OpenSSF Tech Talk

Jumpstart Your Journey: Mastering OSS Security Development with the Linux Foundation Education

October 10th, 10AM PT/1PM ET

Education

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Welcome!

- Thank you for joining us today! We will begin at 10:02am PT.
- While we wait for everyone to join, please take a moment to do one (or more) of the following:
  - Please add questions using the Zoom Q&A feature
  - Follow us on Twitter: @openssf, Mastodon: social.lfx.dev/@openssf, & LinkedIn: OpenSSF
  - Visit our website: https://openssf.org
  - Sign up for training: https://openssf.org/training/courses/
- This Tech Talk is being recorded

Education

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Agenda

- Housekeeping
- Speaker Introductions
- OpenSSF Educational Materials - David A. Wheeler
- Insights from LF Education - Glenn ten Cate
- Insights from Implementing Organization - Sarah Evans
- Panel Discussion & Audience Q&A
- Important announcements

Help us improve! Tech Talk Survey

Education

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Antitrust Policy Notice

Linux Foundation meetings **involve participation by industry competitors**, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at **http://www.linuxfoundation.org/antitrust-policy**. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

Code of Conduct

- The Linux Foundation and its project communities are **dedicated to providing a harassment-free experience** for participants at all of our events, whether they are held in person or virtually.
- All event participants, whether they are attending an in-person event or a virtual event, **are expected to behave in accordance with professional standards**, with both this Code of Conduct as well as their respective employer's policies governing appropriate workplace behavior and applicable laws.
- https://openssf.org/community/code-of-conduct/

Q&A

Please submit your questions during the meeting by using the Q&A feature on Zoom.

Thank you!

Introductions

Christopher “CRob” Robinson

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Christopher “CRob” Robinson - Security Lorax, Chief Architect of OpenSSF

Christopher Robinson (aka CRob) is the Chief Security Architect for the Open Source Software Foundation (OpenSSF). With over 25 years of experience in engineering and leadership, he has worked with Fortune 500 companies in industries like finance, healthcare, and manufacturing, and spent six years as Program Architect for Red Hat’s Product Security team.

CRob has spoken at major events such as RSA, BlackHat, and DefCon, and was recognized as a top presenter at Red Hat Summits in 2017 and 2018. He holds certifications like CISSP and CSSLP. He leads several OpenSSF working groups, chairs its Technical Advisory Committee, and contributes to the FIRST PSIRT SIG.

CRob enjoys hats, herding cats, and moonlit beach walks.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

David A. Wheeler - Director of Open Source Supply Chain Security, the Linux Foundation

Dr. David A. Wheeler is a prominent expert in secure software development and open source software (OSS). He authored “Secure Programming HOWTO” and is recognized for his work on mitigating malicious tools through “Fully Countering Trusting Trust through Diverse Double-Compiling (DDC).” As the Director of Open Source Supply Chain Security at the Linux Foundation, he also leads the OpenSSF Best Practices badge project. Dr. Wheeler teaches secure software courses at George Mason University (GMU), where he earned his PhD in Information Technology and a Master’s in Computer Science. He is a Certified Information Systems Security Professional (CISSP) and a Senior Member of the IEEE.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Glenn ten Cate - Senior Cyber Security Instructor at the Linux Foundation

Glenn is a seasoned cybersecurity expert with an extensive portfolio in secure software development, consultation and cybersecurity training. At the Linux Foundation he is a cybersecurity subject matter expert and Senior Cybersecurity Instructor. Glenn has received WASPY nominations for Innovation/Sharing and Best Innovator and an Honorable Mention for the Security Knowledge Framework project by Black Duck® Rookies of the Year.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

