Web Application Vulnerability Report

Scan Date: 2025-08-20 00:45:45 UTC

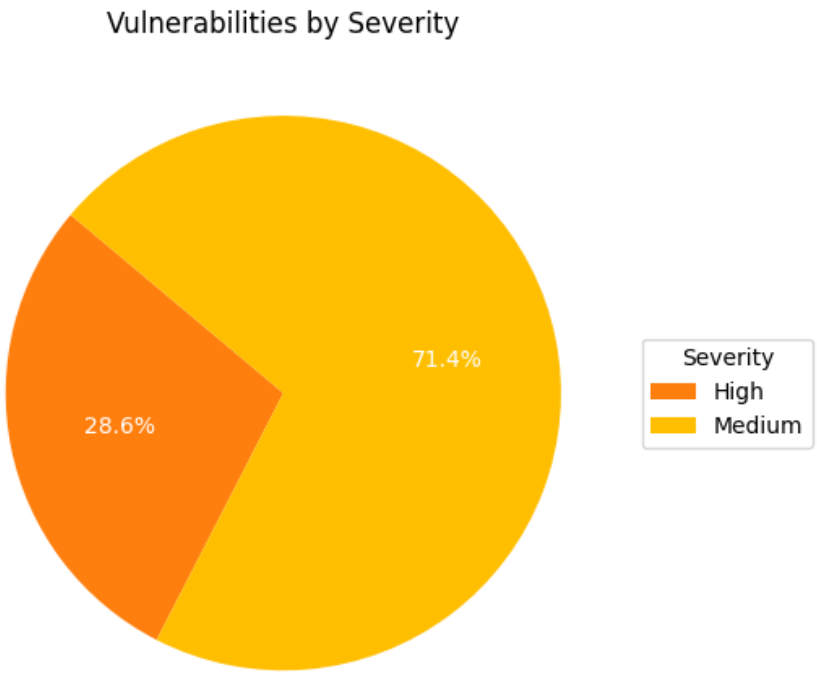
Target URL: https://kb.builtwith.com/general-questions/expired-technology-website/

Executive Summary

Scan Results Summary:

- High: 2

- Medium: 5



Detailed Findings

1. Reflected XSS Vulnerability #1

Severity: High

CVSS Score: CVSS: N/A

Description:

Reflected XSS vulnerability confirmed with payload: ';a=prompt,a()//

Proof of Concept:

Submit to //builtwith.com/ with payload in any text field

Remediation Steps:

- Implement proper input validation
- Use output encoding when displaying user input
- Implement Content Security Policy (CSP)

Business Impact:

N/A

SLA: Fix within 7 days

2. Exposed Sensitive Paths

Severity: High

CVSS Score: CVSS: N/A

Description:

Exposed paths can leak configuration files or admin panels.

Proof of Concept:

https://kb.builtwith.com/general-questions/expired-technology-website/.env

https://kb.builtwith.com/general-questions/expired-technology-website/.env.backup

https://kb.builtwith.com/general-questions/expired-technology-website/.env.bak

https://kb.builtwith.com/general-questions/expired-technology-website/.env.dev

https://kb.builtwith.com/general-questions/expired-technology-website/.env.development.local

https://kb.builtwith.com/general-questions/expired-technology-website/.env.dev.local

https://kb.builtwith.com/general-questions/expired-technology-website/.env.example

https://kb.builtwith.com/general-questions/expired-technology-website/.env.live

https://kb.builtwith.com/general-questions/expired-technology-website/.env.local

https://kb.builtwith.com/general-questions/expired-technology-website/.env.prod.local

https://kb.builtwith.com/general-questions/expired-technology-website/.env.prod

https://kb.builtwith.com/general-questions/expired-technology-website/.env.old

https://kb.builtwith.com/general-questions/expired-technology-website/.env.production

https://kb.builtwith.com/general-questions/expired-technology-website/.env.production.local

https://kb.builtwith.com/general-questions/expired-technology-website/.env.stage

https://kb.builtwith.com/general-questions/expired-technology-website/.env.save

https://kb.builtwith.com/general-questions/expired-technology-website/.env.staging

https://kb.builtwith.com/general-questions/expired-technology-website/.env.www

https://kb.builtwith.com/general-questions/expired-technology-website/.env.testing

https://kb.builtwith.com/general-questions/expired-technology-website/.envrc

https://kb.builtwith.com/general-questions/expired-technology-website/.env_sample

https://kb.builtwith.com/general-questions/expired-technology-website/.git/config

https://kb.builtwith.com/general-questions/expired-technology-website/.env_1

https://kb.builtwith.com/general-questions/expired-technology-website/.htaccess

https://kb.builtwith.com/general-questions/expired-technology-website/.htpasswd

https://kb.builtwith.com/general-questions/expired-technology-website/robots.txt

https://kb.builtwith.com/general-questions/expired-technology-website/robots.txt/../admin/

Remediation Steps:

- Restrict public access to sensitive directories.
- Use proper web server configuration and access controls.

Business Impact:

N/A

SLA: Fix within 7 days

3. Outdated jQuery

Severity: Medium

CVSS Score: CVSS: N/A

Description:

jQuery 3.5.1 is outdated. Latest is 3.7.1.

Proof of Concept:

Version 3.5.1 in use.

Remediation Steps:

- Upgrade to 3.7.1.

Business Impact:

N/A

SLA: Fix within 30 days

4. Outdated Bootstrap

Severity: Medium

CVSS Score: CVSS: N/A

Description:

Bootstrap 4.3.1 is outdated. Latest is 5.3.3.

Proof of Concept:

Version 4.3.1 in use.

Remediation Steps:

- Upgrade to 5.3.3.

Business Impact:

N/A

SLA: Fix within 30 days

5. Outdated Microsoft ASP.NET

Severity: Medium

CVSS Score: CVSS: N/A

Description:

Microsoft ASP.NET 4.0 is outdated. Latest is 4.8.

Proof of Concept:

Version 4.0 in use.

Remediation Steps:

- Upgrade to 4.8.

Business Impact:

N/A

SLA: Fix within 30 days

6. CVE-2019-8331 - Bootstrap -

Severity: Medium

CVSS Score: CVSS: N/A

Description:

In Bootstrap before 3.4.1 and 4.3.x before 4.3.1, XSS is possible in the tooltip or popover data-template attribute.

Proof of Concept:

Version: 4.3.1 is affected by CVE-2019-8331

Remediation Steps:

- Upgrade to the latest patched version.

Business Impact:

N/A

SLA: Fix within 30 days

7. Missing Security Headers

Severity: Medium

CVSS Score: CVSS: N/A

Description:

The following important security headers are missing.

Proof of Concept:

https://kb.builtwith.com/general-questions/expired-technology-website/

Remediation Steps:

- Add the `Strict-Transport-Security` header.
- Add the `Content-Security-Policy` header.
- Add the `X-Frame-Options` header.
- Add the `Referrer-Policy` header.
- Add the `Permissions-Policy` header.

Business Impact:

N/A

SLA: Fix within 30 days