VulneraX Scan Report

Target: https://vulnerax.in | Created: 29-08-25 00:17:26 | Completed: 29-08-25 00:22:15 | Grade: E | Download raw JSON

55%

Scanned 151 modules; detected 459 total issues. Top category: Info (247).

Table of Contents

Top Risk Drivers

- **Low** – Admin Panel Discovery Scanner: Potential admin endpoint (×24)
- **Medium** – Debug Console Exposure Scanner: Debug statement: console.log (×7)
- **High** – Security Header Scanner: Security header rollup for https://vulnerax.in (×5)
- **High** – HTTP Verb Tampering Scanner: Verb tampering roll-up for <nil> (×4)
- **High** – x_content_type_options_scan: X-Content-Type-Options roll-up for https://vulnerax.in (×3)

Immediate Actions

- Low – Admin Panel Discovery Scanner: Potential admin endpoint
- Medium – Debug Console Exposure Scanner: Debug statement: console.log
- High – Security Header Scanner: Security header rollup for https://vulnerax.in
- High – HTTP Verb Tampering Scanner: Verb tampering roll-up for <nil>

- High – x_content_type_options_scan: X-Content-Type-Options roll-up for https://vulnerax.in

Severity Overview

Critical	High	Medium	Low	Info
7	57	52	96	247

Priority Findings (Critical • High • Medium)

Critical

Unauthenticated dashboard exposure — Critical

Scanner: **Admin Panel Discovery Scanner**

Count 1

Acceptance of unsigned JWT (alg=none).. — Critical

Scanner: **JWT Alg=None Acceptance Scanner**

Count 1

Server accepted JWT with alg=none — critical vulnerability.. — Critical

Scanner: **JWT Alg=None Acceptance Scanner**

Count 1

JWT key confusion vulnerability detected (accepted forged HS256 token).. — Critical

Scanner: **JWT Key Confusion Scanner**

Count 1

JWT alg=none accepted.. — Critical

Scanner: **JWT None Algorithm Scanner**

Count 1

Server accepted JWT with alg=none — critical vulnerability.. — Critical

Scanner: **JWT None Algorithm Scanner**

Count 1

No Shellshock vulnerability detected — Critical

Scanner: **Shellshock Scanner**

Count 1

High

Security header rollup for https://vulnerax.in — High

Scanner: **Security Header Scanner**

Count 5

Verb tampering roll-up for <nil> — High

Scanner: **HTTP Verb Tampering Scanner**

Count 4

X-Content-Type-Options roll-up for https://vulnerax.in — High

Scanner: **x_content_type_options_scan**

Count 3

X-Frame-Options roll-up for https://vulnerax.in — High

Scanner: **x_frame_options_scan**

Count 3

X-Content-Type-Options header is missing — High

Scanner: **x_content_type_options_scan**

Count 2

X-Frame-Options header is missing — High

Scanner: **x_frame_options_scan**

Count 2

Issue: No CSP reporting directives (`report-uri` or `report-to`) found. — High

Scanner: **CSP Reporting Scanner**

Count 1

CSRF token found: false — High

Scanner: **CSRF Token Scanner**

Count 1

Missing Clear-Site-Data header on logout routes — High

Scanner: **Clear-Site-Data Header Scanner**

Count 1

X-Content-Type-Options header check — High

Scanner: **Content Sniffing Exposure Scanner**

Count 1

CSP header present: false — High

Scanner: **Content-Security-Policy Scanner**

Count 1

Debug statements detected — High

Scanner: **Debug Console Exposure Scanner**

Count 1

DKIM: missing — High

Scanner: **Email Spoofing Protection Scanner**

Count 1

DMARC record is missing — High

Scanner: **Email Spoofing Protection Scanner**

Count 1

DMARC: missing — High

Scanner: **Email Spoofing Protection Scanner**

Count 1

No DKIM selectors found — High

Scanner: **Email Spoofing Protection Scanner**

Count 1

SPF record is missing — High

Scanner: **Email Spoofing Protection Scanner**

Count 1

SPF: missing — High

Scanner: **Email Spoofing Protection Scanner**

Count 1

Missing Permissions-Policy header — **High**

Scanner: **Feature-Policy Misconfiguration Scanner**

Count 1

No Permissions-Policy or Feature-Policy header found — browser features are unrestricted. — **High**

