Web Security Assessment Report

Executive Summary

Target: https://nonivision.in/
Date: 15 Jan 2026 22:09
Scan Type: Unauthenticated External Assessment
This scan simulates an external attacker without login access.

Overall Risk: LOW
Severity Score: 1.9/10

This report explains security risks in simple language with step-by-step fixes.

Open Ports – Risk Explanation & Fix

Port 80 – HTTP (Risk: Medium)

What is the problem?
HTTP does not encrypt data. Any attacker on the same network can intercept or modify traffic (Man-in-th

How to Secure (Step-by-Step):
Step 1: Install an SSL/TLS certificate (Let's Encrypt recommended).
Step 2: Force HTTPS redirection.

Example (Nginx):
```
server {
    listen 80;
    return 301 https://$host$request_uri;
}
```

Why this works:
All users are automatically redirected to encrypted HTTPS.

How to verify:
Open http://yourdomain.com and confirm it redirects to https://

Related CVEs & CVSS Scores:
CVE-1999-0236 – CVSS: 7.5
CVE-1999-1068 – CVSS: 5.0

Port 443 – HTTPS (Risk: Safe)

What is the problem?
HTTPS encrypts communication between users and the server, protecting credentials and sensitive data

How to Secure (Step-by-Step):
Step 1: Use TLS 1.2 or TLS 1.3 only.
Step 2: Disable SSLv2, SSLv3, TLS 1.0, TLS 1.1.

Why this matters:
Older protocols contain known cryptographic weaknesses.

How to verify:
Use https://www.ssllabs.com/ssltest/

Related CVEs & CVSS Scores:
CVE-1999-1537 – CVSS: 5.0
CVE-2000-0539 – CVSS: 6.4

Security Header Issues

- X-Frame-Options
- X-Content-Type-Options
- Strict-Transport-Security

Server Fingerprint

Server: LiteSpeed
X-Powered-By: PHP/8.2.27

Nmap Scan Result

Nmap scan was not performed because the tool is not installed on the scanning system.

Install command:
sudo apt install nmap

WPScan Result

WPScan was not executed because it is not installed on the system.

Install command:
sudo gem install wpscan

Security Analyst

Ishant Saini

■ Contact Admin on WhatsApp

■ Contact Admin on WhatsApp