Project:

STUDY CONTROL SYSTEM FOR UNIVERSITIES
DIPLOMADA#1100266
MILESTONE 2 COMPLIANCE REPORT
Web source code security and infrastructure vulnerability testing

1. GENERAL INFORMATION:
- Project Name: DIPLOMADA
- Test Date: Wednesday, May 15, 2024
- Objective of Testing: Determine and correct vulnerabilities at the application and infrastructure level.

2. WEB SOURCE CODE SECURITY TESTING:
- Static analysis of the source code:
- Tools used: BASE64-based encryption module that generates a hash in Laravel
- Vulnerability Findings: None
- Severity of Vulnerabilities: None

Personal comments from NandoVitti: I think it can be commented here that the application is protected against SQL Injection and Cross Scripting attacks. In addition, validations are carried out on the client side.

- Dynamic analysis of the source code:
- Tools used: Laravel TEST
- Vulnerability Findings: None
- Severity of Vulnerabilities: None

3. INFRASTRUCTURE VULNERABILITY TESTING:

- Infrastructure Vulnerability Scanning:

- Used tools:
IP address and logical port verifier

- Scan Results: None. Remote access ports are closed and access is only allowed via ports 80 and 443.

- Severity of Vulnerabilities: None

- Security Configuration Evaluation:

- Secure Configurations Implemented: Allowed ports 80 and 443

- Areas of Improvement in Configuration: None

4. FINDINGS AND RECOMMENDATIONS:

- Web Source Code Security Findings:
- Strong Points: the structure of the code generates robustness in the security of the system, since it allows us to quickly locate functionalities that could have been affected by an attack for verification and correction
- Critical Vulnerabilities: None

- Infrastructure Vulnerability Findings:

- Strong Points: Firewall, Proxy, IPS and IDS Service. With these security techniques, possible intrusions from the outside are minimized. A Web Firewall will be installed to block possible layer 7 attacks.

- Critical Vulnerabilities: None.

- General Recommendations: Ensure physical security with an additional UPS. More rigorous Access Control and CCO grounding bar connection.

5. CONCLUSIONS:

- Summary of the results obtained in security tests:

There is good logical security by allowing communications to enter only those IP addresses and ports necessary for the applications.

A WAF (Web Application Firewall) must be configured to implement protection at layer 7.

Properties and permissions are established at the user level for directories (folders) with sensitive information.

- Importance of addressing these aspects to protect the system against possible attacks:

These aspects guarantee the availability of applications and prevent denial of service (DoS) attacks.

- Suggestions for future testing or system security improvements:

In the near future, a system monitoring system must be installed that allows corrective and preventive maintenance to be quickly addressed at the level of networks, servers, applications and security equipment.