OpenSSL CONFERENCE

Student Bug Bounties for OpenSSL-Based Products

Kamil Malinka

15.10.2026

What is bug bounty?

- A crowdsourced approach to vulnerability discovery
- Ethical hackers are rewarded for responsible vulnerability reporting
- Used by platforms and vendors such as **HackerOne, Bugcrowd, Apple, Microsoft, and Samsung**

15.10.2026

The problem

- Lack of cybersecurity experts
- Lack of real world assignments

15.10.2026

Our idea

- Give students hands-on experience with **real vulnerabilities**
- Introduce them to **ethical hacking workflows**
- Help prepare more students for **cybersecurity roles**

15.10.2026

Main questions

OpenSSL CONFERENCE

- Can beginners succeed in a real BBP?
- How do they approach the vulnerability hunting?
  - Tools
  - Methods
  - Strategies
- What do they learn?
- How do they perceive the experience?

Why Bug Bounties?

OpenSSL CONFERENCE

- Teach students to **think like an attacker**
- Build the mindset needed to **anticipate security threats**
- Provide **hands-on security experience**
- Security curricula are broad, with limited time for hands-on practice
- Especially relevant for **IT students outside cybersecurity specializations**

Course details

OpenSSL CONFERENCE

- Master's-level Secure Coding course
- **Not primarily an ethical hacking course**
- Introduces secure coding principles, vulnerabilities, and defenses
  - It covers multiple areas, such as basic vulnerabilities of compiled languages, memory protection mechanisms, input validation, static and dynamic analysis, and more
- Independent semester project
  - Approximately two months, 50% of the course grade
  - Technical report (6+ pages) and oral presentation
- Original project options: Tutorial, implementation, or original work

Experiment – additional project type

OpenSSL CONFERENCE

- New **voluntary** project option: Participate in a real-world bug bounty program
- Student autonomy: Choose from suggested programs or select their own
- Goal: Explore a real system, apply security testing techniques, and document the results
- Assessment: Methodology, tools, learning progress, and final report
- Finding a vulnerability was NOT required for a good grade

Preparation, Ethics and Safety

OpenSSL CONFERENCE

- Optional expert-led introduction
  - Ethical hacking methodologies and tools
  - Learning resources and bug bounty platforms
- Strict ethical and legal boundaries
  - Testing only within the authorized BBP scope and rules
  - Responsible reporting of discovered vulnerabilities
- Risk mitigation
  - No penalty for unsuccessful vulnerability discovery
  - Focus on learning, methodology, and responsible behavior
- Evaluation: Student questionnaire after completion

Results

Student's work on the assignment

15.10.2026

- Average run per year:
  - Approximately 40 students signed up for project/30 successful
- 15-20 students chose BBCh/10-15 successful (12 filled survey)

- The previous experience did not appear to be a major role in selecting this assignment
- The reason for selecting a specific BBP was prior experience with and knowledge of the given system
  - In addition, the majority of the selected BBPs were focused on the security of web applications

BBP Selection

Some students participated on multiple BBPs

15.10.2026

- 5x T-Mobile – due to BBP **availability in native language**
- 3x HackerOne - specifically Shopify's Bug Bounty, Epic Games, and Boozt Fashion AB.
- Other programs were covered by only one of the students:
  - Hacker101
  - Coinbase
  - Moneta
  - Microsoft
  - Hacktrophy
  - Own code

OpenSSL CONFERENCE

Used strategies

How students approached the search

- Mostly relied on **checklists, guides, and tutorials**
  - e.g. OWASP WSTG
- Tested for **known vulnerability classes**
- Some built on **prior personal experience**

- Time frame set for this project (40-60 hours)
- Most students have spent:
  - 15-30 hours with theoretical preparation
  - 15-30 hours with vulnerability identification

