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.

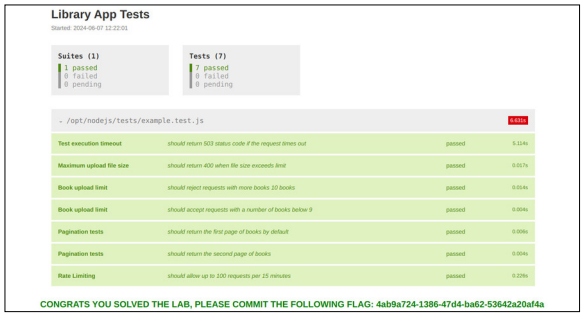
Approach: The initial phase involves a comprehensive literature review, historical API usage, analysis of existing API security threats and standards. The awareness document on OWASP Top 10 API Security vulnerabilities from 2023 forms the basis for this work. It describes the most critical vulnerabilities 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.

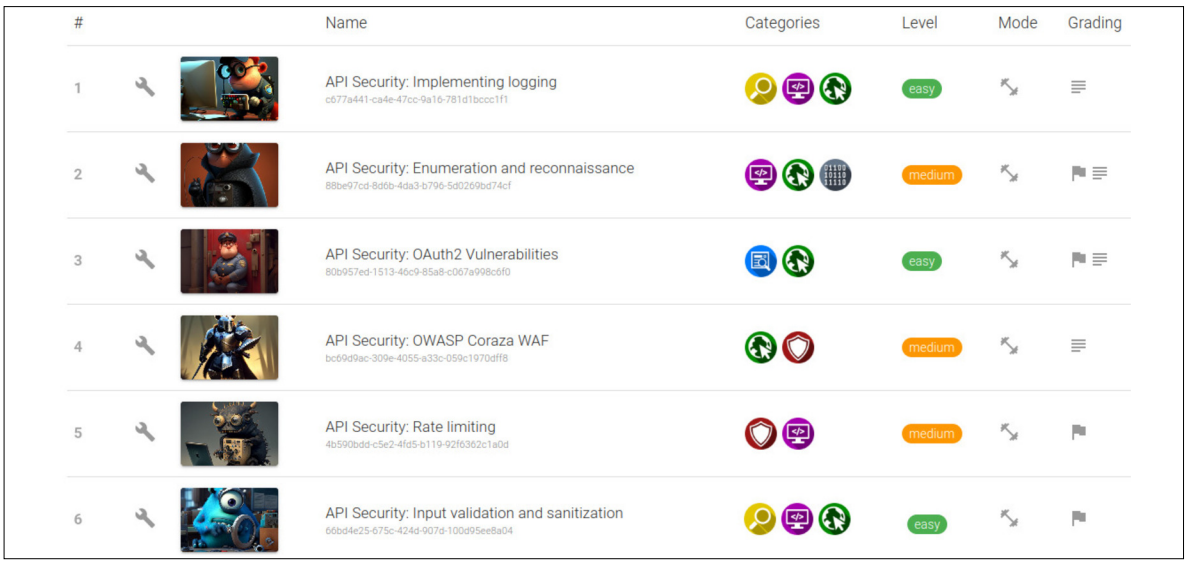
OWASP Top 10 API Security Risks 2023
https://owasp.org/API-Security/editions/2023/en/0x11-t10/

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 presentment



Hacking-Lab: Labs overview
Own presentment



Advisor
Ivan Bütler

Co-Examiner
Dr. Benjamin Fehrensen, Berner Fachhochschule, Bern, BE

Subject Area
Networks, Security & Cloud Infrastructure, Security