Black Belt Pentesting / Bug Hunting Millionaire: Mastering Web Attacks with Full-Stack Exploitation Training

Duration: **2 Day**

BILGINÇ
IT Academy
info@bilginc.com
bilginc.com

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 100% hands-on training is for you. There is a lab exercise for each attack presented in this training + students can take the complete lab environment home after the training session.

Watch 3 exclusive videos (~1 hour) to feel the taste of this training:

- **Exploiting Race Conditions**
- **Token Hijacking via PDF File**
- **Bypassing Content Security Policy**

Black Belt Pentesting / Bug Hunting Millionaire: Mastering Web Attacks with Full-Stack Exploitation Training

Duration: **2 Day**

BILGINÇ
IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

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
- hacking with wrappers
- subdomain takeover
- remote cookie tampering
- non-standard XSS attacks
- hijacking tokens via PDF
- XML attacks
- deserialization attacks
- HTTP parameter pollution
- bypassing XSS protection
- hacking with polyglot
- clickjacking attack
- window.opener tabnabbing attack
- RCE attacks
- and more...

Outline

What Students Will Receive

Students will be handed in a VMware image with a specially prepared testing environment to play with all bugs 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 Dawid Czagan's newsletter.

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

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- DOUBLE Your Web Hacking Rewards with Fuzzing (aka Fuzzing with Burp Suite Intruder)
- How Web Hackers Make BIG MONEY: Remote Code Execution

What Students Say About This Training

This training has been very well-received by students around the world. References are attached to **Dawid Czagan's LinkedIn profile**. **They can also be found here** - training participants from companies such as Oracle, Adobe, ESET, ING, ...

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 x86_64 VMs. 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.

Instructor

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), SINCON (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**. **They can also be found here**).

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** and follow him on Twitter (**@dawidczagan**), **YouTube**, and **LinkedIn**.