Overview of used learning resources

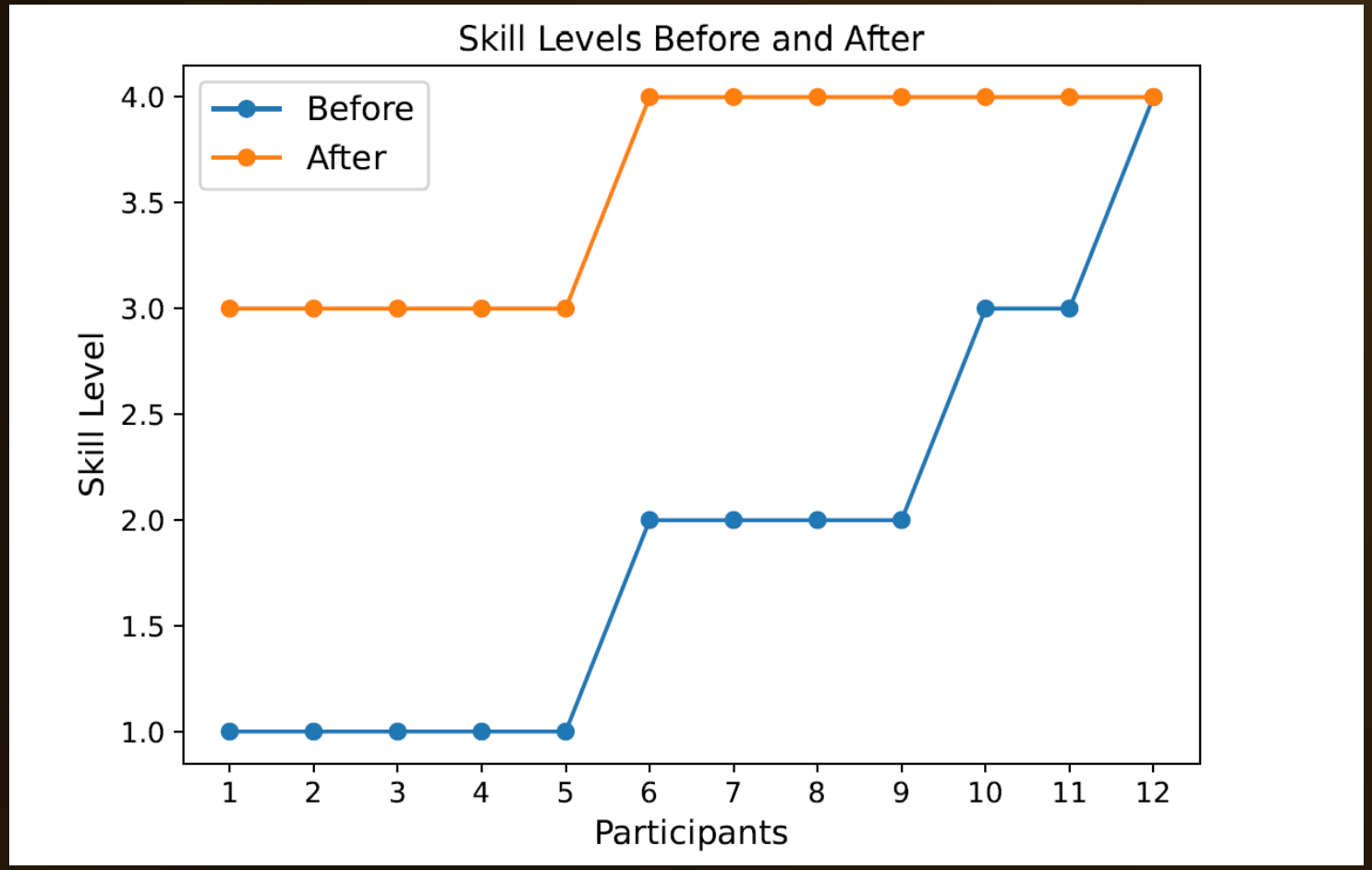
OpenSSL CONFERENCE

- Majority of students utilised the materials we suggested for their additional learning
  - TryHackMe
  - HackTheBox
  - PicoCTF
- Tools used by students:
  - Burp-Suite, Wappalyzer, Kali Linux, Nmap, Ffuf, Metasploit and others
- Reflects the variability of the BBP, as different implementations of the tested systems require different analytical tools

