/Rooted

Black Belt Pentesting / Bug Hunting Millionaire

Mastering Web Attacks with Full-Stack Exploitation

(in ENGLISH)

MADRID

7 & 8 March 2023

TRAINING BROCHURE

/Rooted

6-8 March

Three days for trainings and workshops

HOTEL Eurostars iHotel
Pozuelo de Alarcón

9-11 March

Papers presented by international speakers and technical experts.

KINEPOLIS
Pozuelo de Alarcón

Presentation

- **Mission:** We want to share knowledge, attract different cultures, expose local talent and make a difference.
- **Vision:** be responsible by doing something different, sharing culture and building a knowledge network. Being an honest, reliable, beneficial event and establishing alliances and collaborations with partners, clients and competitors.
- **Our winning culture and values live:** collaboration, diversity, talent everywhere, passion, quality and customer focus (every person who attends our conferences).

/Rooted

Teacher: Dawid Czagan

Dawid Czagan (@dawidczagan) is an internationally recognized security researcher and trainer. He is listed among top hackers at 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 “Black Belt Pentesting / 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), 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 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. To find out about the latest in Dawid Czagan’s work, you are invited subscribe to his newsletter (https://silesiasecuritylab.com/newsletter) and follow him on Twitter (@dawidczagan) and LinkedIn (https://www.linkedin.com/in/dawid-czagan-85ba3666/).

/Rooted

Overview

HackerOne bug hunters have earned over $100 million in bug bounties so far. 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 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.

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

- Exploiting Race Conditions: https://www.youtube.com/watch?v=lLd9Y1r2dhM
- Token Hijacking via PDF File: https://www.youtube.com/watch?v=AWplef1CyQs
- Bypassing Content Security Policy: https://www.youtube.com/watch?v=tTK4SZXB734

/Rooted

Key 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
- XML attacks
- deserialization attacks
- HTTP parameter pollution
- bypassing XSS protection
- clickjacking attack
- window.opener tabnabbing attack
- RCE attacks
- and more…

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
- DOUBLE Your Web Hacking Rewards with Fuzzing
- 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 (https://www.linkedin.com/in/dawid-czagan-85ba3666/). They can also be found here (https://silesiasecuritylab.com/services/training/#opinions) - 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.

/Rooted

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).

Price

- The final Price for this **Bootcamp + ticket** for RootedCON is **1250 €**

- **You can register and pay here: https://reg.rootedcon.com**

IMPORTANT:

It is required a mínimum of eleven **(11)** students.

FAQ

- Where is the training held?
  - Unlike the RootedCON Congress, the trainings are held at the Eurostarts i-Hotel
  - Here you can find the map of the area: Google Maps
- What is the difference between BootCamp and RootedLab?
  - We differentiate the training by hours of training. A RootedLab has 8 hours of training, while a BootCamp has between 16-24.
- What about the timing?
  - The training begins at 9 in the morning, but try to be a bit earlier to be able to get registered and have your laptop ready. The first day we do recommend to be at 8 a.m. :)
  - Trainings usually end between 7:00 p.m. and 8:00 p.m.
- How can I register?
  - For registration, go to the RootedManager: https://reg.rootedcon.com. There, once registered you can select the training and pay directly. Once the training is given, you can request the invoice by following the steps indicated.
- Can I pay with wire transfer?
  - Yes, from the RootedManager you can manage the payment.
- Does the training include food?
  - The training does not include food. But there are several options in the area, and the teacher will give you more information.

/Rooted

Contacto:

info@rootedcon.com