Zero Day Engineering

research & intelligence

Zero Day Engineering LLC
http://zerodayengineering.com

CHROME FULL CHAIN EXPLOIT ENGINEERING

TRAINING OVERVIEW

Rigorous hands-on training in vulnerability research and exploit engineering for up-to-date Google Chrome and the Chromium project. The objective is the full chain: renderer RCE to sandbox escape, the highest-tier target of the Chromium VRP.

The methodology builds offensive research workflows that operate across the entire codebase, through labs and exercises demonstrating patch diffing, variant analysis, attack surface discovery, bug triage, CodeQL query construction, and exploitation with current mitigations; all AI-accelerated with public tools.

Beyond covering up-to-date Chromium security internals and building components of a full chain as worked examples of this year's bugs, this training leans into meta-cognitive skills, abstract models, and specific knowledge of LLM internals to facilitate advanced use of AI models.

All case studies are the author's first-hand VRP research and original frameworks.

AUDIENCE

Primary audience: **working researchers** who wish to focus on Chrome exploit development and ready to operate at a challenging level.

Aspiring **bug bounty hunters** targeting Chromium VRP will find the content of this training essential to their professional journey.

Advanced **browser exploitation specialists** will get an opportunity to quickly catch up with the current state of Chromium security and AI workflows, while future-proofing their methods.

PREREQUISITES

- Binary vulnerability discovery and exploit development experience.
- Building and debugging on Linux and/or Microsoft Windows.
- Comfortable with large codebases.
- Browser Exploit Design or an equivalent system of knowledge of browser-class architectural models and exploit patterns.

OBJECTIVES

This training will enable attendees to:

- Build a research and debugging platform for Chromium supporting the majority of offensive research challenges.
- Navigate Chromium codebase and exploit history with confidence.
- Discover new vulnerabilities and develop exploits for up-to-date Chromium efficiently.
- Use current publicly available AI models and agents to accelerate every workflow.
- Integrate research methodologies that transfer beyond the specific case studies, and persist through the codebase churn.
- Understand current state of the art in Chromium security, and apply it to research objectives.
- Understand and work against modern Chrome-specific exploit mitigations in practice..

LEVELS & CERTIFICATION

Complexity: advanced
Certificate: Completion or Competence.

TRAINING DETAILS

Chrome Full Chain Exploit Engineering is an advanced training for vulnerability researchers and exploit developers working at the frontier of Chromium security. Where a foundational course teaches the skills, this one is about applying them at the level and pace the current target demands: finding live bugs in up-to-date Chromium, understanding the real state of exploit mitigations, and building the research workflows that make a full chain — from RCE to sandbox escape — as a unified undertaking rather than teamwork across domains.

Our objective requires a specific approach rarely taught: building future-proof workflows that out-persist the rate of change in the codebase. As of today, concrete details of Chromium code have short-term value; the real demand is the ability to obtain the knowledge quickly and correctly – what questions to ask, where to look for the answers, how to put it all together and apply it in practice.

The curriculum assumes the browser-class models from Browser Exploit Design as a base, and overlays Chromium-specific depth onto it: architecture and implementation detail, live versus dead bug patterns, mitigations in practice (PartitionAlloc, MiraclePtr, the V8 sandbox), and techniques that work against present-day code. Vulnerability is worked hands-on: patch diffing and variant analysis, AI-assisted bug hunting and exploit development, and CodeQL queries drawn from live research.

Exploitation is taught through complete worked examples, including the honest anatomy of where a real bug meets a real mitigation wall — more instructive to a working researcher than a sanitized success. All code studies are drawn from recent first-hand VRP research.

The operating system is deliberately left as a free choice, as the majority of Chromium security knowledge is OS-neutral. A Linux R&D platform is assumed as a common base, plus ability to build and debug on Windows as an experimental setup. Both setups will be explained in the training, along with the OS-specific differences facing Chromium exploit development in practice.

Chromium has a reputation as unapproachable, which deters capable researchers more than the difficulty itself does. Our methodology with AI-accelerated workflows dissolve that barrier: not by making the target easy, but by putting the workflow within reach of any serious researcher.

Attendees will walk away with a transferable, cutting-edge, and future-proof capability that applies beyond specific case studies.