Resource	*Times reported*
PortSwigger academy	8
Videos	5
TryHackMe	3
OWASP	2
Online blogs	2
Hacker101	2
School lectures	1
Scientific literature	1

Results

Student's self-evaluation of educational impacts



Student Background and Outcomes

OpenSSL CONFERENCE

- Before the project
  - ~50% had theoretical knowledge only
  - Others had limited practical experience
  - Only one student had substantial prior hands-on training
- After the project
  - Better orientation in ethical hacking
  - Practical understanding of penetration testing phases
  - Better understanding of the attacker's perspective
  - Practical experience with security tools
- Cybersecurity career interest
  - 41.7% → 50%

Table 2: Personal likings of the project as reported by students. The responses ranged from 1 - 5, where 1 means the worst (negative) and 5 means the best (positive). σ denotes the standard deviation.

Question	Mean	σ
How much would you like to see this type of project incorporated into regular teaching?	4	0.85
Is the project content beneficial even if the participant has a career path outside of cybersecurity?	3.91	0.79
How do you feel about working in a real environment on real products?	3.92	0.99
How important is the project's social impact to you (helping to improve real safety)	3.42	1.08

Results

Student's self-assessment of the project

- Very beneficial primarily due to the great practical overlap and the ability to work on real problems from practice
- High degree of freedom of the project
- Need for self-study to a greater than usual extent, as the project allowed them to get an assessment in an area that interested them

- *"If this project is chosen by a person who is interested and fond of this field, it is the most useful and interesting project at the school at all."*

Negatives

- Stress of breaking BBP rules
- Frustration of not finding any vulnerabilities

OpenSSL CONFERENCE

Results

How many vulnerabilities actually found?

- Student-reported potential vulnerabilities
  - One student discovered an Insecure direct object reference (IDOR) but did not report it, as the tested platform did not have a proper BBP
  - The second student discovered two potential vulnerabilities (CSRF and incorrect validation of redirect link after login)
    - Reported to the BBP, but no response had yet been received
  - He also found small number of cases of non-standard behaviour:
    - Ex. the existence and availability of non-actual pages or error messages available to users, etc.
    - It is unclear whether or not these instances could be used to mount a successful attack. However, they still violate best practices and should potentially be fixed

Lessons learned

OpenSSL CONFERENCE

- Students **can** identify real vulnerabilities
- Encouraging positive feedback
- Project was deemed beneficial by those participants who do not intend to pursue a career in cybersecurity
- **More focus on legal impacts**
- It proved **essential to allow freedom in the students' choice of technology** by selecting a suitable BBS – saves time, friendly environment with known technology
- **Focusing the assessment on progression** rather than finding vulnerabilities
- According to the feedback, we are considering how to appropriately **integrate existing online courses on ethical hacking**, which students widely used to gain detailed knowledge

OpenSSL CONFERENCE

What happened next?

The students wanted more

- 4 years of continuous interest
  - Approximately 15 students per year
  - One or two of them will find something interesting
- Interest in full-fledged bachelor's theses on this topic
    - 3 already completed
  - Biggest success:
    - From a user account, student successfully elevated privileges to gain admin RDP access to the backend server (already fixed ☺)

OpenSSL CONFERENCE

How OpenSSL Keeps Its Code Secure

- Peer-reviewed development: Pull requests, code reviews, and established contribution policies
- Extensive automated testing: CI pipelines, regression tests, fuzzing (LibFuzzer/AFL), and sanitizers
- Strict release quality gates: Successful CI, Coverity findings reviewed, test coverage monitored, and formal release approval
- Coordinated vulnerability response: Dedicated Security Response Team, severity classification, security advisories, and advance notification to selected distributors

