Zero Day Engineering

research & training

Zero Day Engineering Project
http://zerodayengineering.com

BROWSER EXPLOITATION

TRAINING OVERVIEW

This intensive 4-day / 1-month training course offers a systematic introduction to attacking web browsers, covering many core aspects of the field, and guided by cutting edge trends in real life browser exploits.

Curriculum is structured around a walk-through of exploiting major browsers: Mozilla Firefox, Apple Safari (scoped upstream WebKit), and Google Chrome. Taking a recently disclosed 0-day bug as a case study, attendees will follow the process of exploit development, starting with some minimal input and gathering relevant information as they go, up to a pre-shellcode, non-weaponized proof-of-concept exploit.

In the course of this training attendees will build a debugging and research platform for each browser, learn about the specifics of browser vulnerabilities and exploits, and explore various offensive opportunities that exist in this field, hands-on. Exploit case studies selected for this training target some of the most important attack surfaces, including JavaScript engine, DOM, and renderer sandbox.

AUDIENCE

Primary audience: **professional vulnerability researchers** who wish to specialize on or familiarize with browser exploit development.

Aspiring **bug bounty hunters** targeting browser and javascript engine will find the content of this training essential to their learning journey.

Advanced **browser exploitation experts** may find this training helpful as a refresher to catch up with recent developments in the field, as well as to expand their skillset into new attack surfaces that they are less familiar with.

PREREQUISITES

Mandatory:

- General vulnerability research and low-level hacking skills, as in Zero Day Vulnerability Research training, or equivalent knowledge;
- C++ & JavaScript.

Recommended:

- Assembly programming.

OBJECTIVES

This training will enable attendees to:

- Quickly and methodically acquire the system of knowledge required to **start attacking browsers**;
- Develop specialized **skills to dissect and exploit** advanced classes of vulnerabilities;
- Prepare a **debug-build and research platform** for all major browsers (a VM will be provided, as well as DIY instructions);
- Familiarize with **system internals and offensive research specifics** of different web browsers;
- Attack recently patched vulnerabilities exploited in **0-day attacks on browsers;**
- Make an informed decision regarding their **first browser target and attack vector** through exposure to relevant skills and "state of the art";
- Get **personalized insights** from the expert.

LEVELS & CERTIFICATION

Complexity: intermediate-advanced.
Certification: on-demand completion certificate.

TRAINING DETAILS

This training is designed as a first course in browser exploitation: a broad exploratory dive into the many challenges of the field. Attendees will be guided, by deliberate structure of content, to establish a systematic foundation of knowledge in the topic, as well as to decide which target they want to focus on.

Course Structure

Curriculum is based on the idea of learning through real-life case studies. Training will start with a full-day acquisition of core offensive concepts and skills which apply to all web browsers universally. Students will explore a generalized browser architecture and attack surface, common vulnerabilities and key exploit techniques, as well as core technologies that are commonly involved in browser exploits: such as JavaScript engine with WebAssembly and JIT compilers, DOM, IPC, CSP, GPU and graphics.

With that foundation in place, students will focus on modern web browser, one day at a time: including Mozilla Firefox, Apple Safari (WebKit), and Google Chrome. Starting with setting up a debugging platform on Linux as well as codebase orientation, and leading to hands-on walk-through of exploit development.

Both remote code execution and elevation of privilege or sandbox escape parts of the exploit chain will be considered, based on recently disclosed vulnerabilities. Extra attention will be given to javascript engines - namely, SpiderMonkey, JSC and v8 - as a particularly interesting attack surface of web browser.

Course Schedule

This is an intensive 4-day training which can be taught over an extended period of one month, allowing attendees to complete exercises in reasonable time, as well as to internalize new information in-between the live/online sessions. Anyone taking this training in self-paced mode should aim for same schedule.

