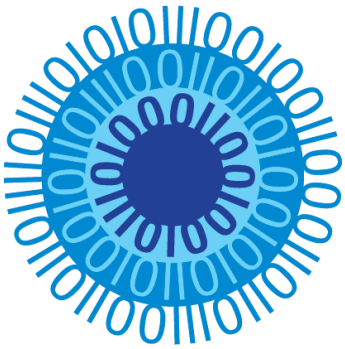

SOURCE INCITE

Web Application Vulnerability Research

Advanced Training

TRAINING OVERVIEW

Full Stack Web Attack is *not* an entry-level course. It's designed to push you beyond what you thought was possible and set you on the path to develop your own workflow for offensive zero-day web research.

Each of the vulnerabilities presented have either been mirrored from real zero-day or are n-day vulnerabilities that have been discovered by the author with a focus on not just exploitation, but also on the discovery.

The course material is fully illustrated with detailed slides, workbook, code samples and an answer sheet given out at the end.

If you want to learn how to exploit web technologies without client interaction for maximum impact, that is, remote code execution then this is the course for you.

Leave your OWASP Top Ten at the door.

AUDIENCE

This course is developed for web penetration testers, bug hunters and developers that want to make a switch to server-side web security research or see how serious adversaries will attack their web-based code.

Students are expected to know how to use web proxies and have a basic understanding of common web attacks as well as perform basic scripting using common languages such as Python, PHP and JavaScript.

Additionally, seasoned professionals are sure to be challenged!

OBJECTIVES

Upon completion of the training course, students should be able to:

- Setup debugging environments for PHP and Java.
- Trace code through a debugger.
- Discover basic zero-day vulnerabilities.
- Chain and exploit web-based vulnerabilities for maximum impact.
- Write quality patches and bypass vendor developed patches.
- Perform patch differentiation to reveal n-day vulnerabilities.
- Write high quality vulnerability reports.
- Stay focused for long periods of time to achieve results.

PREREQUITES

Personal

- An open mind that is ready to focus.
- Basic scripting skills with moderate or advanced preferred.
- Some exposure to container-based technologies and Unix operating systems.
- A strong understanding of various web technologies.
- A foundational understanding of common web vulnerabilities.

Hardware & Internet

- A stable and fast internet connection.
- A x64 host operating system.
- 16 Gig RAM minimum.
- Virtualization software (VMWare Player, Workstation or Fusion).
- 100 Gig of available hard disk space.

CERTIFICATION

We do not provide certifications at this time; however digital certificates are provided upon class completion.

COURSE STRUCTURE

- Training hours: 9am* - 5pm*.
- Lunch break: 12.30pm for 1 hour.
- Coffee break: 10.30am for 10 minutes.
- Coffee break: 3.15pm for 10 minutes.

* The day-to-day hours maybe adjusted at the discretion of the trainer and students.

TRAINING APPROACH

The trainer uses a hybrid model of training combining theory and practice. Each of the theoretical techniques are practically applied in class with a focus on high information retention using Jungian psychological techniques.

The students are lead through a series of exercises and challenges broken down into "modules" that cogitatively reinforce theoretical concepts and encourage creative thinking by applying problem solving skills. The content presented and trained is 100% original and applicable to current real-world software and systems.

All too often training classes miss the gap – They don't cover the complete stages of vulnerability research. In ***Full Stack Web Attack***, we help the student to build their skills in vulnerability discovery ***and*** exploit development.