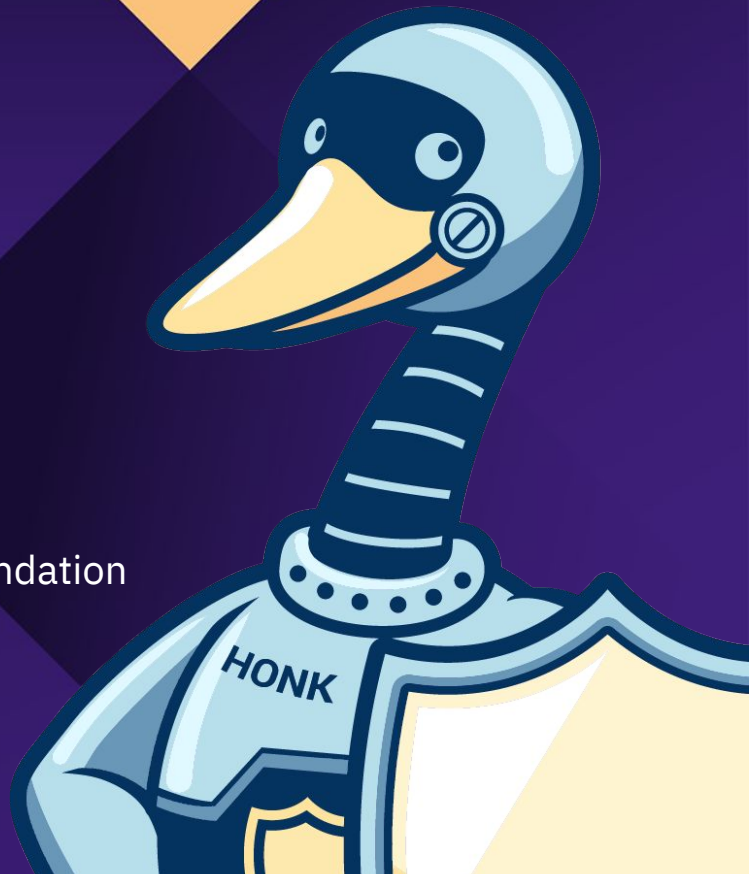
Sarah Evans - Security Research Technologist, Dell Technologies

Sarah is a security innovation researcher at Dell Technologies, on the Product and Operations Global CTO Research & Development team. She focuses on innovation for secure technology adoption, especially functionality that improves security of AI systems and supply chains. Prior to Dell, Sarah has had roles at a large financial institution, the defense industry, a regional Midwest construction company, and as computer information systems faculty at Missouri State University. Sarah also contributes to OpenSSF, working with industry peers and open source projects to secure the open source software supply chain. Sarah is based in Denver, Colorado.

OpenSSF Educational Materials

David A. Wheeler

Director of Open Source Supply Chain Security, Linux Foundation



Outline

- LF Education Research 2024 Survey
  - by Open Source Security Foundation (OpenSSF) & Linux Foundation (LF) Research
- “Developing Secure Software” (LFD121) course
- Other OpenSSF educational materials

Secure Software Development Education 2024 Survey

Key findings from the report indicate that an important minority of developers are not familiar with secure software development, and many identified a lack of training or a lack of awareness around the courses available.

<https://www.linuxfoundation.org/research/software-security-education-study>

28% of professionals directly involved in software development are **not familiar** with secure software development.

Software developers with **less than one year of experience** report the highest lack of familiarity (75%)

69% of professionals rely on on-the-job experience as a learning resource for secure software development, but **it can take more than 5 years of such experience** to achieve familiarity.

50% of professionals identify **a lack of training as a major challenge** for implementing secure software development, with this issue being particularly pronounced among data science roles (73%).

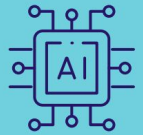
53% of professionals, especially those in system operations (72%), have not taken a course on secure software development, largely due to **the lack of awareness about good courses** (44%).

79% of professionals consider language-agnostic courses highly important, compared with 54% who attribute the same level of importance to language-specific courses.

Popular language-agnostic courses include **security architecture** (64%), **security education and guidance** (64%), and **secure implementation** (63%).

Training needs vary significantly based on **professional roles and experience levels**.

Python is highly favored for language-specific training, with 71% of respondents expressing a preference, although C and Java are selected more frequently when respondents rank their top choices.



57% of respondents identify **AI and ML security** as a critical area for future innovation and attention in secure software development.

56% of respondents see **supply chain security** as a crucial area needing increased focus and innovation.

To start mitigating the need for more secure software development education, the OpenSSF selected **Security Architecture as the topic of a new course.**

Lack of knowledge is leading to vulnerabilities

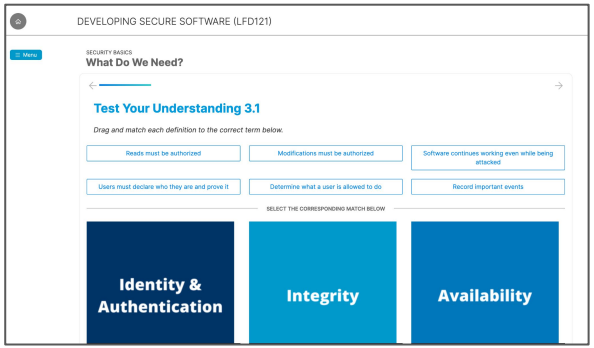
- Most colleges/unis don't require it (1/top 24 CS schools 2022) [Forrester]
- 43% of security breaches linked to insecure sw development practices [Verizon]
- Tools for finding vulnerabilities are valuable, but ***not*** by themselves
  - Tools have false+ and false-
  - Software developers must be educated to be able to use tools effectively
  - "Fool with a tool is still a fool"

