TRAINING TITLE

Black Belt Pentesting / Bug Hunting Millionaire: Mastering Web Attacks with Full-Stack Exploitation (100% Hands-On, Live Online Training)

OVERVIEW

Have you ever thought of hacking web applications for fun and profit? How about playing with authentic, award-winning security bugs identified in some of the greatest companies? If that sounds interesting, join this unique 100% hands-on training!

I will discuss security bugs found in a number of bug bounty programs (including Google, Yahoo, Mozilla, Twitter and others). You will learn how bug hunters think and how to hunt for security bugs effectively.

To be successful in bug hunting, you need to go beyond automated scanners. If you are not afraid of going into detail and diving into full-stack exploitation, then this training is for you.

KEY LEARNING OBJECTIVES

After completing this training, you will have learned about:

- browser-dependent exploitation
- DOM-based exploitation
- exploiting race conditions
- remote cookie tampering
- bypassing Content Security Policy
- exploiting type confusion
- exploiting parameter pollution
- hijacking tokens via PDF
- exploiting DB truncation
- exploiting NoSQL injection
- using wrappers to launch RCE
- RCE via serialization/deserialization
- exploiting path-relative stylesheet import
- exploiting reflected file download (various browsers)
- AngularJS-based application hacking
- non-standard XSS attacks
- hacking with polyglot
- subdomain takeover
- REST API hacking
- XML attacks
- advanced clickjacking in modern browsers
- advanced SSRF with gopher protocol
- protection bypass with Shift_JIS encoding
- and more …

This hands-on training was attended by security specialists from Oracle, Adobe, ESET, ING, Red Hat, Trend Micro, Philips, government sector and it was very well-received. Recommendations are attached to my LinkedIn profile (https://www.linkedin.com/in/dawid-czagan-85ba3666/). They can also be found here (https://silesiasecuritylab.com/services/training/#opinions).

WHAT STUDENTS WILL RECEIVE

Students will be handed in a VMware image with a specially prepared testing environment to play with all attacks presented in this training. When the training is over, students can take the complete lab environment home (after signing a non-disclosure agreement) to hack again at their own pace.

WHAT STUDENTS SHOULD KNOW

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.

WHAT STUDENTS SHOULD BRING

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). 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 (you can get it here: https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/).

INSTRUCTOR

Dawid Czagan is a 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+CyberWeek (Abu Dhabi), 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/subscribe-to-my-newsletter/) and follow him on LinkedIn (https://www.linkedin.com/in/dawid-czagan-85ba3666/).