channel), to discuss, and ask queries, event after the training.

➔ **VantagePoint:** Attendees will be competing in a CTF like fashion on an invite only platform, but instead of finding flags, they will be finding and exploiting real world vulnerabilities.

➔ **Training content:** All the content used in this training will also be provided to all the participants, i.e. presentation, POC apps, notes, exploit codes, solution sheet for challenges etc.

Course Curriculum

Day 1:

- Setting up the lab access (SSH & RDP)
- Cross-Site Scripting
  - Stored XSS
  - DOM XSS
  - Blind XSS
  - Stored XSS
- Understanding authentication & authorization
- Basics of JSON Web Tokens
- Hacking the authorization
- Cracking the JWT secret
- Insecure Direct Object Reference
- SQL Injection:
  - SQL Injection in web apps
  - Exploiting SQL injection in GraphQL
- XML External Entity Attack
- File extraction with XXE
- Out Of Band exploitation of XXE

Day 2:

- Server-Side Request Forgery
- SSRF exploitation scenarios
- Exploiting SSRF for data ex-filtration
- Server-Side Template Injection:
- Testing for SSTI vulnerabilities
- Getting reverse shell with SSTI
- Remote file inclusion
- RFI to reverse shell
- Remote code execution:
- Hacking Insecure Jenkins
- Command Injection
- Command injection to reverse shell
- Insecure De-serialization
- Reverse shell with insecure de-serialization
- Solving challenges on VantagePoint & Feedback

Why Choose Us?

Battle Tested Labs

The labs have been battled tested. We do not have failed demos or failed challenges in our training. Everything works like a charm, everytime.

50+ Training

We have delivered 50+ training on Web & Mobile hacking, worldwide.

Incredible Response

The feedback to all our trainings have been incredibly awesome. Twitter & LinkedIn is filled with lovely posts by the training attendees.

THANK YOU

Contact us

🌐 www.enciphers.com

✉ hello@enciphers.com