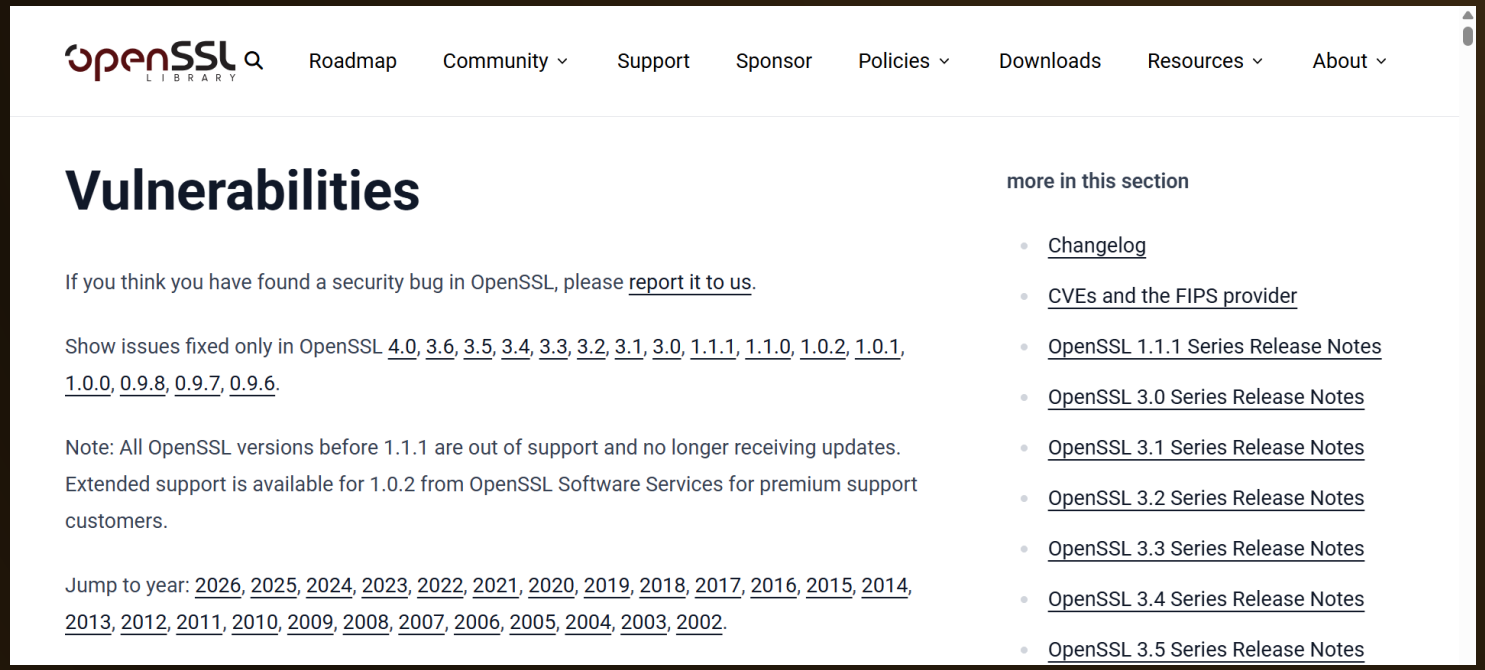
OpenSSL CONFERENCE

Does OpenSSL Need a Bug Bounty?