Solution: “Developing Secure Software” (LFD121) Course

- *Free* course, ~2 days material
- *Free* certificate of completion
- Audience: Software developers
- Online (digital), on-demand, highly rated
- Developed by OpenSSF
- Teaches fundamentals of developing secure software
  - Open Source Software & Closed Source
- Accessible
- Already used by thousands
- See https://hubs.la/Q02S4t2X0

LFD121: Active, not passive

Quizzes throughout help ensure understanding




```
// Set up Express framework and express-validator library
const express = require("express");
const app = express();
const { query, matchedData, validationResult } =
    require('express-validator');

// Implement requests, e.g., http://localhost:3000/invoices?id=1
app.get('/invoices',
  query('id').isint(),
  (req, res) => { // Execute this code if /invoices seen
    const result = validationResult(req); // Retrieve errors
    if (result.isEmpty()) { // No errors
      const data = matchedData(req); // Retrieve matching data
      return res.send(`You requested invoice id ${data.id}!`);
    }
    res.status(422).send(`Invalid input`);
  })
```

Hint | Reset | Give up

Optional interactive labs provide hands-on practice & provide hints

Many labs recently added, more on way

“Developing Secure Software” (LFD121) Outline

Part I: Requirements, Design, and Reuse

- Security Basics
- Design
- Reusing External Software

Part II: Implementation

- Basics of Implementation
- Input Validation
- Processing Data Securely
- Calling Other Programs
- Sending Output

Part III: Verification and More Specialized Topics

- Verification (e.g., tools’ types & use)
- Threat Modeling
- Cryptography
- Other Topics

LFD121 course even more relevant due to AI/ML

- "Traditional" vulnerabilities can seriously impact systems using AI/ML
  - E.g.: Two different cache system vulnerabilities seriously impacted ChatGPT in 2023
  - Common blind spot - AI/ML experts often unaware of these issues, need to fill gap
    - 73% in data science report lack of awareness & training as a challenge for implementing secure software development & deployment [LF 2024 Survey Report]
- LFD121 provides basic intro to AI/ML-specific security issues & concepts
- AI currently generates code with *more* vulnerabilities
  - Humans must detect & counter vulnerabilities generated by AI

Sources: "OpenAI Reveals Redis Bug Behind ChatGPT User Data Exposure Incident" by Ravie Lakshmanan <https://thehackernews.com/2023/03/openai-reveals-redis-bug-behind-chatgpt.html> ; LF 2024 Survey Report <https://www.linuxfoundation.org/research/software-security-education-study>; "Do Users Write More Insecure Code with AI Assistants?" by Neil Perry, Megha Srivastava, Deepak Kumar, Dan Boneh, Dec 2022, <https://arxiv.org/abs/2211.03622>; "Security Vulnerabilities of ChatGPT-Generated Code" by Trend Micro <https://www.trendmicro.com/en_us/devops/23/e/chatgpt-security-vulnerabilities.html>; blog post <https://madappgang.com/blog/chat-gpt-code-errors/>; : "Security Weaknesses of Copilot Generated Code in GitHub" by Fu et al, 2023-10-03, <https://arxiv.org/abs/2310.02059>

Please have your software developers enroll in LFD121!

- “Start here” if you develop software & don’t know how to develop *secure* software
- Encourage all software developers (who haven’t had any such course) to enroll
- Check out LFD121 at: https://hubs.la/Q02S4t2X0

