CyberSec Pro cyber-sec-pro.com

Executive Summary — Sample

Executive Summary

REPORT DATE	**SCANS PERFORMED**
2026-11-12 01:38 UTC	3 scan(s)
TOTAL FINDINGS	**RISK LEVEL**
21	Critical

CONFIDENTIAL — AUTHORIZED RECIPIENTS ONLY

Generated by CyberSec Pro | cyber-sec-pro.com

© 2026 CyberSec Pro. All rights reserved.

Table of Contents

01 Risk Assessment

02 Executive Summary

03 Action plan

04 Scans in this report

05 Methodology

06 Content digest

Executive Summary — Sample

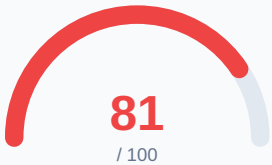
CyberSec Pro cyber-sec-pro.com

Executive Summary

Generated: 2026-11-12 01:38 UTC Scans: 3 Findings: 21 **Risk: Critical**

About this sample. This is a sample. Its three scans are real: they were run through CyberSec Pro on 12 November 2026 against scanme.nmap.org and testasp.vulnweb.com, hosts their owners keep online for people to practise on. The tool output is shown as it was recorded and the findings are what the product derived from it. Nothing was added or removed.

Risk Assessment



Overall Risk Score: 81/100

The risk score is calculated based on the severity and quantity of findings discovered during the assessment.

CRITICAL	HIGH	MEDIUM	LOW / INFO
1	0	1	19
4.8%	0.0%	4.8%	90.5%

Executive Summary

The assessment covered **3** target(s) with: **nikto, nmap, sqlmap**. Targets scanned: `http://testasp.vulnweb.com/showforum.asp?id=0` , `scanme.nmap.org` , `testasp.vulnweb.com` .

Fix first: **SQL injection in id (GET)** (critical, 1 target); **SSH** (medium, 1 target). The action plan lists every issue with its first step.

This security assessment was conducted on **2026-11-12** covering **3 scan(s)** across the target infrastructure. A total of **21 finding(s)** were identified, including **1 critical**, **0 high**, **1**

CONFIDENTIAL

medium, and **17 low** severity issues. Overall risk level: **Critical**.

Action plan

Worst first. Each row is one issue, with every place it was found; the full steps are in the Technical Report over the same scans. Informational findings are left out.

#	FIX BY	ISSUE	WHERE	FIRST STEP
1	CRITICAL Now	**SQL injection in id (GET)**	http://testasp.vulnweb.com/showforum.asp?id=0	Find the query that uses the named parameter and rewrite it as a parameterized query (prepared statement). Never build SQL by joining strings with request values.
2	MEDIUM Within 30 days	**SSH**	scanme.nmap.org, port 22	Restrict SSH to known management addresses with a firewall rule or security group.

13 low-severity items are left for the next maintenance window. The Technical Report over the same scans lists each of them with the steps.

Scans in this report

#	SCAN	TARGET	COMPLETED	CRITICAL	HIGH	MEDIUM	LOW	INFO
1	**sqlmap**	http://testasp.vulnweb.com/showforum.asp?id=0	2026-11-12 01:38	1	0	0	0	0
2	**nmap**	scanme.nmap.org	2026-11-12 01:31	0	0	1	1	1
3	**nikto**	testasp.vulnweb.com	2026-11-12 01:33	0	0	0	16	1

Each finding, the steps to fix it and the tools' own output are in the Technical Report over the same scans.

Methodology

This assessment was performed with **CyberSec Pro**, using the tools named with each scan under Scans in this report. Every target was either a public practice host or confirmed in writing, by the person who started the scan, as one they are authorized to test.

Platform	CyberSec Pro v4.0
Report Template	Executive Summary
Generated	2026-11-12 01:38 UTC
Classification	Confidential
Data residency	Canada

Automated assessment

Produced by CyberSec Pro — not reviewed by an analyst

Content digest

Generated: 2026-11-12 01:38 UTC | Scan ID: e7b7a6fa-261f-4048-b677-47293899b729

SHA-256: 5df2fd3a32679aa9a7d0072abbbb942215a75264804214909a19f2693774f010

Generated by **CyberSec Pro** | **cyber-sec-pro.com**

This report is confidential and intended only for authorized recipients.

© 2026 CyberSec Pro. All rights reserved.