Vulnerability Assessment Report

Generated on: 2025-10-25 21:00:54

Total Findings: 15

Name: Cross-Site Scripting (XSS)

Severity: Medium
Date: 2025-10-14 13:55:31

Reflected XSS detected in user comments.

Mitigation:
Escape user output in HTML/JS contexts and implement Content Security Policy (CSP).

Name: Open Port 22 (SSH)

Severity: Low
Date: 2025-10-20 16:59:54

SSH service exposed on public IP.

Mitigation:
Restrict SSH access to trusted IPs and use key-based authentication.

Name: Cross-Site Scripting (XSS)

Severity: Medium
Date: 2025-10-20 17:00:31

Reflected XSS detected in user comments.

Mitigation:
Escape user output in HTML/JS contexts and implement Content Security Policy (CSP).

Name: Server Misconfiguration

Severity: Medium
Date: 2025-10-20 17:00:32

Directory listing is enabled.

Mitigation:
Disable directory listing, remove default server pages, and restrict access to sensitive files.

Name: SQL Injection

Severity: High
Date: 2025-10-20 17:00:34

Unsanitized input in login form.

Mitigation:
Use parameterized queries or ORM to avoid string concatenation. Validate user inputs.

Name: SQL Injection

Severity: High
Date: 2025-10-20 17:00:35

Unsanitized input in login form.

Mitigation:
Use parameterized queries or ORM to avoid string concatenation. Validate user inputs.

Name: Insecure HTTP Headers

Severity: Low
Date: 2025-10-20 17:00:36

Missing Content-Security-Policy header.

Mitigation:
Implement headers such as X-Frame-Options, X-Content-Type-Options, and CSP.

Name: Insecure HTTP Headers

Severity: Low
Date: 2025-10-20 17:00:37

Missing Content-Security-Policy header.

Mitigation:
Implement headers such as X-Frame-Options, X-Content-Type-Options, and CSP.

Name: Cross-Site Scripting (XSS)

Severity: Medium
Date: 2025-10-20 17:00:39

Reflected XSS detected in user comments.

Mitigation:
Escape user output in HTML/JS contexts and implement Content Security Policy (CSP).

Name: Open Port 22 (SSH)

Severity: Low
Date: 2025-10-20 17:00:40

SSH service exposed on public IP.

Mitigation:
Restrict SSH access to trusted IPs and use key-based authentication.

Name: Open Port 22 (SSH)

Severity: Low
Date: 2025-10-20 17:29:24

SSH service exposed on public IP.

Mitigation:
Restrict SSH access to trusted IPs and use key-based authentication.

Name: Server Misconfiguration

Severity: Medium
Date: 2025-10-24 01:29:28

Directory listing is enabled.

Mitigation:
Disable directory listing, remove default server pages, and restrict access to sensitive files.

Name: Server Misconfiguration

Severity: Medium
Date: 2025-10-25 19:31:08

Directory listing is enabled.

Mitigation:
Disable directory listing, remove default server pages, and restrict access to sensitive files.

Name: Advanced Scan for www.google.com

Severity: Info
Date: 2025-10-25 19:47:52

Nmap and OWASP ZAP scan executed for www.google.com.

--- Nmap ---
Nmap Error: [WinError 2] The system cannot find the file specified

--- ZAP ---
ZAP Error: [WinError 2] The system cannot find the file specified

Mitigation:
Apply general secure coding practices.

Name: Open Port 22 (SSH)

Severity: Low
Date: 2025-10-25 20:00:52

SSH service exposed on public IP.

Mitigation:
Restrict SSH access to trusted IPs and use key-based authentication.