

Project – CVE discovery and reporting

Version 1.0.1

Updated: 2023-10-27.

1. Introduction to the project

Learning outcomes

- Learn the different stages of identifying a new vulnerability and reporting it.
- Learn about the process of issuing a CVE.
- Applying the knowledge to identify a vulnerability in an **open-source solution**.

Groups

The team should be composed by 4 students. Students who are unable to form a group within the first week should contact the teacher to agile the process. Missing submission deadlines as a result of this issue will not be considered a valid excuse.

Stages

The project is divided into three stages (with different grading weights).

2.1 Scope

The first stage is based on the scope definition. Students are expected to establish specific criteria for the selection of open-source repositories to be subsequently analyzed. These criteria may include factors such as:

- the programming language of the solution;
- the usage environment (e.g., desktop or web);
- the area of the assessment (e.g., access control, architecture, both, and/or others)
- other relevant considerations.

Additionally, the students should identify a set of criteria that will be used as guidelines during the assessment of these open-source repositories. See OWASP Application Security Verification Standard (ASVS) for inspiration.

2.2 Initial assessment and first findings

In the second phase, your objective is to identify a vulnerability and create a proof-of-concept demonstrating how to exploit this vulnerability. This phase entails submitting a comprehensive report and maintaining a private GitHub repository, accessible to the user 'joaorafaelalmeida,' containing the code necessary to replicate your findings

2.3 Findings and CVE issuing experience

In the final phase, the team should proactively reach out to the software vendor to address and initiate the CVE issuance process for the identified vulnerability. In the last week, the group should present their findings to the class, which should include a comprehensive final report summarizing all stages of the project and a 15-minute presentation accompanied by slides.

3. Deadlines

Each task comes with a firm deadline, and it is crucial to adhere to these dates.

- First task: Due by 11:50 pm on 09/11/2023
- Second task: Due by 11:50 pm on 01/12/2023
- Third task: Due during the class on 22/12/2023, with the report to be submitted by 11:50 pm on the same day.