Scanner: **Feature-Policy Misconfiguration Scanner**

Count 1

No suspicious HTML comments detected — **High**

Scanner: **HTML Comment Disclosure Scanner**

Count 1

Uncommon HTTP method allowed: DELETE — **High**

Scanner: **HTTP Verb Tampering Scanner**

Count 1

Uncommon HTTP method allowed: PATCH — **High**

Scanner: **HTTP Verb Tampering Scanner**

Count 1

Uncommon HTTP method allowed: PUT — **High**

Scanner: **HTTP Verb Tampering Scanner**

Count 1

Server accepted JWT signed with 'alg=HS256' using public key as secret.. — High

Scanner: **JWT Key Confusion Scanner**

Count 1

Server accepted 5MB payload without throttling at https://vulnerax.in/ — High

Scanner: **Large Payload Handling Scanner**

Count 1

Missing 7 security headers — High

Scanner: **Missing Security Headers Scanner**

Count 1

Missing header: Content-Security-Policy — High

Scanner: **Missing Security Headers Scanner**

Count 1

No Permissions-Policy or Feature-Policy headers found — High

Scanner: **Permissions-Policy Scanner**

Count 1

Permissions-Policy header check — High

Scanner: **Permissions-Policy Scanner**

Count 1

Permissions-Policy header missing — High

Scanner: **Permissions-Policy Scanner**

Count 1

Referrer-Policy header evaluation — High

Scanner: **Referrer Policy Scanner**

Count 1

Referrer-Policy header is missing — High

Scanner: **Referrer Policy Scanner**

Count 1

Missing header: Content-Security-Policy — High

Scanner: **Security Header Scanner**

Count 1

Missing security headers detected — High

Scanner: **Security Header Scanner**

Count 1

Sensitive server error messages exposed: Internal Server Path — High

Scanner: **Server Error Leak Scanner**

Count 1

Session ID accepted via URL parameter: sessionid=fake123456 — High

Scanner: **Session Fixation Scanner**

Count 1

URL sessionid parameter — High

Scanner: **Session Fixation Scanner**

Count 1

Metadata endpoint SSRF test — High

Scanner: **ssrf_scan**

Count 1

SSRF vulnerability detected against internal metadata endpoint — High

Scanner: **ssrf_scan**

Count 1

Dashboard accessible with status 200 (possible exposure) — High

Scanner: **status_code_mapping**

Count 1

Dashboard status check — High

Scanner: **status_code_mapping**

Count 1

X-Content-Type-Options header details — High

Scanner: **x_content_type_options_scan**

Count 1

X-Frame-Options header details — High

Scanner: **x_frame_options_scan**

Count 1

Medium

Debug statement: console.log — Medium

Scanner: **Debug Console Exposure Scanner**

Count 7

X-DNS-Prefetch-Control roll-up for https://vulnerax.in — Medium

Scanner: **x_dns_prefetch_control_scan**

Count 3

X-Download-Options roll-up for https://vulnerax.in — Medium

Scanner: **x_download_options_scan**

Count 3

HSTS rollup for https://vulnerax.in — Medium

Scanner: **HSTS Scanner**

Count 2

X-DNS-Prefetch-Control header is missing — Medium

Scanner: **x_dns_prefetch_control_scan**

Count 2

X-Download-Options header is missing — Medium

Scanner: **x_download_options_scan**

Count 2

High Entropy String (possible secret) leak detected — Medium

Scanner: **API Key Leak Scanner**

Count 1

No CDN fingerprint headers detected — Medium

Scanner: **CDN Fingerprint & Caching Strategy Scanner**

Count 1

No CDN headers detected — Medium

Scanner: **CDN Misconfiguration Scanner**

Count 1

CMS detection failed — Medium

Scanner: **CMS Fingerprint Scanner**

Count 1

CORP header check — Medium

Scanner: **CORP Header Scanner**

Count 1

Content-Security-Policy header — Medium

Scanner: **CSP Level Validation Scanner**

Count 1

Missing CSP reporting directive — Medium

Scanner: **CSP Reporting Scanner**

Count 1

Debug statement: stack trace — Medium

Scanner: **Debug Console Exposure Scanner**

Count 1

ETag header present on response — Medium

Scanner: **ETag Header Scanner**

Count 1

Favicon is fingerprintable — Medium

Scanner: **Favicon Hash Scanner**

Count 1

favicon.ico present and fingerprintable — Medium

Scanner: **Favicon Hash Scanner**

Count 1

