SE4030– Secure Software Development

Assignment

Marks allocated – 25

Note that this is a group assignment. Maximum group size is 4. The groups may include a mix of weekday and weekend students.

Consider any web or mobile application that you may have already developed or an application whose source code is available online (**the last commit date of the original code should be earlier than the start date of the semester**). Identify at least 8 vulnerabilities of that application and try to fix them. You may use security related open-source testing tools (both black box and white box testing tools) to identify potential vulnerabilities. Write a report on the vulnerabilities that were there in the original application and how these vulnerabilities were fixed. Identify any vulnerabilities that were not fixed and the reason for not fixing them. You may describe the best practices in software engineering processes that may have prevented these vulnerabilities being introduced in the first place.

Further, implement an OAuth or OpenID connect based grant type to add a new feature or an update an existing feature in the application. You may use any publicly available OAuth server (google, Facebook, etc) or any open-source OAuth server (e.g. WSO2 identity server) for this task.

Note: When choosing an app for the assignment DO NOT choose a well-known app that is used for learning purposes (webgoat, Damn Vulnerable Web app (DVWA)), etc). Instead, use an app where the improved version is not publicly available and an app that is NOT currently used to teach about vulnerabilities.

Presentations and vivas will be scheduled towards the end of the semester.

Deliverables.

1. Readme text file with the following information.

   Member names and index numbers.

   Github link to the original project (if it's a third-party project, include the reference to that project).

   Github link to the modified project after fixing the vulnerabilities

   Link to a Youtube video describing the vulnerabilities and the fixes done and the OAuth/Open ID connect implementation. Maximum video length 10 minutes. Each member may use maximum 2.5 minutes to explain their contribution.

2. Report in pdf format.

Upload all the files as a single zip file to the courseweb submission link.

Some useful references:

1. https://owasp.org/www-project-top-ten/
2. https://owasp.org/www-project-mobile-top-10/
3. https://owasp.org/www-project-java-encoder/
4. https://owasp.org/www-project-dependency-check/
5. https://www.zaproxy.org/
6. https://owasp.org/www-project-webgoat/#:~:text=WebGoat%20is%20a%20deliberately%20insecure,and%20popular%20open%20source%20components.
7. https://github.com/digininja/DVWA
8. https://github.com/payatu/diva-android
9. https://github.com/appsecco/dvna
10. https://github.com/logicalhacking/DVHMA
11. https://sqlmap.org/

Marking rubric

Marking criteria	Good (10-8)	Average (7-4)	Poor (3-0)
Choosing an application with sufficient scope and complexity			
Identifying potential vulnerabilities			
Fixing the vulnerabilities			
Implementing an OAuth/Open ID connect based function			
Discussion			
Individual contribution			
Viva			