



Zero Day Engineering

training & intelligence

ZERO DAY VULNERABILITY RESEARCH

TRAINING OVERVIEW

This 4-day training course comprehends essential knowledge and skills required to conduct modern low-level security research, vulnerability exploit development, secure software engineering and hardening. The course is created and taught by a professional vulnerability researcher and low-level hacker who is actively engaged in security bounty hunting and zero day vulnerability discovery and exploitation as her main job, and qualified as a top zero day hacker by successful participation in Pwn2Own competitions.

This course is designed for complete beginners, yet inclusive of many advanced aspects of the craft that students will likely need as they advance. Following the always systematical structure of Zero Day Engineering Project courses, it covers all the essentials that students need to get started with arbitrary research targets in a compact and practical way. Excluded are specialized topics: advanced exploit techniques and mitigations, OS & hardware theory, and threat models for specific software classes.

Training course theory will be illustrated and practiced with modern and immediately relevant real-life examples, including high-impact vulnerability case studies and non-trivial examples.

AUDIENCE

This training course is primarily intended for beginners in low-level security research with basic knowledge in computer science.

Materials of this course comprehend an essential base of knowledge and skills for software vulnerability researchers, security-minded software developers, and DevSecOps engineers.

Systematical structure and strategic insights of this course would be valuable for seasoned hackers and professional security researchers.

PREREQUISITES

Mandatory:

- General computer science.
- A laptop with a modern Linux VM.

Optional.

- C-language.
- Familiarity with basic concepts of low-level computer security.

OBJECTIVES

Upon completion of this training course the students should – with a certain commitment – be able to:

- Engage in bug bounty hunting.
- Participate in CTF competitions.
- Conduct exploit & vulnerability analysis.
- Find simple oday vulnerabilities.
- Reverse-engineer simple softwares..
- Avoid security bugs in their code.
- Write and customize fuzzing tools.
- Apply public tools and scripts in the right order.
- Make independent and reasonably correct judgements about 3rd party bugs & exploits.
- Choose further specialization and research focus wisely.

LEVELS & CERTIFICATION

Complexity: beginners, involved.

Certificate grade: CoDEo (Foundation).

Next level training: "<Target> Vulnerability Research"

TRAINING DETAILS

This training course assumes an extremely ambitious goal: to comprehend everything you need to get started with modern application security research in just 4 days. This is accomplished by following a deeply systematical learning model created by the instructor with an extensive experience in multiple specializations of the subject, alongside with time-proven techniques of cognitive optimization.

Despite the sassy name, the knowledge presented in this course is ethically neutral. It provides a universal foundation theory and skills for writing secure code, as much as for offensive security research of arbitrary software, firmware and hardware targets. Students are encouraged to think generically in terms of universal models, that makes a solid ground for arbitrary specializations: such as bug hunting, writing fuzzing tools, exploit development, reverse-engineering, or malware analysis.

The course deliberately ignores any differences between attacking binary code and web applications, because the underlying threat models are essentially the same, as explained on Day 1. That said, course approach is heavily geared towards binary analysis. Even logic vulnerabilities – the bug class which is commonly associated with web applications – are considered with respect to modern binary programs.

Key principle is to expose attendees immediately to some of the most impactful real-life case studies. While it may be impossible to learn it all in a few days, eager students are expected to be able to enter CTF competitions and find some easy bugs straight out of the training. In addition, the solid foundation given by this course will later help them to learn specialized knowledge faster and more systematically.

An empirical sampling of various specializations in the field of application security, alongside with insights of a seasoned hacker, comes as a side effect in this course. That would enable newcomers to choose their specialization based on personal experience rather than theoretical reasoning or fashion.

Course experience is a mixture of theory and practice. Practicals – that's small exercises and labs – are based on Linux, as the most versatile technical research platform that every low-level hacker eventually employs extensively in their workflow, even if their research is focused on a different OS.

