SECURITY ASSESSMENT REPORT

Target: vardhaman.org
Date: November 24, 2025
Scan ID: 22

Prepared by Sarral Scan

1. Executive Summary

Sarral Scan performed a comprehensive security assessment of **vardhaman.org** on 2025-11-24. The objective was to identify potential security vulnerabilities and provide recommendations for remediation.

Findings Summary

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

2. Detailed Findings

1. SSH Connection Refused/Timeout

Severity: MEDIUM **Tool:** Active Recon

Description:

The scan was unable to establish an SSH connection to the target host. This could indicate that the SSH service is not running, is blocked by a firewall, or the host is unreachable. While not a direct vulnerability, it prevents further security assessment of the SSH service and could indicate a misconfiguration or denial-of-service.

Remediation:

1. Verify that the SSH service is running on the target host. 2. Check firewall rules on the target host and any network firewalls to ensure that port 22 (or the configured SSH port) is open. 3. Verify network connectivity between the scanning host and the target host. 4. Investigate potential denial-of-service attacks targeting the SSH service.

---

2. SSH Connection Refused/Timeout

Severity: LOW **Tool:** Passive Recon

Description:

The scan was unable to establish an SSH connection to the target host on port 22. This could be due to the SSH service not running, a firewall blocking the connection, or network connectivity issues.

Remediation:

1. Verify that the SSH service is running on the target host. 2. Check the target host's firewall rules to ensure that inbound connections on port 22 are allowed from the scanning host. 3. Investigate network connectivity between the scanning host and the target host. 4. If SSH is intentionally disabled, document the reason and ensure alternative secure access methods are in place.

---

3. Appendix: Raw Tool Output

The following section contains raw output from the security tools used during the assessment.

Tool: Passive Recon


```
{"error": "SSH Error: [Errno 10060] Connect call failed ('192.168.29.205', 22)"}
```


Tool: Active Recon


```
{"error": "SSH Error: [Errno 10060] Connect call failed ('192.168.29.205', 22)"}
```