CENTER FOR
CYBER SECURITY
TRAINING

Bug Hunting Millionaire: Mastering Web Attacks with Full-Stack Exploitation

Abstract

HackerOne bug hunters have earned $20 million in bug bounties until 2017 and they are expected to earn $100 million by the end of 2020. Some of HackerOne customers include the United States Department of Defense, General Motors, Uber, Twitter, and Yahoo. It clearly shows where the challenges and opportunities are for you in the upcoming years. What you need is a solid technical training by one of the Top 10 HackerOne bug hunters.

Modern web applications are complex and it’s all about full-stack nowadays. That’s why you need to dive into full-stack exploitation if you want to master web attacks and maximize your payouts. Say ‘No’ to classical web application hacking. Join this unique hands-on training and become a full-stack exploitation master.

Learning Objectives

After completing this training, you will have learned about

- REST API hacking
- AngularJS-based application hacking
- DOM-based exploitation
- bypassing Content Security Policy
- server-side request forgery
- browser-dependent exploitation
- DB truncation attack

- NoSQL injection
- type confusion vulnerability
- exploiting race conditions
- path-relative stylesheet import vulnerability
- reflected file download vulnerability
- subdomain takeover
- and more…

Target Audience

Penetration testers, ethical hackers, bug hunters, security researchers/consultants/engineers

What students will receive

Students will be handed in a VMware image with a specially prepared testing environment to play with the bugs. What's more, this environment is self-contained and when the training is over, students can take it home (after signing a non-disclosure agreement) to hack again at their own pace.

Special bonus

The ticket price includes FREE access to Dawid Czagan's 6 online courses:

- Start Hacking and Making Money Today at HackerOne
- Keep Hacking and Making Money at HackerOne
- Case Studies of Award-Winning XSS Attacks: Part 1
- Case Studies of Award-Winning XSS Attacks: Part 2
- DOUBLE Your Web Hacking Rewards with Fuzzing
- How Web Hackers Make BIG MONEY: Remote Code Execution

REQUIREMENTS

Student Machine/ Laptop Requirements

Students will be handed in a VMware image with a specially prepared testing environment to play with the bugs. What's more, this environment is self-contained and when the training is over, students can take it home (after signing a non-disclosure agreement) to hack again at their own pace.

Students will need:

- Laptop with 64-bit operating system, at least 4 GB RAM (8 GB preferred), 35 GB free hard drive space, USB port (2.0 or 3.0), wireless network adapter, 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).
- Please also make sure that you have Internet Explorer 11 installed on your machine or bring an up-and-running VM with Internet Explorer 11

Students Knowledge Pre-Requisites:

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

Bio

Dawid Czagan is an internationally recognized security researcher and trainer. He is listed among Top 10 Hackers (HackerOne). Dawid Czagan has found security vulnerabilities in Google, Yahoo, Mozilla, Microsoft, Twitter and other companies. Due to the severity of many bugs, he received numerous awards for his findings.

Dawid Czagan shares his security bug hunting experience in his hands-on trainings “Hacking Web Applications – Case Studies of Award-Winning Bugs in Google, Yahoo, Mozilla and More” and “Bug Hunting Millionaire: Mastering Web Attacks with Full-Stack Exploitation”. He delivered security training courses at key industry conferences such as Hack In The Box (Amsterdam), CanSecWest (Vancouver), 44CON (London), Hack In Paris (Paris), DeepSec (Vienna), 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.

Dawid Czagan is a founder and CEO at Silesia Security Lab – a company which delivers specialized security testing and training services. He is also an author of online security courses.