Course Context

This training logically follows the universal knowledge of Zero Day Vulnerability Research course, taking it further to specialize on browser exploit development. After completing this course, the attendee will need to hone in on a particular attack surface in the browser, such as with JavaScript Engines Vulnerability Research training.

ABOUT THE INSTRUCTOR

Alisa Esage is an independent vulnerability researcher, as well as the founder of the Zero Day Engineering Project. With over 15 years of experience in low-level hacking, Alisa has risen to authority as an expert in 0-day vulnerabilities and binary exploitation, ensured by a strong record of technical hacking accomplishments, which include discovery of critical security issues in many popular software systems, as well as participating in Pwn2Own competitions.

As the Founder of Zero Day Engineering Project, Alisa guides offensive cybersecurity industry from ad hoc learning towards structured knowledge transfer. Under her leadership the project built a reputation as a unique professional training system, consistently receiving excellent course reviews, while fostering a loyal community of returning students eager for new trainings.

WHAT TO EXPECT?

Below is a selection of reviews from attendees of our different trainings.

Jael Koh · 1st
OSEE | OSCE3 | ZDE VR | Corelan Advanced | WISE | HackSys AKE
7mo · Edited ·

I'm excited to start off 2024 by completing Zero Day Engineering's Zero Day Vulnerability Research course.

Alisa Esage does an amazing job of taking something as complex and intimidating as Vulnerability Research and breaking it down into a comprehensive yet approachable curriculum.

One of my biggest takeaways from the course was Alisa's methodology for finding zero days in modern software. She teaches a systematic approach, using models of vulnerabilities, exploits, and application threats.

For example, by modeling the subsystems and threats of an application, I learned how to prioritize which subsystems to target and discover new conceptual attack vectors.

This course was both enjoyable and incredibly informative. I felt significantly better prepared for vulnerability research by the end, and I believe this systematic approach will help me avoid common pitfalls.

Overall, the course offers a powerful, systematized methodology that I haven't encountered before. It's also a great foundation for beginners interested in entering the field of Vulnerability Research.

I thoroughly enjoyed this course and am eagerly looking forward to its major upgrade later this year.

Peleg Hadar
@peleghd

The Hypervisor Exploitation One training by @alisaesage was simply incredible. Alisa is a great teacher with a lot of experience in the Vuln research field.
The Training contains practical exercises, it provides the knowledge you'll need for starting a Hypervisor vuln research!

Mohammad Hussam Alzeyyat · 2nd
Vulnerability Researcher/Cyber Security(Instructor,Labs Developer,Upwork Top Rated)/OSED,OSMR
2mo · Edited ·

I just finished the "Masterclass: Hacking open source fuzzers for smarter bughunting" from zerodayengineering.com by Alisa Esage.

The 4-hour training is an eye-opening to more advanced fuzzing and it's more oriented to learn how to customize the fuzzer for your own purpose and not to learn how to fuzz.

The masterclass focuses on AFL and WinAFL since those are the most powerful frameworks for fuzzing and explains the anatomy of fuzzing and the differences between the old generation fuzzers methodology and the new ones.

I don't think the masterclass is for beginners as much as for intermediate people or those with fuzzing experience.

Josh Pitts
@ausernamedjosh

The JavaScript Engines for Hackers by @zerodaytraining was great. Shortened the time to get familiar with V8. Thx @alisaesage!

Gal Z
@0xgalz

What a blast! Just finished @alisaesage 3 days deep technical Hypervisor Vulnerability Research course. Incredible and well designed with high quality materials.
Thanks for everything! Now, off to look at some VMM code \o/

Carlomagno A. · 2nd
Security Researcher
6mo ·

My review for #ZeroDayVulnerability course by Alisa Esage.

Alisa's does an amazing job at explaining more than decade of wisdom, insights and knowledge on a complex topic as Vulnerability Research in a 4 days course. The value of this information and training goes beyond just specific attack vectors or simplistic how-to's, it covers deep technical hands on training on real world vulnerable applications.

