

VULNERABILITY ASSESSMENT REPORT

The Clean Divorce
Toronto, ON

<https://www.thecleandivorce.com/>



Executive Summary

12/07/2024

v. 1.1.0

PREPARED BY	Felipe Rincon	DATE	15/07/2024
Team Members	Carmen Kwan, Jessica Beirne and Shuyuan Wang	DATE	

CONTENTS

TABLE OF CONTENTS.....2

Executive Summary.....3

Scan Results.....3

Findings.....4

Risk Assessment..... 10

TCD Risk tolerance 10

Recommendations 11

Conclusion..... 12

References..... 12

1. Executive Summary

The purpose of this report is to identify and prioritize potential vulnerabilities within The Clean Divorce Network infrastructure. Recommendations are provided to mitigate these vulnerabilities and improve overall security posture.

2. Scan results

Scope:

Testing period: July 6-11, 2024.

URL domain: <https://www.thecleandivorce.com/>

Permanent open ports: 80 / 443

IP address: 199.15.163.128

Hostname: unallocated.163.wixsite.com

Web sites included: <https://frog.wix.com>, <https://update.googleapis.com>,
<https://www.thecleandivorce.com>, <https://static.parastorage.com>

I ran the vulnerability assessment scan over the main Web page of the organization, with the domain <https://www.thecleandivorce.com/> powered by WIX, with a scope across the whole site, in a timeframe of 2 hour during the morning and 2 hours during the afternoon, these were includes the following location of the domain, as follow:

Name	Domain
Clean divorce main page	https://www.thecleandivorce.com/
Blog Post	https://www.thecleandivorce.com/blog
Get in touch – form-	https://www.thecleandivorce.com/getintouch
Log In	https://www.thecleandivorce.com/
Journey to Freedom	https://www.thecleandivorce.com/journeytofreedomearlysignup
Services	https://www.thecleandivorce.com/book-online
Resources -forms-	https://www.thecleandivorce.com/partnership-site
About	https://www.thecleandivorce.com/about-1-2

The vulnerability assessment conducted over the Clean Divorce Network, revealed some vulnerabilities across the domain. Based on the preliminary evaluation of the results, the following test have been conducted based on four different tools, and some results have pop ups:

- Scanning test using Zenmap
- Vulnerability analysis using Wireshark
- Vulnerability scan using Shodan and checking the source code
- Penetration Testing using OWASP ZAP

Each vulnerability is scaled depending on the data under risk, the weight of vulnerability, and damage that might arise from the affected system breach. This step's main idea is to measure the threat and

clearly identify the urgency behind each vulnerability or the risk level and potential effect. 1. “Five Steps of a Good Vulnerability Assessment and How to Write Report <https://securityforeveryone.com/blog/a-good-vulnerability-assessment-and-how-to-write-report>”

3. Findings

- a) **Scanning the Network using Zenmap** – Help us to recognize vulnerabilities of a URL web page or and IP address. Both performance over the clean divorce domain. Checked for vulnerabilities in the web, testing for Heartbleed in SSL/TLS ports, having the following findings:

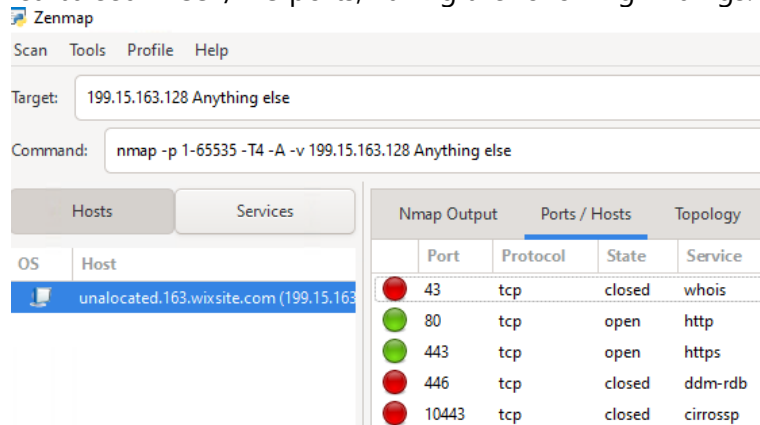


Image 1

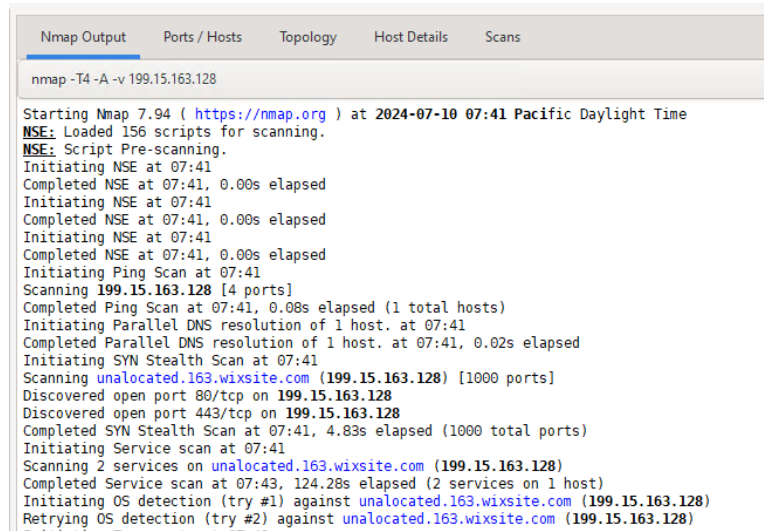


Image 2

Some vulnerabilities were identified across the IP, through the ports:

Port 80 (HTTP): This service is open and should be checked, to ensure sensitive data is not transmitted over HTTP. Check for outdated web server software.

Port 443 (HTTPS): This service is also open and requires inspection for SSL/TLS-related vulnerabilities, Verify strong encryption protocols, valid SSL certificates.

OS and Device type – Low load balancer firewall, and apply any necessary patches.

- b) **Packets analysis using Wireshark** - Detecting vulnerabilities involves analyzing network traffic for signs of suspicious or malicious activity. From this packet capture, we can see two apparently risks, that are:

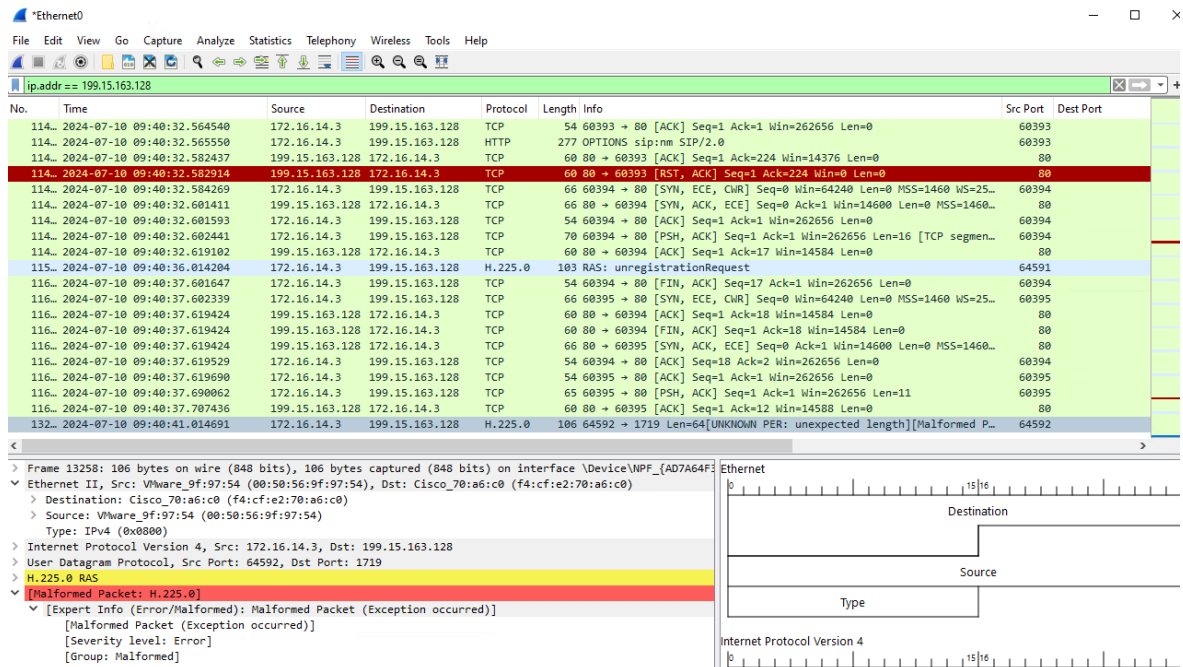


Image 3

- A malformed H.225.0 packet indicates that there is an anomaly or inconsistency in the packet that prevents proper decoding. If the problem persists, further analysis with a focus on the specific anomalies detected may be necessary.