ABOUT THE INSTRUCTOR

Alisa Esage is an independent security researcher and the founder of Zero Day Engineering, specializing in offensive vulnerability research and exploitation. The first woman to compete solo at Pwn2Own and author of original research methodologies for the world's most hardened systems, she has spent over two decades at the frontier of the field — finding the bugs and building the exploits that most consider intractable.

Alisa's work decenters the shallow "break and abuse" hacker culture in favor of building deep transferable models and workflows beneath elite exploitation: the frameworks that let a single researcher operate across classes and codebases, and stay ahead of a moving target. These methods are the foundation of Zero Day Engineering's research and products.

TRAINING CURRICULUM

DAY 1. SETUP

Lectures:

- Chrome security internals SOTA.
- Bug patterns per subsystem: dead and alive.
- Review of past year's bug trends.
- Selective deep-dive case studies.

Labs and walkthrough:

- Building the R&D platform.
- Automation of routine maintenance with custom scripts.
- Debugging and experimental best practices.

Exercises:

- Inspection of system internals in the codebase, with anti-anti-AI awareness.
- Live runtime introspection of self-built Chromium with our own tooling.

DAY 2. DISCOVERY

Lectures:

- What makes bughunting competitive when everyone has AI.
- CodeQL best practices for Chromium.
- LLM internals for offensive prompting and agent management.

Labs and walkthrough:

- Chrome security patch advisories: navigation, evaluation, analysis.

Exercises:

- CodeQL base experiments and bug query construction.
- Patch diffing and variant hunting.
- Bug candidate triage in code.

DAY 3. EXPLOIT ENGINEERING

Lectures:

- RCE objective: cognitive models, bug patterns, exploit techniques
- Exploit mitigation internals: v8 heap sandbox
- v8 sandbox bug patterns and trends.
- Current state of exploit techniques for v8.
- Deep dive into our v8 bug archetype – structural foundations and relevant case studies from history.

Labs and walkthrough:

- Inspecting the current state of v8 sandbox implementation in the code.
- Building custom tooling for Chromium.

Exercises:

- Exploit development – RCE: from code hypothesis to testcase to AAW exploit POC (multi-stage exercise).

DAY 4. EXPLOIT ENGINEERING

Lectures:

- Sandbox escape objective: cognitive models, bug patterns, exploit techniques
- Exploit mitigation internals: MiraclePtr and PartitionAlloc
- Exploit mitigation bypass techniques, prerequisites, constraints – MiraclePtr and PartitionAlloc
- Deep dive into our browser bug archetype.

Labs and walkthrough:

- Introspection of PartitionAlloc allocations and metadata with no-debugger tooling

Exercises:

- Exploit development – EoP in browser process: from code hypothesis to testcase to mitigation wall (multi-stage exercise)

TRAINING FEES & PLATFORMS

This training is available live: online and in-person.

Online training is hosted on Zoom platform. The instructor will be available for in-scope technical questions in dedicated Q&A slots during live sessions, and by email afterwards.

Students will prepare their own lab setup, either from scratch with provided instructions or by downloading and installing a pre-configured Virtual Machine.

All training packages are specifically optimized for online teaching and self-paced delivery.

LIVE PUBLIC TRAINING

Online cohorts

What's included:

- Access to public online training via Zoom.
- Slides and supplementary materials.
- Certificate – Completion and/or Competence – arranged upon request.
- Technical consultation – 1 month.
- Access to recordings – 3 months.

Training schedule – each day:

- 4h live online lectures + Q&A
- 2-4h self-study practice and exercise with prerecorded content.

Instructor availability for technical consultations:

- During the live online sessions, in specifically designated sections for discussion.
- By email – one month after the training.

Price: €8,000.- NET per person.

SELF-PACED COURSE (N/A)

Basic package

What's included:

- Video lectures, exercises, and walk-through.
- Training slides and supporting materials.
- Access to videos for 3 months.

Price: n/a

Complete package

What's included:

- Everything in the Basic package.
- One month of technical support by email.
- One on-demand consultation call with the founder.
- Training certificate.

Price: n/a

Note: certificates will be issued upon request.

PRIVATE IN-PERSON TRAINING

Private training can be arranged online or in-person for institutional teams, subject to availability.