The knowledge presented in this course is 100% original, based on independent technical research and reverse engineering work done by the author herself, and illustrated with security vulnerabilities discovered by the author, as well as with publicly available sources. Course content is kept up-to-date.



ABOUT THE INSTRUCTOR

Alisa Esage is a lifetime code breaker, vulnerability researcher and reverse engineer. She was credited by Microsoft, Google, Firefox, Oracle, Schneider Electric, and other leading software vendors for discovery of previously unknown security bugs. She is specialized on binary-level offensive security research and exploit development for hardened systems.

Alisa taught herself assembly programming and reverse-engineering while studying in school. She is active in today vulnerability research since 2011, is deeply familiar with key research directions in the fields of offensive security and exploitation, while leaning to generalization and abstract modeling. Alisa is qualified as a top zero day hacker by successful participation in Pwn2Own competitions.

PROGRAM AT A GLANCE

DAY 1. FOUNDATION

Abstract models and essential general theory.

Theory (2 h)

- Mindset.

What makes an effective zero day engineer?

- Program theory concepts.

System design, state space, code correctness.

Core topic (4 h)

- Model of Vulnerability.

Bug vs. Vuln. Root cause vs. effect. Exploitability

- Model of Exploit.

Objectives, stages, primitives, payload.

- Application Threat Models.

Attack surfaces & attack vectors in applications.

Essential skills & research topics (2 h)

- General vulnerability classification.

Design bugs, logic bugs, memory safety bugs.

- C and C++, JavaScript, Python.

Overview & exploitation-relevant bits.

DAY 3. BINARY HACKING

Get started with binary code analysis and exploit development.

Theory (2 h)

- Compiler theory.

From HLL to binary code.

- Assembly programming vs. shellcoding.

CPU models & popular architectures.

Core topic (4 h)

- Fuzzing essentials: basic & next level.

From random inputs to vulnerability discovery.

Essential skills & research topics (2 h)

- Memory safety bugs vs. exploit mitigations.

Classification & common patterns. Case studies.

- Reverse code engineering.

From binary to assembly to code to architecture.

- Binary debugging.

DAY 2. PROGRAM ANALYSIS & LOGIC BUGS

Working with source code. Discovering, evaluating and reproducing simple types of bugs.

Theory (2 h)

- Logic bugs.

Classification and common patterns.

- Case studies.

High-impact logic bugs in modern software.

Core topic (4 h)

- Static code analysis.

Bug hunting in large and complex code bases.

- Assisted code analysis.

Finding bugs in code with modern tools. CodeQL.

Essential skills & research topics (2 h)

- Security patch analysis.

Understanding bugs via source code patches.

- Introduction to dynamic analysis.

Debuggers in source mode. Frida.

DAY 4. INTO THE FUTURE

Up-and-coming essentials in low-level security.

Theory (2 h)

- Mathematics of low-level security.

Program modeling efforts, weird machines, abstract interpretation.

- Memory-safe programming languages.

Rust. Internals, threats, bugs, academic research.

Core topic (4 h)

- Blockchain security.

Novel threat models. Case studies.

Research topics (2 h)

- Hardware bugs.

Speculative execution, Rowhammer, FI.

- DSP and NPU.

Software, firmware and hardware that powers artificial neural networks and deep learning.

TRAINING PACKAGES & FEES

This training course is publicly available online (live), in self-paced packages, and privately.

Online and on-demand trainings are based on a modern streaming platform with high-quality audio and video, and a group chat. The instructor will be available for questions, feedback and technical support, according to specific package conditions.

Payments through the website are subject to merchant fees, which can be waived by paying via bank transfer or with crypto currencies.

LIVE TRAINING

View-only access

What's included:

- Access to public online training.
- Guaranteed instructor's feedback by email.
- Training slides and materials.
- Training completion certificate.

Price: €3,900.- per person.

Interactive access

What's included:

- Everything in the View-only option.
- Personal feedback and technical support from the instructor during the live training.
- A possibility to receive a Training Achievement certificate by undergoing an assessment.

