CENTER FOR CYBER SECURITY TRAINING

Full-Stack Pentesting Laboratory

Abstract

Modern IT systems are complex and it's all about full-stack nowadays. To become a pentesting expert, you need to dive into full-stack exploitation and gain a lot of practical skills. That's why I created the Full-Stack Pentesting Laboratory.

For each attack, vulnerability and technique presented in this training there is a lab exercise to help you master full-stack pentesting step by step. What's more, when the training is over, you can take the complete lab environment home to hack again at your own pace.

The instructor has found security bugs in many companies including Google, Yahoo, Mozilla, Twitter and in this training and he'll share my experience. The content of this training has been carefully selected to cover the topics most frequently requested by professional penetration testers.

Learning Objectives

After completing this training, you will have learned about:

- Hacking cloud applications
- API hacking tips & tricks
- Data exfiltration techniques
- OSINT asset discovery tools
- Tricky user impersonation
- Bypassing protection mechanisms
- CLI hacking scripts

- Interesting XSS attacks
- Server-side template injection
- Hacking with Google & GitHub search engines
- Automated SQL injection detection and exploitation
- File read & file upload attacks
- Password cracking in a smart way
- Hacking Git repos
- XML attacks
- NoSQL injection
- HTTP parameter pollution
- Web cache deception attack
- Hacking with wrappers
- Finding metadata with sensitive information
- Hijacking NTLM hashes
- Automated detection of JavaScript libraries with known vulnerabilities
- Extracting passwords
- Hacking Electron applications
- Establishing reverse shell connections
- RCE attacks
- XSS polyglot
- and more …

Target Audience

Penetration testers, red and blue team members, SOC analysts, software developers, security engineers

Special bonus

The ticket price includes FREE access to my 6 online courses:

- Fuzzing with Burp Suite Intruder
- Exploiting Race Conditions with OWASP ZAP
- Case Studies of Award-Winning XSS Attacks: Part 1
- Case Studies of Award-Winning XSS Attacks: Part 2
- How Hackers Find SQL Injections in Minutes with Sqlmap
- Web Application Security Testing with Google Hacking

What Students Will Receive

Students will be handed in a VMware image with a specially prepared lab environment to play with all attacks, vulnerabilities and techniques presented in this training (*). When the training is over, students can take the complete lab environment home to hack again at their own pace.

(*) The download link will be sent after signing a non-disclosure agreement and subscribing to my newsletter.

Requirements

Students will need:

- A laptop with 64-bit operating system, at least 8 GB RAM, 35 GB free hard drive space, administrative access, ability to turn off AV/firewall and VMware Player/Fusion installed (64-bit version). Prior to the training, make sure there are no problems with running 64-bit VMs (BIOS settings changes may be needed).

Students' Knowledge Pre-Requisites:

To get the most of this training intermediate knowledge of pentesting and web application security is needed. Students should have experience in using a proxy, such as Burp Suite Proxy, or similar, to analyze or modify the traffic.

Instructor's Bio

Dawid Czagan is an internationally recognized security researcher and trainer. He is listed among top hackers at HackerOne. Dawid Czagan has found security bugs in Apple, Google, Mozilla, Microsoft and many others. Due to the severity of many bugs, he received numerous awards for his findings.

Dawid Czagan shares his offensive security experience in his hands-on trainings. He delivered trainings at key industry conferences such as Hack In The Box (Amsterdam), CanSecWest (Vancouver), 44CON (London), Hack In Paris (Paris), NorthSec (Montreal), HITB GSEC (Singapore), BruCON (Ghent) and for many corporate clients. His students include security

specialists from Oracle, Adobe, ESET, ING, Red Hat, Trend Micro, Philips and government sector (references are attached to Dawid Czagan's LinkedIn profile (https://www.linkedin.com/in/dawid-czagan-85ba3666/). They can also be found here: https://silesiasecuritylab.com/services/training/#opinions).

Dawid Czagan is the founder and CEO at Silesia Security Lab. To find out about the latest in his work, you are invited to subscribe to his newsletter (https://silesiasecuritylab.com/newsletter) and follow him on Twitter (@dawidczagan) and LinkedIn (https://www.linkedin.com/in/dawid-czagan-85ba3666/).