- Independent audit (Trail of Bits, 2024):
  - 24 security-related findings: 4 medium, 6 low, 14 informational.
  - No findings required a CVE; four new fuzzers were developed.
  - Auditors praised defensive implementation and extensive testing
- Established vulnerability handling: A dedicated Security Response Team coordinates fixes, advisories, and responsible disclosure
- No OpenSSL-operated bug bounty: Researchers can still report vulnerabilities, with potential rewards from third-party programs

15.10.2026

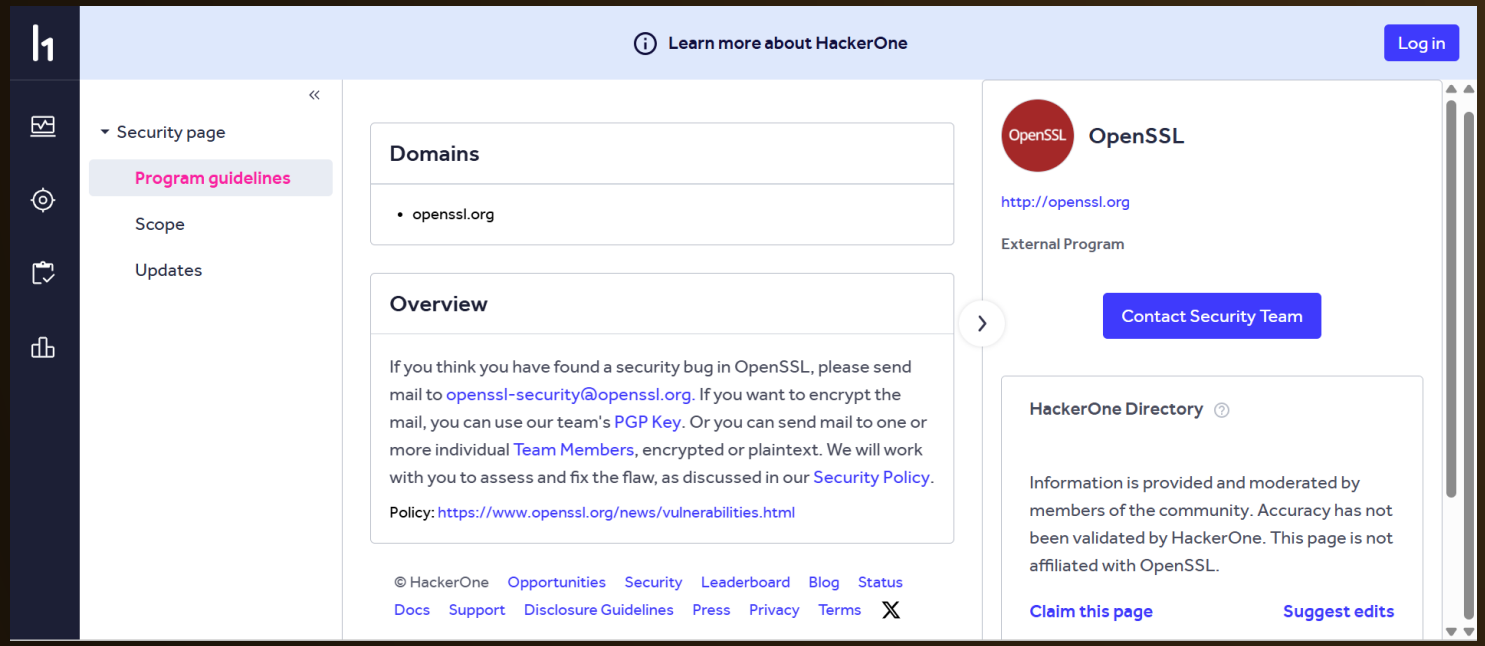
Yet...

