

# SARRAL SECURITY

**sarral.io**

## Security Assessment Findings Report

Business Confidential

Date: November 29, 2025  
Project: SAR-061  
Version 1.0

## Confidentiality Statement

This document is the exclusive property of the Client and Sarral Security. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent.

## Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

## Contact Information

| Name        | Title             | Contact Information |
|-------------|-------------------|---------------------|
| Sarral Scan | Automated Scanner | support@sarral.io   |
| Client      | Security Team     | security@sarral.io  |

## Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range used throughout the document.

| Severity      | CVSS V3 Range | Definition  |
|---------------|---------------|---|
| Critical      | 9.0-10.0      | Exploitation is straightforward and usually results in system-level compromise.   |
| High          | 7.0-8.9       | Exploitation is more difficult but could cause elevated privileges and data loss. |
| Moderate      | 4.0-6.9       | Vulnerabilities exist but are not exploitable or require extra steps.             |
| Low           | 0.1-3.9       | Vulnerabilities are non-exploitable but reduce attack surface.                    |
| Informational | N/A           | No vulnerability exists. Additional information provided.                         |

## Executive Summary

Sarral Security evaluated sarral.io's security posture on November 29, 2025. The following sections provide a high-level overview of vulnerabilities discovered.

## Testing Summary

The assessment evaluated the target's external network security posture. The team performed vulnerability scanning and reconnaissance to identify potential risks such as exposed services, misconfigurations, and sensitive information disclosure.

# Vulnerability Summary & Report Card

|          |      |          |     |               |
|----------|------|----------|-----|---------------|
| 0        | 0    | 0        | 0   | 0             |
| Critical | High | Moderate | Low | Informational |

No findings to report.

## Technical Findings