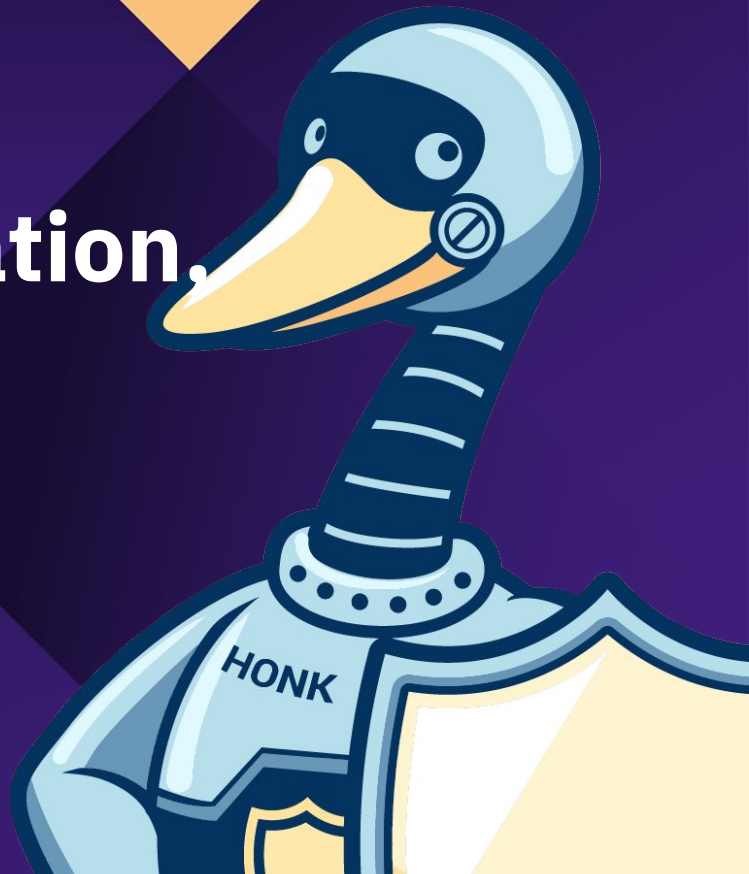
Other OpenSSF Educational Materials

- Existing courses
  - “Developing Secure Software” (LFD121), as noted
  - “Securing Projects with OpenSSF Scorecard” (LFEL1006)
  - “Securing Your Software Supply Chain with Sigstore” (LFS182x)
  - See: https://openssf.org/training/
- In development
  - “Security for Software Development Managers” (LFD125)
  - “Security Architecture” (for-pay, profit returns to LF/OpenSSF so we can do more)
- For more about OpenSSF & materials available, see https://openssf.org!
- Education/need for cyber-related skills known to be important
  - E.g., EU Cyber Resilience Act (CRA)

Insights from LF Education, What's available?