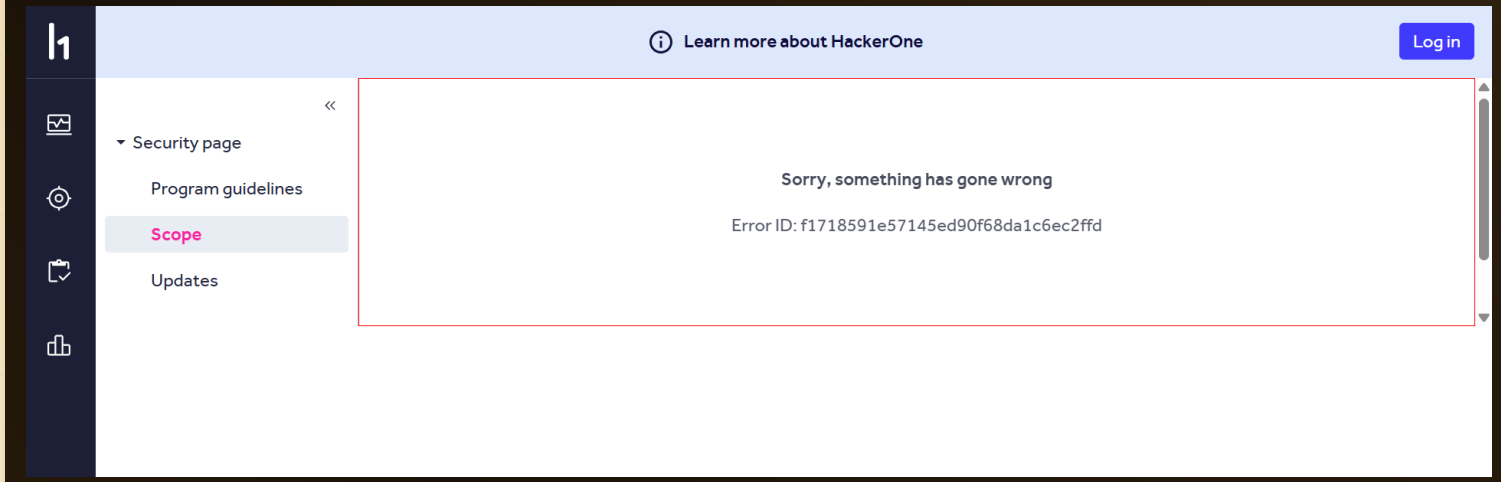

OpenSSL LIBRARY
Roadmap
Community
Support
Sponsor
Policies
Downloads
Resources
About
Vulnerabilities
If you think you have found a security bug in OpenSSL, please report it to us.
Show issues fixed only in OpenSSL 4.0, 3.6, 3.5, 3.4, 3.3, 3.2, 3.1, 3.0, 1.1.1, 1.1.0, 1.0.2, 1.0.1, 1.0.0, 0.9.8, 0.9.7, 0.9.6.
Note: All OpenSSL versions before 1.1.1 are out of support and no longer receiving updates. Extended support is available for 1.0.2 from OpenSSL Software Services for premium support customers.
Jump to year: 2026, 2025, 2024, 2023, 2022, 2021, 2020, 2019, 2018, 2017, 2016, 2015, 2014, 2013, 2012, 2011, 2010, 2009, 2008, 2007, 2006, 2005, 2004, 2003, 2002.
more in this section
Changelog
CVEs and the FIPS provider
OpenSSL 1.1.1 Series Release Notes
OpenSSL 3.0 Series Release Notes
OpenSSL 3.1 Series Release Notes
OpenSSL 3.2 Series Release Notes
OpenSSL 3.3 Series Release Notes
OpenSSL 3.4 Series Release Notes
OpenSSL 3.5 Series Release Notes

OpenSSL CONFERENCE

Yet...

https://hackerone.com/openssl





15.10.2026

OpenSSL CONFERENCE

Final thoughts

- We have mature security processes
  - Code reviews, automated testing, fuzzing, independent audits
- We now have increasingly powerful AI-assisted tools
  - Making sophisticated security analysis more accessible than ever
- But we also need the next generation of security researchers
  - People who question assumptions, think creatively, and understand the systems they test

- **What happens when we give motivated students powerful AI-assisted security tools?**
  - Will they find more vulnerabilities, or become better security researchers?

Thank you for your attention