



COMPREHENSIVE SECURITY TEST¹ No 19

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	25.11.2024 – 31.12.2024
Objective of the Penetration Testing	Detect vulnerabilities in existing web application using OWASP framework.
Approach, Scope and Caveats	Approach: Gray box testing with access to software documentation. Scope: OWASP ASVS 4.0.3 level 2
Penetration Testing Team	
Organisation	
Penetration Testing Tools Used	
Summary of the penetration test performed	Authentication flaw with medium impact. Authentication flaw with low impact. Input validation flaw with low impact. Configuration flaw with low impact.
Summary of Penetration Testing Findings according to CVSS 3.1	1 findings with high impact 3 finding with medium 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

Comprehensive security test – penetration test



Annex 1 – Findings and Impact

CWE ID	Section	Confidentiality Impact	Integrity Impact	Accessibility Impact	CVSS 3.1 Score
540, 1002	Authentication	Medium	Medium	Medium	8.1 High Calculation
330	Authentication	Low	Low	None	6.5 Medium Calculation
20	Input Validation	Low	Low	Low	5.0 Medium Calculation
1021	Configuration	Low	Low	Low	4.4 Medium (Temporal metrics) Calculation