Glenn ten Cate,

Senior Cyber Security Instructor at the Linux Foundation



Insights from Linux Foundation

Linux Foundation Training & Certification has officially changed its name to

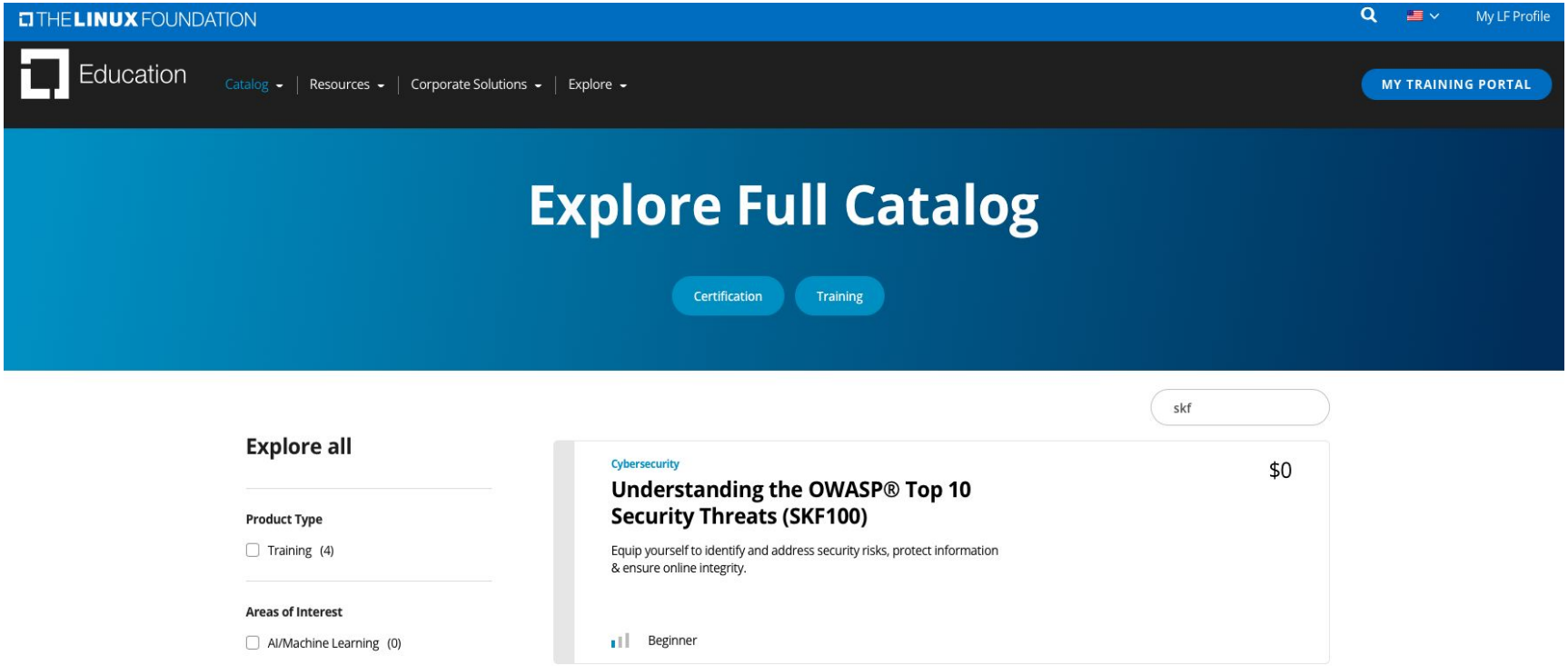
Insights - CyberSecurity Framework

Linux Foundation Education is about to release the **CyberSecurity Framework**

- Broad Applicability
  - Designed for a wide range of job families, not limited to cybersecurity professionals.
  - Every organization, regardless of size or industry, can benefit from implementing this framework.
- Calibrated by Experience
  - Tailored to different levels of expertise, from entry-level to senior roles.
  - Provides guidance based on real-world experience and varying needs.
- Continuous Updates and Community Support
  - Commitment to annual updates – a **living document**, unlike frameworks that update every 5 years.
  - Ongoing improvements and relevance for organizations using it..

Connect with me later to learn more!

Insights - Course Catalog



Insights - Instructor led trainings

THE LINUX FOUNDATION

My LF Profile

Education

Catalog | Resources | Corporate Solutions | Explore

MY TRAINING PORTAL

Training > Cybersecurity > Securing Coding Fundamentals (WSKF601)

INSTRUCTOR-LED COURSE

Securing Coding Fundamentals (WSKF601)

Empower yourself to write and verify secure software by design. Learn and practice with hands-on labs that build behavior-changing skills fundamental to security implementation, boosting your professional IT security maturity.

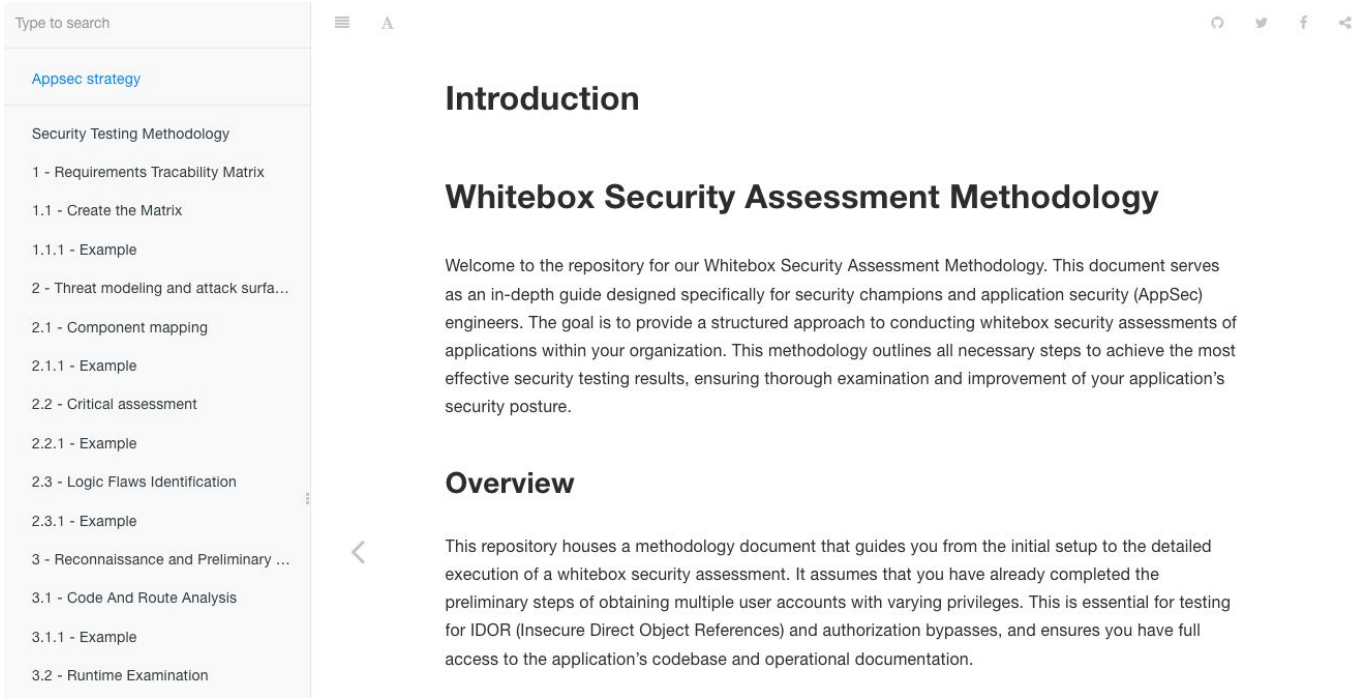
Key Benefits for You:

✔ Live, instructor-led hands-on labs
✔ Learn to incorporate security into your software design process
✔ Increase your productivity and the security of your coding