Missing includeSubDomains directive — Medium

Scanner: **HSTS Scanner**

Count 1

Header injected with JNDI payload: Referer — Medium

Scanner: **JNDI Injection Scanner**

Count 1

Header injected with JNDI payload: User-Agent — Medium

Scanner: **JNDI Injection Scanner**

Count 1

Header injected with JNDI payload: X-JNDI-Test — Medium

Scanner: **JNDI Injection Scanner**

Count 1

JNDI payload dispatched **Medium**

Scanner: **JNDI Injection Scanner**

Count 1

Unsigned JWT dispatched.. **Medium**

Scanner: **JWT Alg=None Acceptance Scanner**

Count 1

Forged JWT dispatched (HS256 using public key as secret).. **Medium**

Scanner: **JWT Key Confusion Scanner**

Count 1

Unsigned JWT dispatched.. **Medium**

Scanner: **JWT None Algorithm Scanner**

Count 1

5MB payload accepted **Medium**

Scanner: **Large Payload Handling Scanner**

Count 1

JNDI payload dispatched **Medium**

Scanner: **Log4Shell Scanner**

Count 1

Missing header: Permissions-Policy — Medium

Scanner: **Missing Security Headers Scanner**

Count 1

Missing header: X-Content-Type-Options — Medium

Scanner: **Missing Security Headers Scanner**

Count 1

Missing header: X-Frame-Options — Medium

Scanner: **Missing Security Headers Scanner**

Count 1

Feature-Policy header check — Medium

Scanner: **Permissions-Policy Scanner**

Count 1

Feature-Policy header is missing — Medium

Scanner: **Permissions-Policy Scanner**

Count 1

Permissions-Policy header is missing — Medium

Scanner: **Permissions-Policy Scanner**

Count 1

Missing header: X-Content-Type-Options — Medium

Scanner: **Security Header Scanner**

Count 1

Missing header: X-Frame-Options — Medium

Scanner: **Security Header Scanner**

Count 1

Check /.well-known/security.txt — Medium

Scanner: **Security_txt & Humans_txt Scanner**

Count 1

Error leak test — Medium

Scanner: **Server Error Leak Scanner**

Count 1

X-DNS-Prefetch-Control header details — Medium

Scanner: **x_dns_prefetch_control_scan**

Count 1

X-Download-Options header details — Medium

Scanner: **x_download_options_scan**

Count 1

CVE Findings (Enriched with NVD, EPSS, KEV)

No CVE-mapped findings in this scan.

Modules Scanned

API Authentication Scanner
API Key Leak Scanner
Admin Panel Discovery Scanner
Authorization Bypass via Object ID Scanner
Blind SQL Injection Scanner
Blind XSS Scanner
Boolean-based SQL Injection Scanner
Broken Access Control Scanner
Browser Extension Exposure Scanner
CDN Fingerprint & Caching Strategy Scanner
CDN Misconfiguration Scanner
CMS Fingerprint Scanner
CNAME Inspection Scanner
CORP Header Scanner
CORS Overly Permissive Scanner
CORS Policy Scanner
CRLF Injection Scanner
CSP Bypass Scanner
CSP Level Validation Scanner
CSP Reporting Scanner
CSP Wildcard Scanner
CSRF Token Scanner
Cache Poisoning Scanner
Cache-Control Misconfiguration Scanner
Cache-Control Scanner
Charset Mismatch Scanner
Clear-Site-Data Header Scanner
Clickjacking Protection Scanner
Clickjacking via Nested Frames Scanner
Client-Side Routing Exposure Scanner
Cloud Service Exposure Scanner
Command Injection Scanner
Configuration Leak Scanner
Content Sniffing Exposure Scanner
Content-Disposition Header Scanner
Content-Security-Policy Scanner
Content-Type Mismatch Scanner
Cookie Flags Scanner
DNS Misconfiguration (NXDOMAIN Hijack) Scanner
DNS Zone Transfer Scanner
DOM Clobbering Scanner
DOM-Based Redirect Scanner
DOM-based XSS Scanner
Dead JavaScript Endpoint Scanner
Debug Console Exposure Scanner
Default Credentials Scanner
Directory Listing Scanner
ETag Header Scanner
Email Spoofing Protection Scanner
Environment Variable Exposure Scanner
Error-Based SQL Injection Scanner
Exposed Debug Endpoints Scanner
External Protocol Reference Scanner
Favicon Hash Scanner
Feature-Policy Misconfiguration Scanner
File Upload Exposure Scanner
Form Auto-Complete & PII Leakage Risk Scanner
Framework Exposure Scanner
GraphQL Introspection Scanner
HSTS Scanner
HTML Comment Disclosure Scanner
HTML5 Feature Abuse Scanner
HTTP Methods Scanner
HTTP TRACE Method Scanner

