Web Application Vulnerability Report

Scan Date: 2025-08-17 14:25:07 UTC

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

Executive Summary

Scan Results Summary:

- High: 1

- Medium: 5

Detailed Findings

1. Exposed Sensitive Paths

Severity:	High
CVSS Score:	CVSS: 7.5 (High)

Description:

Sensitive paths (e.g., /admin, /config, /backup) are exposed, risking unauthorized access to configuration files, administrative interfaces, or other critical resources.

Proof of Concept:

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

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.dev.local

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.local

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

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.live

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

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

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

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.staging

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

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

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/.htpasswd

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

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:

- Remove or rename exposed sensitive files and paths.
- Implement strict access controls and restrict directory listing.
- Use security scanners to identify and secure additional hidden paths (e.g., .git, .env).

Business Impact:

Exposed paths can lead to configuration leaks, system takeover, or data breaches. This poses a high risk to operational continuity and regulatory compliance.

2. Outdated jQuery

Severity:	Medium
CVSS Score:	CVSS: 5.0 (Medium)

Description:

The application is using jQuery version 3.5.1, which is outdated. The latest version is 3.7.1, and this leaves the system vulnerable to potential XSS and other security flaws fixed in newer releases.

Proof of Concept:

Version 3.5.1 in use.

Remediation Steps:

- Upgrade jQuery to version 3.7.1 or later.

- Review all dependencies and ensure compatibility with the updated version.
- Test the application post-upgrade to confirm functionality remains intact.

Business Impact:

Using an outdated library increases the risk of exploitation through known vulnerabilities, potentially leading to data breaches or client-side attacks. Maintaining up-to-date dependencies is critical for protecting user data and preserving trust.

3. Outdated Bootstrap

Severity: Medium

CVSS Score: CVSS: 5.0 (Medium)

Description:

Bootstrap 4.3.1 is outdated, with the latest version being 5.3.3. This exposes the application to security issues resolved in newer versions, such as XSS vulnerabilities in components like tooltip and popover.

Proof of Concept:

Version 4.3.1 in use.

Remediation Steps:

- Upgrade Bootstrap to version 5.3.3 or later.
- Migrate code to align with the updated framework's syntax and features.
- Validate all user inputs and sanitize templates to mitigate XSS risks.

Business Impact:

Unpatched Bootstrap versions could allow attackers to inject malicious scripts, compromising user sessions or sensitive data. This risks brand reputation and may lead to compliance violations.

4. Outdated Microsoft ASP.NET

Severity: Medium

CVSS Score: CVSS: 5.0 (Medium)

Description:

Microsoft ASP.NET 4.0 is outdated compared to the latest version, 4.8. Older versions may lack critical security patches, exposing the application to known exploits.

Proof of Concept:

Version 4.0 in use.

Remediation Steps:

- Upgrade ASP.NET to version 4.8 or later.
- Apply all available security patches for the existing version if immediate upgrade is not feasible.
- Verify application compatibility with the updated framework.

Business Impact:

Outdated server frameworks increase the risk of system compromise, data leaks, and potential downtime. Non-compliance with modern standards may also result in legal or financial penalties.

5. CVE-2019-8331 - Bootstrap -

Severity:	Medium
CVSS Score:	CVSS: 5.0 (Medium)

Description:

CVE-2019-8331 affects Bootstrap versions prior to 3.4.1 and 4.3.1, enabling XSS via the tooltip or popover data-template attribute. Malicious payloads could be executed in user sessions.

Proof of Concept:

Version: 4.3.1 is affected by CVE-2019-8331

Remediation Steps:

- Update Bootstrap to version 3.4.1 or 4.3.1 and above.
- Sanitize and validate all user-supplied content used in tooltip/popover templates.
- Implement Content Security Policy (CSP) headers to restrict script execution.

Business Impact:

XSS vulnerabilities can lead to data theft, session hijacking, or malware distribution. This undermines user confidence and exposes the organization to financial and reputational harm.

6. Missing Security Headers

Severity: Medium

CVSS Score: CVSS: 5.0 (Medium)

Description:

Missing essential HTTP security headers (e.g., HSTS, Content-Security-Policy, X-Content-Type-Options) weakens the browser's defense mechanisms against common attacks.

Proof of Concept:

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

Remediation Steps:

- Add missing headers via server configuration (e.g., IIS, Apache, Nginx).
- Use strict CSP rules to control resource loading and script execution.
- Regularly audit headers using tools like SSL Labs or Burp Suite.

Business Impact:

Lack of security headers increases susceptibility to clickjacking, MIME-type sniffing, and XSS attacks. This could result in unauthorized access or compromise of user data.