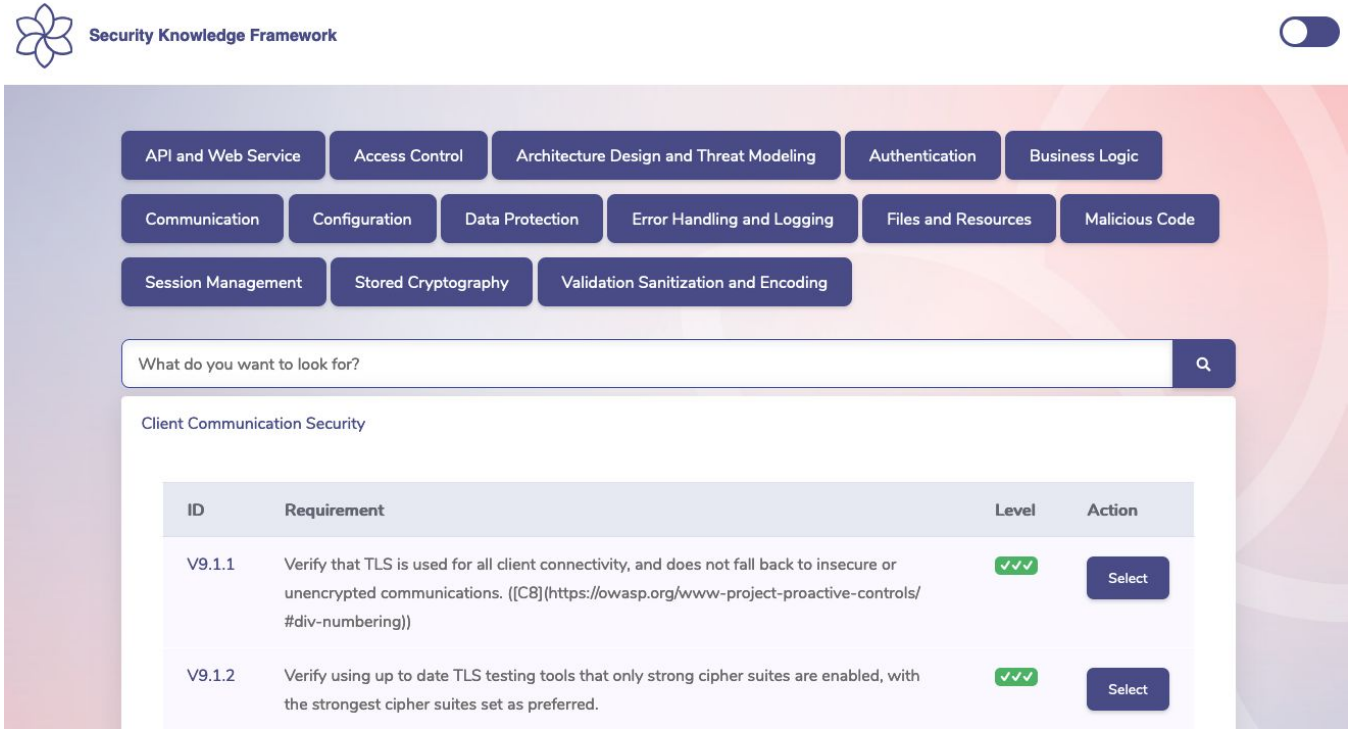
Linux Foundation Education - Security Courses

- Existing courses
  - “Understanding the OWASP® Top 10 Security Threats” (SKF100)
  - “Mastering Infrastructure Security: Strategies, Tools, and Practices“ (SKF200)
  - “XSS Exploits and Defenses” (LFEL1010)
  - “Understanding Vulnerabilities and Security Threats” (WSKF603) ILT
  - “Securing Coding Fundamentals” (WSKF601) ILT
- In development
  - “Threat Modeling” (SKF201) - release this month
  - “Security Deployment and DevOps“ (SKF202)
  - “Security Testing and Code Review“ (SKF203)
- For more about courses and certifications, see https://training.linuxfoundation.org/full-catalog/

