

API Security Lab

Understanding and defending against attacks on APIs

Graduate



Corsin Salutt



Thajakan Thirunavukkarasu

Initial Situation: APIs play a crucial role in software development and digital business transactions. However, with the increasing spread and importance of APIs, there is also a growing threat landscape. This bachelor thesis aims to develop an API Security Lab curriculum for future students of the OST using the Hacking-Lab platform. This curriculum will provide practical exercises that allow students to apply theoretical concepts in a hands-on environment, simulating real-world scenarios and challenges.

Approach: The initial phase involves a comprehensive literature review, historical API usage, analysis of existing API security threats and standards. The awareness document on OWASP Top 10 API Security vulnerabilities from 2023 forms the basis for this work. It describes the most critical vulnerabilities that organizations should address to secure their API's. In the next phase, lab ideas are developed based on the OWASP Top 10 API Security risks to provide participants with various aspects of API Security. The challenge ideas are fitted into a generic framework to enable comparison, even though they differ in context. The final part involves going through a selection based on meaningful criteria and evaluating labs to determine the final candidates.

Result: As a result of this project, six challenges were created on the Hacking-Lab platform. Each lab covers separate vulnerabilities from the OWASP Top 10 API Security awareness document. The labs can be divided into three categories: tool-based labs in which existing tools such as Burp Suite or Coraza WAF must be learned and used in a ready-made setup, implementation-based labs in which JavaScript applications must be secured, or where students have to exploit a vulnerable authentication flow.

OWASP Top 10 API Security Risks 2023
<https://owasp.org/API-Security/editions/2023/en/0x11-t10/>

OWASP Top 10 API Security Risks – 2023	
API1	Broken Object Level Authorization
API2	Broken Authentication
API3	Broken Object Property Level Authorization
API4	Unrestricted Resource Consumption
API5	Broken Function Level Authorization
API6	Unrestricted Access to Sensitive Business Flows
API7	Server-Side Request Forgery (SSRF)
API8	Security Misconfiguration
API9	Improper Inventory Management
API10	Unsafe Consumption of APIs

Rate limiting lab: Test report

Own presentation

Test Name	Expected Behavior	Actual Result	Status
Test execution timeout	should return 503 status code if the request times out	passed	1.00%
Maximum upload file size	should return 400 when file size exceeds limit	passed	0.00%
Book upload limit	should reject requests with more books 20 books	passed	0.00%
Book upload limit	should accept requests with a number of books below 9	passed	0.00%
Pagination tests	should return the first page of books by default	passed	0.00%
Pagination tests	should return the second page of books	passed	0.00%
Rate Limiting	should allow up to 100 requests per 15 minutes	passed	0.00%

CONGRATS YOU SOLVED THE LAB, PLEASE COMMIT THE FOLLOWING FLAG: 4ab9a724-1386-47d4-ba62-53642a20af4a

Hacking-Lab: Labs overview

Own presentation

#	Name	Categories	Level	Mode	Grading
1	API Security: Implementing logging c677a441-ca4e-47cc-9a16-781d1bccc1f1		easy		
2	API Security: Enumeration and reconnaissance 88be97cc-80bb-4da3-b795-500269ed74c1		medium		
3	API Security: OAuth2 Vulnerabilities 80b957ed-1513-46c9-85a8-c067a998c6f0		easy		
4	API Security: OWASP Coraza WAF bc69d9ac-309e-4055-a33c-059c1970dff8		medium		
5	API Security: Rate limiting 4b590bdc-c5e2-4fd5-b119-92f6362c1a0d		medium		
6	API Security: Input validation and sanitization 66bd4e25-675c-424d-9076-100d95ee8a04		easy		

Advisor

Ivan Bütler

Co-Examiner

Dr. Benjamin Fehrenschen, Berner Fachhochschule, Bern, BE

Subject Area

Networks, Security & Cloud Infrastructure, Security

