

**/Rooted®**



# Web Hacking 101 & Bug Bounty Hunting

Led by **Prash Somaiya**  
*Security Solutions Architect @ HackerOne*

**MADRID**

2<sup>nd</sup> - 4<sup>th</sup> March 2020

**TRAINING DOSSIER**

# /Rooted<sup>®</sup>

## 2-4 March

*Three days of workshops  
and trainings*

*HOTEL Eurostars iHotel  
Pozuelo de Alarcón*

## 5-7 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:** to be responsible by doing something different, sharing culture and building a knowledge network. Be an honest, reliable, beneficial event and establish alliances and collaborations with partners, customers and competitors.
- **Our winning culture and our live values:** collaboration, diversity, talent everywhere, passion, quality and focus on customers (each person attending our congresses).

# Meet your trainers

---



🇬🇧 **Prash Somaiya**, Lead Instructor  
*Security Solutions Architect @ HackerOne*

Prash manages some of the largest bug bounty programs on the internet, including: **Verizon Media**, **Airbnb**, **Uber** and more. Prash has years of experience in the cybersecurity industry and, as an **ethical hacker**, has uncovered vulnerabilities in organisations such as **Facebook**, **US Dept. of Defense** and **StackOverflow**.



🇪🇸 **Carlos Rivero Molina**, Teaching Assistant  
*Senior Pentester @ Deloitte*

Carlos has a strong red-team and pentesting background. Having completed his **OSCP**, Carlos has found great success in the **bug bounty** realm, reporting vulnerabilities to organisations such as **AT&T**, **Verizon Media**, **monday.com**, and more.

# What will you learn?

---

**With world class instruction, you will hone your hacking skills, testing them out on a custom built vulnerable platform.**

- **The most common vulnerabilities found in the real world today, including**
  - Cross-Site Scripting (XSS)
  - Server-Side Request Forgery (SSRF)
  - Cross-Site Request Forgery (CSRF)
  - Insecure Direct Object Reference (IDOR)
  - Remote Code Execution (RCE)
  - SQL Injection
- **Develop your own bug hunting methodology**
  - Don't just understand the theory behind a vulnerability, we'll teach you how to exploit it

## What will you learn? (cont.)

---

- **Use industry standard tools**
- **How to write vulnerability reports**
  - Demonstrating impact if it were to get into the hands of a malicious actor
  - Assessing vulnerability severity (CVSS)
- **Recon - discover what's out there!**
  - Certificate transparency
  - Sensitive data leaked in GitHub and other sources
  - Fingerprinting
  - Bruteforcing
- **Finding the right program for you**
  - If you're interested in bug bounty, we'll help you find the program(s) that are right for you!

# Training Platform

## Apply the theory, learn by doing.

After we learn about each vulnerability type, you will be given the chance to hunt for it in our custom-built vulnerable training platform, **BUGBANK**.

The practical labs will really enforce the theory, allowing you to experience the thrill of finding a real vulnerability!

The screenshot shows the 'Activity' page for a user named 'BUGBANK'. The page has a dark header with navigation links: Overview, Contacts, Support, and API. A 'Transfer money' button is in the top right. The main content area shows a balance of \$19750.00 and a table of transactions for the account with IBAN NL84INTI6998399955.

Receipient	Description	Amount
test_2	Incoming	+50.00 \$
test_18	<script>alert('xss test')</script>	-50.00 \$
test_19	This is a test	-150.00 \$
test_19	Happy birthday!	-100.00 \$

The screenshot shows the 'Contacts' page for a user named 'BUGBANK'. The page has a dark header with navigation links: Overview, Contacts, Support, and API. A 'Transfer money' button is in the top right. The main content area shows a table of contacts with columns for Name, IBAN, and edit.

Name	IBAN	edit
test_2	NL84INTI6998399955	

# Target Audience & Previous Knowledge Requirements

---

This workshop is primarily aimed at those **new to the world of web hacking** and/or bug bounty hunting. We will however cover some more advanced concepts, to keep those with some experience interested!