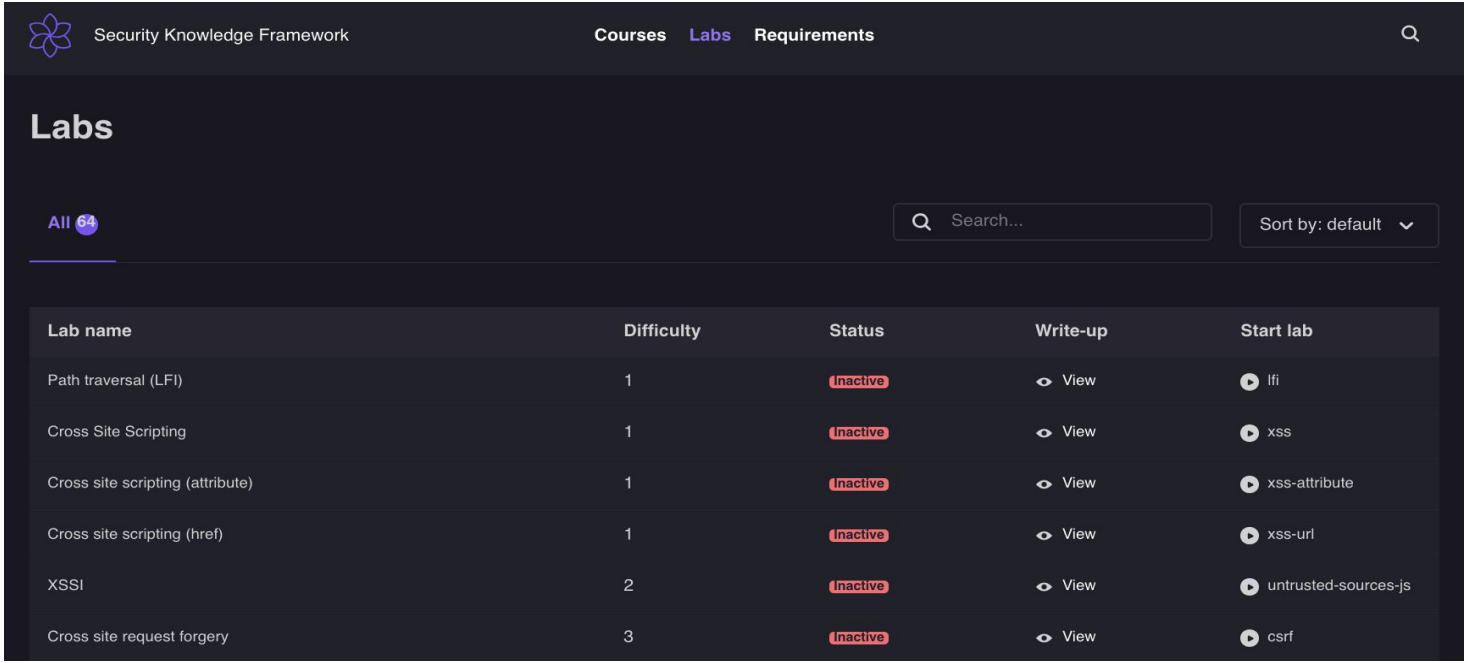
Insights from Linux Foundation - AppSec strategy



Insights from Linux Foundation - Requirements tool



Insights from Linux Foundation - Free labs



Insights from Linux Foundation - Writeups labs

Security Knowledge Framework

- **Introduction**
- Auth Bypass
- Auth Bypass - 1
- Auth Bypass - 2
- Auth-bypass - 3
- Auth-bypass - Simple
- Client Side Restriction Bypass
- Client Side Restriction Bypass - Harder
- Client Side Template Injection (CSTI)
- Command Injection (CMD)
- Command Injection 2 (CMD-2)
- Command Injection 3 (CMD-3)
- Command Injection 4 (CMD-4)
- Command Injection Blind (CMD-Blind)
- Content-Security-Policy (CSP)

Introduction

security knowledge framework

Here we find all the labs and write-ups for the security knowledge framework! These labs are correlated to knowledge-base id's which are on their place again correlated to security controls such as from the ASVS or NIST, etc.

The labs are all downloadable from the following Github repository:

SKF Labs repo

The images can also be found on the skf docker hub. These skf-labs images are automatically pushed to the docker registry on each commit to the Github repository.

