[redacted]

COMPREHENSIVE SECURITY TEST[1] No 3

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	24.01.2024 – 31.01.2024
Objective of the Penetration Testing	Detect vulnerabilities in existing web application using OWASP framework.
Approach, Scope and Caveats	Approach: White box testing using existing non-privileged user account and access to source code. Privileged account for final testing. Scope: OWASP ASVS 4.0.3 level 2
Penetration Testing Team	[redacted]
Organisation	[redacted]
Penetration Testing Tools Used	[redacted]
Summary of the penetration test performed	Input validation flaw with high impact. Session management flaws with medium impact. Error handling flaw with medium impact. Configuration flaw with medium impact.
Summary of Penetration Testing Findings according to CVSS 3.1	3 findings with high impact
Prioritized Vulnerabilities Findings	Please see annex 1
Risk and Impact Ranked Findings	Please see annex 1
Follow-up activities	Report handed over to [redacted] 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
79	XSS in file upload element label field	Medium	High	Low	8.2 (High) Calculation
79	XSS in radio form label field	Medium	High	Low	8.2 (High) Calculation
79	Potential XSS in createBadge	Informational	Informational	Informational	8.2 (High) Calculation

[1] Comprehensive security test – penetration test