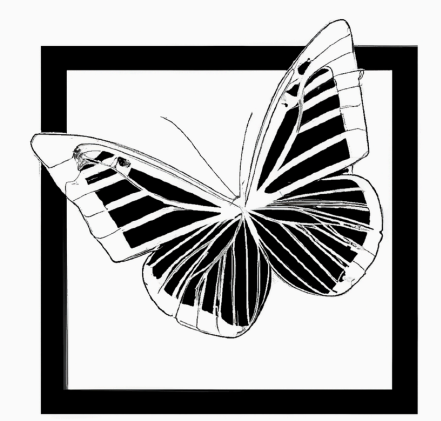

Zero Day Engineering

research & training

Zero Day Engineering LLC
http://zerodayengineering.com

BROWSER EXPLOIT DESIGN

TRAINING OVERVIEW

Advanced systems training for weaponized security research, targeting modern browsers and JavaScript engines through cutting edge theoretical models, structured frameworks and deep exploit case studies.

We start by introducing core models and technological stacks that apply universally to all browsers. Then overlay implementation-specific technicalities, focusing on one popular browser at a time: including Mozilla Firefox, Google Chrome and Apple Safari WebKit.

Practicalities are based on full-stack exploit engineering workflows, especially the roadmap from security patch or a fuzzed testcase to proof-of-concept exploit. Specific exploit case studies were selected to represent 80%+ of common bug classes attacking mainstream browsers in modern 0-day chains across RCE & EoP attack surfaces, including: a renderer DOM use-after-free, a JavaScript engine non-trivial type confusion in JIT compiler, and a sandbox escape via IPC memory corruption.

Once you see how the architecture folds, you won't need to guess where the next exploit is.

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 professional 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.

PREREQUISITES

Mandatory:

- General vulnerability modeling and exploit engineering, 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.
Certificate: available upon request.

PROGRAM AT A GLANCE

DAY 1. FOUNDATIONS

Concept:

- Core models, concepts and skills which apply to all browsers universally

Core models:

- Browser Attack Topology
- JavaScript Engine Map

Technological stack:

- Document Object Model (DOM) & WebAPI
- JavaScript Engine
- Graphics & Media
- Sandbox & EoP
- Browser exploit techniques - universal

Skills:

- OSINT & theoretical analysis
- Codebase navigation

DAY 2. MOZILLA FIREFOX

Concept:

- Firefox implementation technicalities and security aspects
- Exploit engineering practice: RCE in Renderer

Exploit:

- Use-after-free in Document Object Model stack of Web Platform API implementation
- Vector: JavaScript
- High impact 0-Day of 2023-2024
- Full stack walkthrough from patch to leak or code execution
- Testbed: either self-built (documentation provided) or our VM (self-hosted downloadable)
- Complexity: Medium - moderately isolated canonical use-after-free vulnerability

DAY 3. GOOGLE CHROME

Concept:

- Chrome implementation technicalities and security aspects under our models
- Exploit engineering practice: EoP - Sandbox Escape via IPC

Exploit:

- Memory corruption in a privileged process
- Vector: Mojo IPC, renderer JavaScript
- Canonical bug pattern, instance of 2020-2021
- Full stack walkthrough from patch to leak or code execution
- Testbed: either self-built (documentation provided) or our VM (self-hosted downloadable)
- Complexity: medium - mostly standard techniques in a deep attack surface

DAY 4. APPLE SAFARI & WEBKIT

Concept:

- WebKit implementation technicalities and security aspects under our models
- Exploit engineering practice: RCE - JavaScript Engine vulnerability

Exploit:

- Non-trivial logic issue in JIT compiler, convertible to Type Confusion
- High impact 0-Day of 2023-2024
- Full stack walkthrough from patch to leak or code execution
- Testbed: either self-built (documentation provided) or our VM (self-hosted downloadable)
- Complexity: hard - involves non-trivial modeling of exploit path

INDUSTRY FEEDBACK - ZERO DAY ENGINEERING 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

APPLICATIONS & INQUIRIES

E-mail: contact@zerodayengineering.com.
Public cohorts and booking: zerodayengineering.com
Socials: @zerodaytraining