The segment of the course that I enjoyed the most was the establishment of the correct/appropiate mindset, definition of abstract models/frameworks, cognitive skills needed to better improve, this specific points matched with a well structured self-study roadmap will allow you to track your progress by establishing a feedback loop on the concepts that you need to improve upon to excel at Vulnerability Research.

rui
@fdiskyou

Alisa's training completely changed my mindset and the way I was looking at hypervisors. I highly recommend the Advanced Hypervisor Exploitation training. Actually, if you're interested in hypervisors it's mandatory.

Kapil Khot · 1st
Security Consultant/Penetration Testing | CoreLAN Exploit Dev | OSCP
7mo · Edited ·

Here's my review for #ZeroDayVulnerabilityResearch class offered by Zero Day Engineering. It's an intensive four days training where Alisa Esage shares some important tips from her Pwn2Own competition and decade long zero day research experience.

She walked us through real world application's code base to demonstrate how to indentify its subsystems and which one to prioritze for testing. Additionally, she walked us through some of the real world vulnerable code snippets from various enterpriese and real-world applications to demonstrate several bug classes such as memory corruption vulnerabilities, hardware bugs, and logic bugs etc. Furthermore, she also touched base on the security weaknesses of one of the memory safe languages and shared research tips on upcoming technologies.
One of the modules, Fuzzing Masterclass took us through the internals of coverage guided fuzzers and offered guidance on customizing them for applications not supported out of the box.

Overall, this course helps you build a zero day research mindset, guides you on what needs to be done, and forces you to figure out the most of the "how-to" part, which in my opinion is the best thing.

Mario Romero Serrano · 2nd
Senior Vulnerability Researcher - Cryptography Research Centre at Technology Innovation Institute (TII) | Cryptograp...
5mo ·

The last few months I have been enjoying and learning about vulnerability research from one of the best trainings available today.

The 4-day Zero Day Vulnerability Research course from Zero Day Engineering by Alisa Esage is not only exceptional on a technical level, but it also teaches you a methodology to follow, and personally, what for me is most valuable and concentrates Alisa's years of experience and knowledge: it introduces you to the mindset necessary for your vulnerability research to be successful.

I am already applying the knowledge I have acquired and I am eager to continue learning from her. I'm sure I'll be taking some more of her courses. For now, I will enjoy the course for the second time.

Don't miss the opportunity to do it:

Jacolon Walker
@call_eax

Big thanks to @alisaesage and @zerodaytraining for their top-notch training content! Just wrapped up a refreshing course with promising results - from bug discovery to exploitable vulnerability in just 9 days. Dive into my chronicle here: https://t.co/PCfqzCLs6B

Veer Singh · 1st
Security Practitioner
7mo ·

I recently (2023) completed the "Hypervisor Vulnerability Research" course by Alisa Esage, which provided a comprehensive exploration of virtualization technology and its security aspects. The course began with a clear introduction to virtualization technology, distinguishing between various types of hypervisors. We then explored the rich functionality of guest services, understanding their practical implementation and potential security challenges. The module on attacking guest services equipped us with valuable perspective on attack vectors, and the in-depth look at VirtualBox's implementation was insightful. Overall, this course is highly recommended for both beginners and experienced professionals looking to enhance their virtualization security skills. Here is a link to the course for anyone interested -
https://lnkd.in/g5N2gNmT

Training: Hypervisor Vulnerability Research
zerodayengineering.com

scryh
@scryh_

Just finished the @zerodaytraining hypervisor vulnerability research offline course by @alisaesage. Impressive research bundled into very well structured lessons, which are communicated in a clear and comprehensible way. Learned a lot. Thank you very much!
https://t.co/iW3UAGBtUq

Read more: Reviews & Buzz

FURTHER INQUIRIES

E-mail: contact@zerodayengineering.com.
Schedule and booking: zerodayengineering.com
Updates on social media: @zerodaytraining.