A Gradišćanska 24, HR-10000 Zagreb
T (01) 2222 182
E student@algebra.hr
www.algebra.hr

ALGEBRA

Secure coding – project description

The following document describes the expected deliverables based on the chosen web application. Each module needs to be adequately implemented to pass the learning outcome.

MODULE 1 (15 points): Use tools OWASP ZAP and Burp Suite to scan your application for vulnerabilities. Choose three most significant vulnerabilities, document them, fix them and re-scan the application to prove that the vulnerabilities are fixed.
MODULE 2 (15 points): Use SonarQube tool and scan your application for the bugs. Choose three most significant bugs, document them, fix them and re-scan the application to prove that the bugs are fixed.
MODULE 3 (15 points): implement a JWT access and refresh token in your web application and document the example of token usage.
MODULE 4 (15 points): analyze the SQL injection vulnerability of your application with one of available tools online (for example: https://pentest-tools.com/website-vulnerability-scanning/sql-injection-scanner-online), document the potential bugs and describe the current way how the application protects it's database from SQL injection attacks.
MODULE 5 (15 points): implement an example of serialization (if it does not exist in your application) and implement the deserialization protection based on whitelisting the classes that can be deserialized.
MODULE 6 (13 points): use the best practices in implementing authentication and authorization to prevent unauthorized access to confidential data.