COMPREHENSIVE SECURITY TEST[1] No 8

BACKGROUND INFORMATION[2]:

Related reform	3.5 Reconfiguration of basic digital services and safe transition to cloud infrastructure
Target name	58. Central security testing of public authorities' information systems
Target description	Number of comprehensive security tests carried out by the Information System Authority – the test results shall be summarised in reports.
The test was financed by the European Union from the NextGenerationEU Recovery Fund.	

PENETRATION TESTING INFORMATION:

Date / period of testing	09.05.2024 – 15.05.2024
Objective of the Penetration Testing	Detect vulnerabilities in existing web application using OWASP framework.
Approach, Scope and Caveats	Approach: White box testing with access to source code and configuration. Scope: OWASP ASVS 4.0.3 level 2
Penetration Testing Team	████████████████████████
Organisation	████████████
Penetration Testing Tools Used	██████████████████████████████
Summary of the penetration test performed	Configuration flaw with medium impact. Cryptography at rest flaw with medium impact. Business logic flaw with low impact. Error handling and logging flaw with low impact.
Summary of Penetration Testing Findings according to CVSS 3.1	2 findings with medium impact 2 findings with low impact
Prioritized Vulnerabilities Findings	Please see annex 1
Risk and Impact Ranked Findings	Please see annex 1
Follow-up activities	Report handed over to ███████████████ Fixing activities are pending.
Annex No and name (if relevant)	Annex 1 – Findings and Impact

---

[1] Comprehensive security test – penetration test
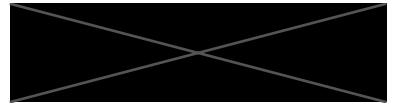
Annex 1 – Findings and Impact

CWE ID	Section	Confidentiality Impact	Integrity Impact	Accessibility Impact	CVSS 3.1 Score
1395	Configuration	Medium	Medium	None	6.2 Medium (Temporal metrics) Calculation
326, 327	Cryptography at Rest	Medium	Medium	None	4.4 Medium (Temporal metrics) Calculation
841	Business Logic	None	None	Medium	3.1 Low Calculation
117	Error Handling and Logging	None	Medium	None	3.5 Low (Temporal metrics) Calculation