

Vulnerability Scan Report

Target: http://127.0.0.1:5000/login

Scanned at (UTC): 2026-09-02T09:18:58.538724

Risk Score: 100/100 (Critical Risk)

Severity	Count
Critical	1
High	6
Medium	3
Low	3
Info	1

HTTP Security Headers

[HIGH] Missing Strict-Transport-Security header

HSTS header is missing, so browsers won't be forced to use HTTPS on every visit.

Recommendation: Add 'Strict-Transport-Security: max-age=31536000; includeSubDomains' to enforce HTTPS.

[HIGH] Missing Content-Security-Policy header

No Content-Security-Policy set, increasing exposure to XSS and data-injection attacks.

Recommendation: Define a CSP restricting sources for scripts, styles, images, and frames.

[MEDIUM] Missing X-Frame-Options header

X-Frame-Options is missing, so the page can be embedded in a hidden iframe (clickjacking).

Recommendation: Add 'X-Frame-Options: DENY' or 'SAMEORIGIN', or use CSP 'frame-ancestors'.

[MEDIUM] Missing X-Content-Type-Options header

X-Content-Type-Options is missing, allowing browsers to MIME-sniff responses.

Recommendation: Add 'X-Content-Type-Options: nosniff'.

[LOW] Missing Referrer-Policy header

No Referrer-Policy set; full URLs (possibly containing sensitive data) may leak to third parties.

Recommendation: Add 'Referrer-Policy: strict-origin-when-cross-origin' or stricter.

[LOW] Missing Permissions-Policy header

No Permissions-Policy set; browser features (camera, mic, geolocation) aren't explicitly restricted.

Recommendation: Add a 'Permissions-Policy' header limiting powerful browser APIs to what's needed.

[LOW] Server banner disclosure

Server header reveals: 'Werkzeug/3.1.8 Python/3.10.0', which can help attackers fingerprint software/versions.

Recommendation: Suppress or genericize the Server header at the web server/proxy level.

[CRITICAL] Site served over plain HTTP

The final response was served over HTTP, not HTTPS — all traffic is unencrypted.

Recommendation: Serve the site exclusively over HTTPS and redirect all HTTP traffic to HTTPS.

SSL/TLS Certificate

[MEDIUM] Could not establish SSL connection

[WinError 10061] No connection could be made because the target machine actively refused it

Recommendation: Confirm the target serves HTTPS on this port (443 by default).

Security Misconfigurations

[INFO] No common misconfigurations detected

The checks performed did not surface obvious misconfigurations.

Recommendation: Continue periodic reviews — this is not an exhaustive audit.

Open Ports

[HIGH] Sensitive port 445 (SMB) is open

Port 445 (SMB) responded as open, which is risky if exposed publicly.

Recommendation: Restrict access to SMB via firewall/VPN, or disable it if not required.

[HIGH] Sensitive port 3306 (MySQL) is open

Port 3306 (MySQL) responded as open, which is risky if exposed publicly.

Recommendation: Restrict access to MySQL via firewall/VPN, or disable it if not required.

[HIGH] Sensitive port 5432 (PostgreSQL) is open

Port 5432 (PostgreSQL) responded as open, which is risky if exposed publicly.

Recommendation: Restrict access to PostgreSQL via firewall/VPN, or disable it if not required.

[HIGH] Sensitive port 27017 (MongoDB) is open

Port 27017 (MongoDB) responded as open, which is risky if exposed publicly.

Recommendation: Restrict access to MongoDB via firewall/VPN, or disable it if not required.