## Basic technical requirements:

- A high-level understanding of how the web works (DNS, HTTP)
- Familiarity with a terminal shell
- Familiarity with some basic hacking terminology
- Understand what a “bug bounty program” is

## Nice to haves:

- Some programming experience
- Some experience with non-web hacking
- Familiarity with Burp Suite
- Participation in CTFs
- Participation in a bug bounty program

# What you need

---

We will provide you with your very own instance of our training platform that you can access via the web. Other than the technical requirements listed on the slide below, you will need:

- **Your own laptop**
  - Windows/Linux/MacOS is fine as long as you have access to a terminal and administrator privileges
- **Burp Suite installed**
  - Community edition (free) is fine
  - Burp can be quite heavy, make sure your laptop is up to the task

# Content

---

We will spend three days learning to hack together, in a **collaborative environment** with a small group of students. There will be a mix of lecturing, practical labs, and **real-world activities**.

In addition to the technical side of web hacking, you will gain **soft-skills**, learning how to communicate effectively the impacts of vulnerabilities, assessing severity through the **CVSS** framework, and writing concise vulnerability reports. We will also look at how to find the right bug bounty programs for you.

# Agenda - Day One

---

- **Welcome & Introductions**
- **Getting started**
  - Browser developer tools
  - Burp Suite
- **XSS**
  - Reflected
  - DOM
  - Stored
  - Angular
- **CSRF**
- **IDOR**
- **Practical Labs**

# Agenda - Day Two

---

- **Local File Inclusion (LFI)**
- **SSRF**
  - Blind
  - via redirect
  - Extracting data
- **File upload vulnerabilities**
  - Unvalidated upload
  - Achieving RCE
  - Path traversal
- **SQL Injection**
  - Blind
  - Safe testing
  - Extracting data
- **Practical Labs**

# Agenda - Day Three

---

- **Recon**
  - Certificate transparency
  - Gathering data from various sources
- **Subdomain/DNS takeover**
- **Information Disclosure**
- **Weak Credentials**
  - Default configurations
- **Fingerprinting**
  - Exploiting vulnerable components
- **Report writing**
  - What's importing
  - Demonstrating impact
- **Bug bounty programs and platform overview**
- **Hack the world!**
  - CTF
- **Wrap-up**

# Experienced Instruction

---

## Learn from the experts.

Your lead instructor, Prash, has a vast amount of training experience, having taught classes targeted at a variety of abilities, including corporate training and university modules.

Prash has also been quoted in multiple tech publications on current cyber security news and events, including **BBC**, **ComputerWeekly**, **TechRadar**, **SC Magazine**, and more.

You can rest assured that complex topics will be broken down into easily digestible knowledge bites, ready for your consumption!

## Costs

---

- The final price of the Bootcamp + entrance to the RootedCON Congress is € 1250
- When registration is open for tickets to Congress, you will be sent a code to redeem your ticket.

**IMPORTANT:** A minimum of TEN (10) attendees are required for the course to take place.

## FAQ

---

- Where is the training held?
  - Unlike the RootedCON Congress, trainings are held at the Hotel 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 about 24 hours.
- What schedule does the training have?
  - The training begins at 9 in the morning, but try to be a little earlier to be able to facilitate the access, make the registration and have your laptop ready. The first day we recommend being at 8AM :)
  - Formations usually end between 7pM and 8PM.
- How can I register?
  - For registration, go directly to the [RootedManager](#). There, once registered you can select the training and pay directly. Once the training is completed you can request the invoice following the steps indicated in the Portal.
- Can I pay by bank wire?
  - Yes, from RootedManager you can manage the payment by bank wire.
- Does the training include food?
  - Trainings do not include food. But there are several options in the area, and the teacher will give you more information.

**/Rooted®**

