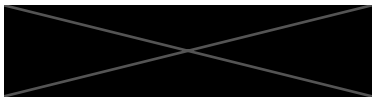
[redacted]

COMPREHENSIVE SECURITY TEST[1] No 9

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	04.04.2024 – 19.04.2024
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. 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	Session management flaws with medium impact. Input validation flaw with medium and high impact. Cryptography flaw with medium impact. Communication security flaw with medium impact. Configuration flaws with low and medium impact. API and web services flaw with low impact. Malicious code flaw with medium impact.
Summary of Penetration Testing Findings according to CVSS 3.1	1 finding with high impact 13 findings with medium impact 1 finding 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 [redacted] Fixing activities are pen ng.
Annex No and name (if relevant)	Annex 1 – Findings and Impact

[1] Comprehensive security test – penetration test

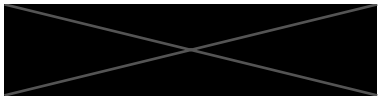
Article 35 subsection 1 clause 9 of Public Information Act: https://www.riigiteataja.ee/en/eli/503052023003/consolide; "9) information including a description of security systems, security organisations or security measures;"



Annex 1 – Findings and Impact

CWE ID	Section	Confidentiality Impact	Integrity Impact	Accessibility Impact	CVSS 3.1 Score
16	Session management	Low	Medium	None	6.4 Medium (Temporal variables) Calculation
601	Input validation	None	Low	None	3.3 Low (Temporal variables) Calculation
611	Input validation	Medium	Medium	Low	7.2 High (Temporal variables) Calculation
116	Input validation	Medium	Medium	Low	6.0 Medium (Environmental variables) Calculation
310, 326, 327, 798	Cryptography	Medium	Low	None	5.9 Medium (Temporal variables) Calculation
295	Communication security	Medium	Medium	Low	6.0 Medium (Temporal variables) Calculation
507	Malicious code	None	None	Medium	5.1 Medium (Temporal variables) Calculation
650	API and web services	None	Low	Low	4.2 Medium (Temporal variables) Calculation
497	Configuration	Medium	Medium	None	6.0 Medium (Temporal variables) Calculation

[1] Comprehensive security test – penetration test



Annex 1 – Findings and Impact

200	Configuration	Low	None	None	4.0 Medium (Environmental variables) Calculation
1021	Configuration	Medium	Medium	None	5.2 Medium (Temporal variables) Calculation
116	Configuration	None	Medium	Low	5.2 Medium (Temporal variables) Calculation
523	Configuration	Medium	Medium	Low	6.0 Medium (Temporal variables) Calculation
116	Configuration	Low	None	None	4.1 Medium (Temporal variables) Calculation
1021	Configuration	Medium	Medium	None	5.2 Medium (Temporal variables) Calculation

[1] Comprehensive security test – penetration test