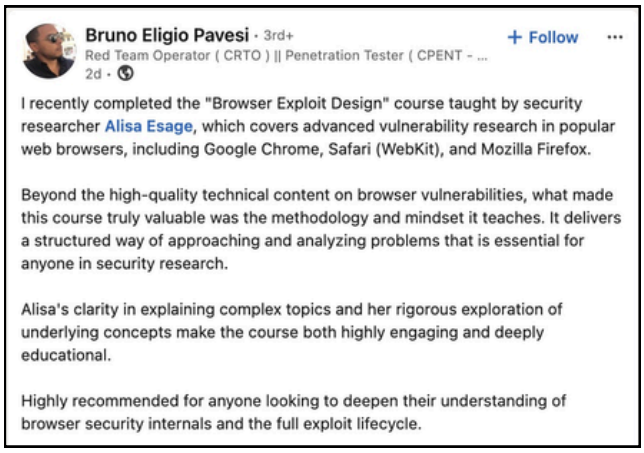
PUBLIC TRAINING DATES & TERMS OF BOOKING

Refer to our schedule for the dates of the nearest public cohort.

Training seats will be available for purchase exclusively through our website zerodayengineering.com, which is the only point of sales. We may refuse to accommodate unauthorized third party bookings.

Bookings of public training seats will be accepted via website checkout system. A standard invoice will be sent automatically by email after the purchase. We do not support custom paperwork for individual seat purchases in public cohorts and self-paced packages.

TRAINING REVIEWS – BROWSER EXPLOITATION



Bruno Eligio Pavesi · 3rd+ + Follow
Red Team Operator (CRTO) || Penetration Tester (CPENT - ...
2d ·

I recently completed the "Browser Exploit Design" course taught by security researcher Alisa Esage, which covers advanced vulnerability research in popular web browsers, including Google Chrome, Safari (WebKit), and Mozilla Firefox.

Beyond the high-quality technical content on browser vulnerabilities, what made this course truly valuable was the methodology and mindset it teaches. It delivers a structured way of approaching and analyzing problems that is essential for anyone in security research.

Alisa's clarity in explaining complex topics and her rigorous exploration of underlying concepts make the course both highly engaging and deeply educational.

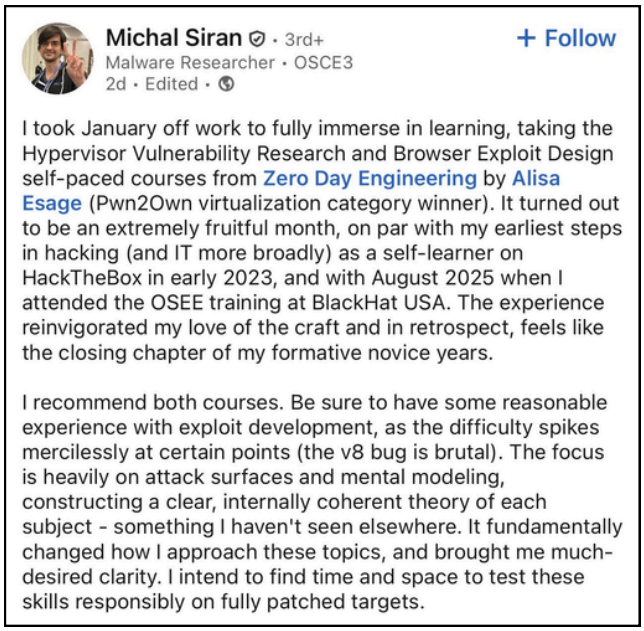
Highly recommended for anyone looking to deepen their understanding of browser security internals and the full exploit lifecycle.

Ian van der Wurff · 3rd+
Hacker || OSCE3 | OSCP | tozetta.com | ian.nl
1w ·

Zo'n drie maanden geleden ben ik begonnen aan de Browser Exploit Design training van Zero Day Engineering.

Een hele interessante self-paced course waar een combinatie van browser internals, realistische exploit development workflows en hands-on oefeningen gebaseerd op moderne browser 0-days aan bod komt. Met daarin onderwerpen zoals DOM use-after-free bugs, JavaScript engine type confusion en sandbox escapes in oa Chrome, Firefox en Safari/WebKit.