TRAINING OVERVIEW

Day 1

Introduction

- PHP & Java language fundamentals
- Debugging PHP & Java applications
- Course overview
    - Module 1, 2, 3, 4, 5
    - Required background knowledge
- Auditing tips for zero-day discovery

PHP

- Loose typing
- Logic authentication bypasses
- Code injection
- Filter bypass via code reuse
- Patch bypass

Day 2

Java

- RMI
    - JRMP
    - Registry attack/JEP290 bypass
- JNDI Injection
    - Remote class loading
    - Deserialization 101
        - Existing gadget chains
    - Unsafe Reflection

PHP

- Introduction to object instantiation
- Introduction to protocol wrappers
- External entity (XXE) injection
    - Full response attacks
    - Error response attacks

- Blind attacks

Day 3

PHP

- Patch analysis and bypass
- Introduction to object injection
- Magic methods
  - Customized serialization
  - Phar deserialization
  - Property oriented programming (POP)
  - Custom gadget chain creation
- Information disclosure
- Phar planting
- Building an exploit chain to achieve remote code execution

Day 4

PHP

- Blocklist bypasses – n-day vulnerability analysis and exploitation

Java

- Introduction to reflection
- Expression language injection
- Bypassing URI filters
- URI forward authentication bypasses
- Deserialization 102
  - Custom gadget chains
  - Trampoline gadgets
  - Exploiting reflection
  - Allow list flexibility (ab)use
- Server-Side Template Injection

ABOUT THE INSTRUCTOR

Steven Seeley is a world-renowned security researcher who has over a decade of experience in application security. He has been credited with finding over 1500 high impact security vulnerabilities affecting vendors such as Microsoft, VMWare, Apple, Adobe, Cisco and many others.

In 2020, Steven teamed up with Chris Anastasio competing in Pwn2Own Miami - winning the ***Master of Pwn*** title. In 2021, Steven reached 12th position on the MSRC top 100 Vulnerability Researchers list.

TRAINING PACKAGE AND PRICING

This course is typically available twice a year using any combination of “live” or “online” delivery depending on the geopolitical climate. The online class is delivered at Central Standard Time (CST) and requires students to have an active GitLab account to receive training materials. The live classes may be held anywhere in the world at the discretion of the trainer.

Online classes have a maximum of 16 students including 2 student tickets and 4 early bird tickets. Live classes have a maximum of 22 students including 3 student tickets and 5 early bird tickets.

Private training classes are available and subject to the instructor’s schedule. These bookings require 2 months advance notice. Additionally, they typically require a minimum of 8 students with the travel expenses covered for the trainer ($2,000 USD). If 14 or more tickets are purchased, then the travel expenses are waved.

The below table reflects the current pricing model for public trainings.

Ticket Type	Price in USD
Student	$3,133.70
Early Bird	$3,600.00
General	$4,000.00

Please note – private trainings ticket price is set to $4,000 USD for each ticket. Public trainings can be booked via our signup page and private trainings can be booked by emailing us.

STUDENT FEEDBACK

Student feedback is critical to us and at the end of every training class we ask students to evaluate our performance and course content through an efficient anonymous survey. We use this feedback loop to actively look for ways to improve our class. Below is some of the feedback that has been received from past students

"I recommend @steventseeley's Full Stack Web Attack from @sourceincite. I know it's going to be offered a few times next year, you should take it! It's training unlike anything else. ***I am excited to put my newly found skills to work****. Awesome stuff!"*

"Just finished FSWA from @sourceincite, wow! ***Everything presented is applicable and nothing is contrived. Well executed as a remote training as well****."*

"I finally got to take FSWA with @steventseeley. ***It's one of the best offensive courses I've taken*** *and seen available today.* ***Highly recommend for anyone doing exploit development and bug hunting****"*

"I finally attended the Full Stack Web Attack (FSWA) course by @sourceincite/@steventseeley earlier this week! The course is full of insights on vuln discovery, debugging and exploit techniques. ***Exercises are challenging and thought-provoking****. Overall, it's an awesome course!"*

"The @sourceincite #FSWA training from @steventseeley was simply badass! Highly recommend anyone who wants to ***learn the latest techniques in getting web shells on hard targets****"*

"It was very inspiring to see your strategy, way of thinking and searching through code. That is even more valuable than the vulnerabilities themselves. ***It was possibly one of the most challenging trainings, I took, in a good way****."*

FURTHER INQUIRES

PGP: 5B1183EE04FD7FFE68BE48E264AE09A98432FB9B

Email: training@srcincite.io

Web: https://srcincite.io/

Note – We typically respond to all business inquires within 1-2 business days.