Price: €4,100.- per person.

Note: Limited number of seats for the Interactive access option.

SELF-PACED PACKAGES

Basic package

What's included:

- Video lectures, exercises, and walk-through.
- Training slides and materials.
- Training completion certificate.

Price: €2,500.- per person.

Complete package

What's included:

- Everything in the Basic package.
- One month of 1-on-1 technical consultation with the instructor by email.
- One on-demand technical consultation with the instructor by video call.

Price: €4,100.- per person.

Note: Self-paced packages are recordings of our live online training. Videos can be viewed on-demand through a streaming platform (no offline access, except for the slides).

PRIVATE & CUSTOMIZED TRAINING

Minimal private group size is 10 persons. Availability is limited, book at least 3 months in advance.

LIVE TRAINING DATES & BOOKING

Refer to our [website](#) for the dates of the nearest public training.

All our online training courses are offered exclusively at the Zero Day Engineering company website: <http://zerodayengineering.com>.

Bookings of public training seats are accepted via the website. For custom and private bookings, [email us](#).

WHAT TO EXPECT?

Quoted below are public reviews of our students of the Zero Day Vulnerability Research training.

"I'm taking the self-paced Zero Day Engineering course and it's **one of the best investments I've ever made**. I'm on Day 3 and I've already **had several insights** and the certainty that I'm **building a solid, long-term foundation**. There's still the Binary Hacking part that I love most and I'm sure I'll also have several insights. I can imagine how valuable 1:1 mentoring would be if group training is already so good." — Igor Ladessa on Telegram

"Completely agree with this take. I took the sel-paced and currently Im doing a **second run** while saving for the hypervisor exploit dev training too :)" — @alephox00 reply on Twitter

"Finally managed to find some time to commit to the Zero Day Vulnerability Research course! Loving the **organized and systematic approach**. Kudos to the **impressive research and theoretical insights** from [@zerodaytraining](#)" — @Pohakyu on Twitter

"Just finished day 1 and looking forward to the rest. [Alisa Esage](#) is great! The **pace** is great, **building up** from the ground up, emphasizing the **mindset** and **frameworks** necessary to handle any **future** vulnerability research topics. Looking forward to the rest!" — Oscar De La Rosa on LinkedIn

Quoted below are excerpts of relevant feedback for our other courses.

"I had an amazing time in the training. I feel like a lot of the **knowledge I had was clarified in the training and is now more organized**. Of course I also **learned a lot of new stuff** and it was really interesting and useful."

"The **processes and workflows** that you demonstrated. Particularly during your walkthroughs of the exercises, it was incredibly valuable to see and hear your own methodology for completing each example. The exercises themselves where also a fantastic learning tool."

"Here is what I loved about the whole thing:

- **Well organized content**, with a good order of things.
- A decent **balance of theory and hands-on** (I'm probably biased to hands-on).
- Pomodoro, time boxing, neural net.. liked the **meta-learning** touch there.
- Discussions on **threat models, vuln discovery strategies, potential fuzzing designs.**"

Additional reviews from our students of other courses can be found on [our website](#) and in our social channels ([Twitter](#), [Telegram](#)).

FURTHER INQUIRIES

E-mail: contact@zerodayengineering.com

Note: we typically respond to all business e-mails within 1-2 business days. In case of any communication issues, we're on Signal +1(707)505-93-43, Telegram [@zerodayengineering](#).

CHANGELOG

09.01.2024. Price increase of Complete package due to instructor's availability; new reviews; updated contacts.

05.12.2023. Training package conditions changed.

30.08.2023. Minor updates and style fixes.

22.02.2022. Initial release of this document; training program version 0.1.

13.06.2022. Optimized the course program.

24.08.2022. Minor fixes (style).

22.09.2022. Design (new logo).

01.12.2022. Updated availability and conditions per self-paced packages.