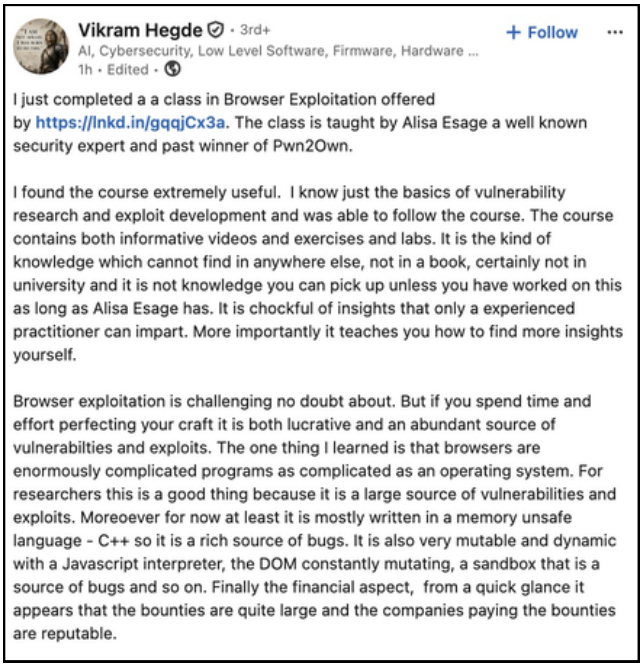
Het is zonder twijfel de meest uitdagende course die ik tot nu toe heb gevolgd op het gebied van (browser) exploitation. En ik heb nog veel te leren hierin. Maar veel meer inzicht gegeven in hoe browsers werken en hoe browser exploits in de praktijk worden gedaan. Wordt vervolgd.



Michal Siran · 3rd+ + Follow
Malware Researcher • OSCE3
2d • Edited •

I took January off work to fully immerse in learning, taking the Hypervisor Vulnerability Research and Browser Exploit Design self-paced courses from Zero Day Engineering by Alisa Esage (Pwn2Own virtualization category winner). It turned out to be an extremely fruitful month, on par with my earliest steps in hacking (and IT more broadly) as a self-learner on HackTheBox in early 2023, and with August 2025 when I attended the OSEE training at BlackHat USA. The experience reinvigorated my love of the craft and in retrospect, feels like the closing chapter of my formative novice years.

I recommend both courses. Be sure to have some reasonable experience with exploit development, as the difficulty spikes mercilessly at certain points (the v8 bug is brutal). The focus is heavily on attack surfaces and mental modeling, constructing a clear, internally coherent theory of each subject - something I haven't seen elsewhere. It fundamentally changed how I approach these topics, and brought me much-desired clarity. I intend to find time and space to test these skills responsibly on fully patched targets.



Vikram Hegde · 3rd+ + Follow
AI, Cybersecurity, Low Level Software, Firmware, Hardware ...
1h • Edited •

I just completed a a class in Browser Exploitation offered by https://lnkd.in/gqqjCx3a. The class is taught by Alisa Esage a well known security expert and past winner of Pwn2Own.

I found the course extremely useful. I know just the basics of vulnerability research and exploit development and was able to follow the course. The course contains both informative videos and exercises and labs. It is the kind of knowledge which cannot find in anywhere else, not in a book, certainly not in university and it is not knowledge you can pick up unless you have worked on this as long as Alisa Esage has. It is chockful of insights that only a experienced practitioner can impart. More importantly it teaches you how to find more insights yourself.

Browser exploitation is challenging no doubt about. But if you spend time and effort perfecting your craft it is both lucrative and an abundant source of vulnerabilties and exploits. The one thing I learned is that browsers are enormously complicated programs as complicated as an operating system. For researchers this is a good thing because it is a large source of vulnerabilities and exploits. Moreoever for now at least it is mostly written in a memory unsafe language - C++ so it is a rich source of bugs. It is also very mutable and dynamic with a Javascript interpreter, the DOM constantly mutating, a sandbox that is a source of bugs and so on. Finally the financial aspect, from a quick glance it appears that the bounties are quite large and the companies paying the bounties are reputable.

More reviews: https://zerodayengineering.com/training/reviews/index.html

APPLICATIONS & INQUIRIES

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