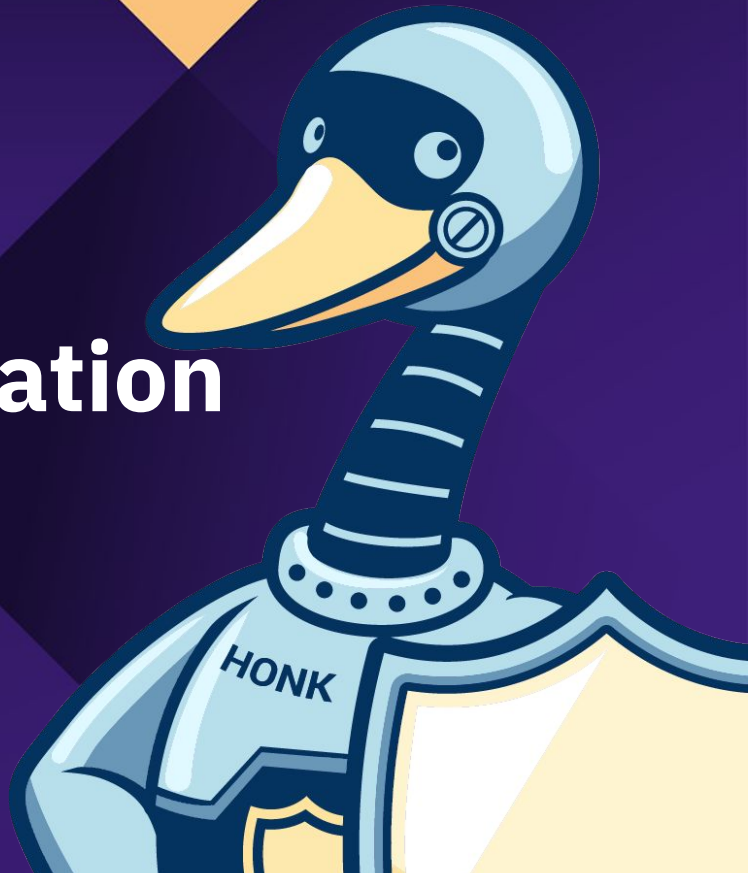
Linux Foundation Education - Resources and links

- Courses & Trainings
  - https://training.linuxfoundation.org/full-catalog/
- More free labs
  - Labs:
    - https://secureby.design/labs
  - Writeups:
    - https://skf.gitbook.io/asvs-write-ups
- Security requirements tool
  - https://starfish-app-kd3eo.ondigitalocean.app/
- Open Source AppSec strategy methodology
  - https://appsec.secureby.design/

Insights from Implementing Organization

Sarah Evans

Security Research Technologist, Dell Technologies



Insights from an Implementing Organization

- Enterprises have often have internal secure software development programs, which include employee training requirements and internal software development requirements

- Linux Foundation (or foundations like OpenSSF under the Linux Foundation) may offer members a training benefit that includes access to educational courses and certificates

- Enterprises can integrate Linux Foundation courses into their Learning Management Systems (LMS)

OSS security = more secure software supply chain

- *Participating* in OSS development = the projects to which you contribute are a part of the software supply chain (and growing AI supply chain)

- *Contributing* to OSS used for technology innovation around the world = a OSS security vulnerability can have an outsized impact on the technology we use everyday.

- *Learning and applying* secure software development principles to OSS = reduce security impacts on our shared global software supply chain

Panel Discussion & Audience Q&A

Panel Prep - From Tech Talk announcement

- What are essential skills/foundational skills and advanced techniques needed to develop secure open source software?
- How can attendees/listeners gain this comprehensive training on essential skills from industry experts/resources in the Linux Foundation and OpenSSF?
- What examples of key/valuable certifications to enhance attendees/listeners careers in OSS security, and where can they find them?
    - If a listener has already taken coding classes in college or a bootcamp, what value will they receive from also taking the Secure Software Development course? What about other Linux Foundation courses? - Sarah + pile on
    - If a listener has already experience coding, perhaps even already participating in OSS, what value will they receive from also taking the Secure Software Development course? What about other Linux Foundation courses? David
- What are examples of practical applications and tools that enhance your ability to create and maintain secure OSS projects?
- Where can listeners/attendees learn these skills through real-world scenarios and tools?
- If a listener is not a software developer, but works around/with software developers, what options do they have for learning about secure software development concepts? - David
- If there are attendees/listeners who are aspiring open source professionals and newcomers eager to step into the field of open source software security, how can they get started?
    - If a listener is not a software developer, but wants to pivot into the field of software developer, and be security conscious, what options do they have for learning about secure software development? - Glen

Developing Secure Software (LFD121)

The “Developing Secure Software” (LFD121) course is available on the Linux Foundation Education platform. Both the course and certificate (valid for 2 years) of completion are free. It is entirely online, takes about 14-18 hours to complete, and you can go at your own pace.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Upcoming Events

SOSS Fusion Conference

When: October 22-23, 2024

Where: Atlanta, Georgia 🍑

Register now!

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Ways to Participate

- Join a Working Group/Project
- Come to a Meeting (see Public Calendar)
- Collaborate on Slack
- Contribute on GitHub
- Become an Organizational Member
- Keep up to date by subscribing to the OpenSSF Mailing List

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Engage with us on social media

X
@openssf

LinkedIn
OpenSSF

Mastodon
social.lfx.dev/@openssf

YouTube
OpenSSF

Facebook
OpenSSF

Subscribe to our mailing list

openssf.org/sign-up

Is your organization a member?

Questions? Contact membership@openssf.org

openssf.org/join

Thank You

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Take our quick Tech Talk Survey

Help us improve!

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Legal Notice