HTTP Verb Tampering Scanner
HTTPS Certificate Pinning Scanner
Heartbleed Scanner
Hidden Parameter Scanner
Improper SameSite _ Cookie Scope Scanner
Insecure Form Action Scanner
Insecure JWT Storage Scanner
JNDI Injection Scanner
JSONP Endpoint Scanner
JWT Alg=None Acceptance Scanner
JWT Exposure in JavaScript Scanner
JWT Key Confusion Scanner
JWT None Algorithm Scanner
JWT Revoked Token Reuse Scanner
JavaScript Source Map Leak Scanner
Large Payload Handling Scanner
Local File Inclusion Scanner
Log4Shell Scanner
Metadata Exposure in Office_PDF Files Scanner
Missing Security Headers Scanner
OAuth Misconfiguration Scanner
OAuth Token Leakage in URL Scanner
Object ID Access Control Scanner
Obsolete JavaScript Library Scanner
Open Redirect Scanner
OpenID Misconfiguration Scanner
Out-of-band SSRF Scanner
Parameter Pollution & Open Redirect Scanner
Password Field Exposure Scanner
Path Traversal Scanner
Permissions-Policy Scanner
Port Probing Scanner
Powered-By & Server Header Scanner
Prototype Pollution Scanner
Public Environment & Debug Info Exposure Scanner
Redirect Chain Scanner
Referer Token Leakage Scanner
Referrer Policy Scanner
Reflected HTML Injection Scanner
Reflected URL Parameter Leak Scanner
Remote File Inclusion Scanner
Response Time Scanner
Robots & Sitemap Scanner
S3 Bucket Exposure Scanner
SQL Injection Scanner
SRI Hash Missing Scanner
Script Source Mapping Leak Scanner
Security Header Scanner
Security_txt & Humans_txt Scanner
Sensitive Form AutoComplete Scanner
Sensitive JavaScript Variable Leak Scanner
Server Error Leak Scanner
Service Worker Scanner
Session Fixation Scanner
Session Replay Detection Scanner
Session Token Lifetime Scanner
Shellshock Scanner
Static Resource Tampering Risk Scanner
postMessage Injection Scanner
ssl_scan
ssrf_scan
ssti_scan
status_code_mapping
subdomain_enumeration

subdomain_takeover_scan swagger_endpoint technology_stack_scan time_based_sql_injection token_in_url_scan trace_method_scan tracking_script_scan unauthenticated_api_scan unsafe_eval_usage_scan url_scheme_hijack_scan version_scan web_storage_leak_scan webdav_scan websocket_hijack websocket_open_endpoint_scan x_content_type_options_scan x_dns_prefetch_control_scan x_download_options_scan x_frame_options_scan x_permitted_cross_domain_policies_scan x_xss_protection_scan xml_external_entity_scan xss_scan

For full module-level evidence and per-finding fields (CVSS/EPSS/KEV/CWE, remediation, references), download the raw JSON export.

Data & Methods

- **Scoring:** Overall security score and grade computed server-side before rendering.
- **CVSS:** CVSS v3.1 base scores computed locally from vectors; vectors sourced from cache (NVD feed) or heuristic fallback.
- **Threat Likelihood:** EPSS and CISA KEV flags applied for CVE-mapped findings.
- **Compliance Tags:** CWE→OWASP Top 10 / PCI DSS / ISO mappings applied when CWE available.
- **Data Export:** The *raw JSON* contains the complete, per-finding schema for programmatic use.

Download raw JSON

About VulneraX (MVP)

Version: v0.9 | **Release:** August 2025 | **Scope:** Automated web vulnerability scanning and reporting.

This report presents a concise view of risk posture. For detailed evidence and reproduction steps, use the raw JSON export.