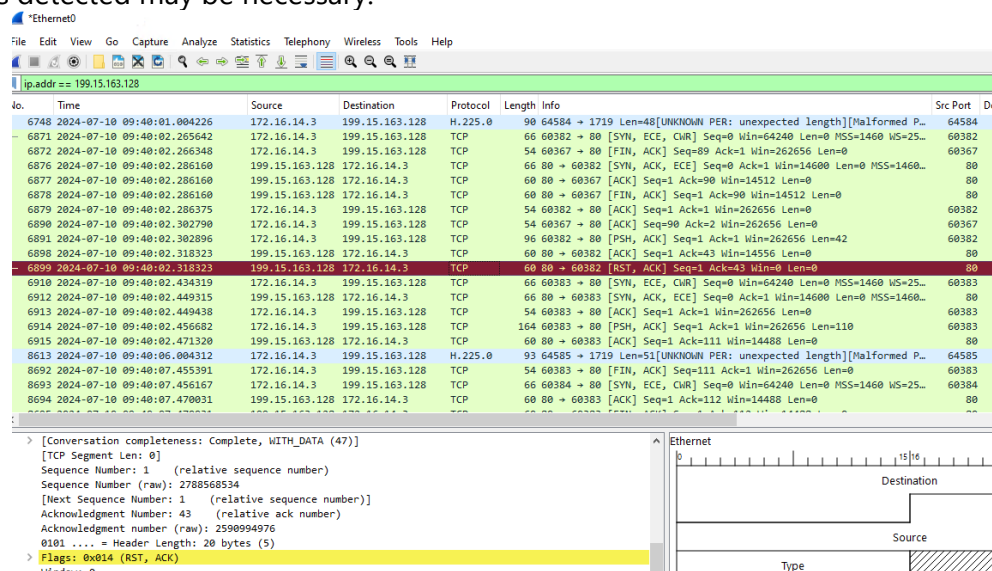


Image 4

- TCP flags** - A packet with flags (RST, ACK), should indicate that the sender is forcefully terminating the TCP connection and acknowledging the receipt of any data up to that point. Analyzing these packets helps in understanding network issues.

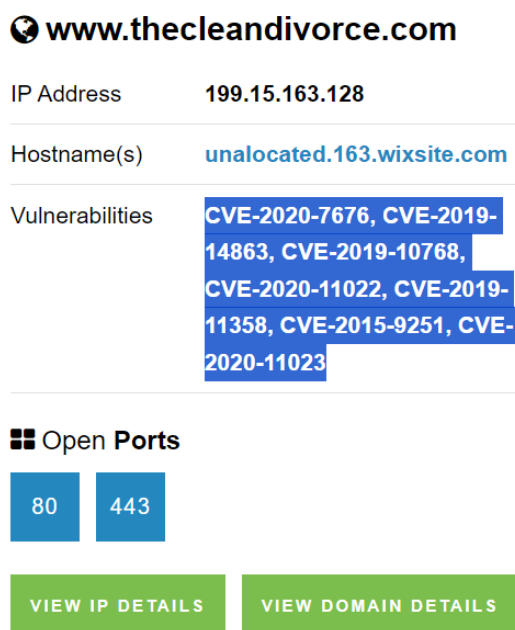
- c) **The Shodan application** is a powerful tool that allow us to access to a vast database of internet-connected devices directly from their browser, that enable to View Devices Details, and detect potential vulnerabilities, and help us to have real-Time Alerts about changes in the status or security of monitored devices, obtained the following results for the clean divorce web page:

Port 80 (HTTP) open.

- Severity: Medium
- Description: Unencrypted HTTP traffic exposes the server to attacks.
- Affected Systems: Any web server on port 80.

Port 443 (HTTPS) open.

- Severity: Medium
- Description: HTTPS traffic encrypted but vulnerable if misconfigured.
- Affected Systems: Web servers with SSL/TLS on port 443.



The screenshot displays the Shodan search results for the domain **www.thecleandivorce.com**. It shows the IP address **199.15.163.128** and the hostname **unallocated.163.wixsite.com**. A list of vulnerabilities is provided, including CVE-2020-7676, CVE-2019-14863, CVE-2019-10768, CVE-2020-11022, CVE-2019-11358, CVE-2015-9251, and CVE-2020-11023. Below the vulnerabilities, there is a section for **Open Ports** showing ports **80** and **443**. At the bottom, there are two green buttons: **VIEW IP DETAILS** and **VIEW DOMAIN DETAILS**.

Image 5

CVE-2020-7676

- Severity: High
- Affected Systems: thst using the merge npm package versions prior to 1.2.1.
- Description: Prototype pollution vulnerability in the merge npm package.

CVE-2019-14863

- Severity: Medium
- Affected Systems: That using Ansible Engine prior to version 2.8.5.
- Description: Improper handling of host_key_checking in Ansible Engine.

CVE-2019-10768

- Severity: Medium

- Affected Systems: the event-stream npm package versions prior to 4.0.1.
- Description: Arbitrary code execution in event-stream npm package.

CVE-2020-11022

- Severity: Medium
- Affected Systems: Using jQuery versions 1.2 and 3.4.0 through 3.5.0.
- Description: Prototype pollution vulnerability in jQuery.

CVE-2019-11358

- Severity: Medium
- Affected Systems: Using jQuery versions prior to 3.4.0.
- Description: Prototype pollution in jQuery.

CVE-2015-9251

- Severity: Medium
- Affected Systems: Systems using jQuery version 1.12.4 or earlier.
- Description: Cross-site scripting (XSS) vulnerability in jQuery.

CVE-2020-11023

- Severity: Medium
- Affected Systems: Systems using jQuery 3.5.0.
- Description: XSS in jQuery 3.5.0.

- d) **Penetration Testing Report** – Using Zap for the domain The Clean Divorce, that scans include related sites like static.parastorage.com and browser.sentry-cdn.com.

We identified a total of 14 alerts, categorized by risk at three levels.

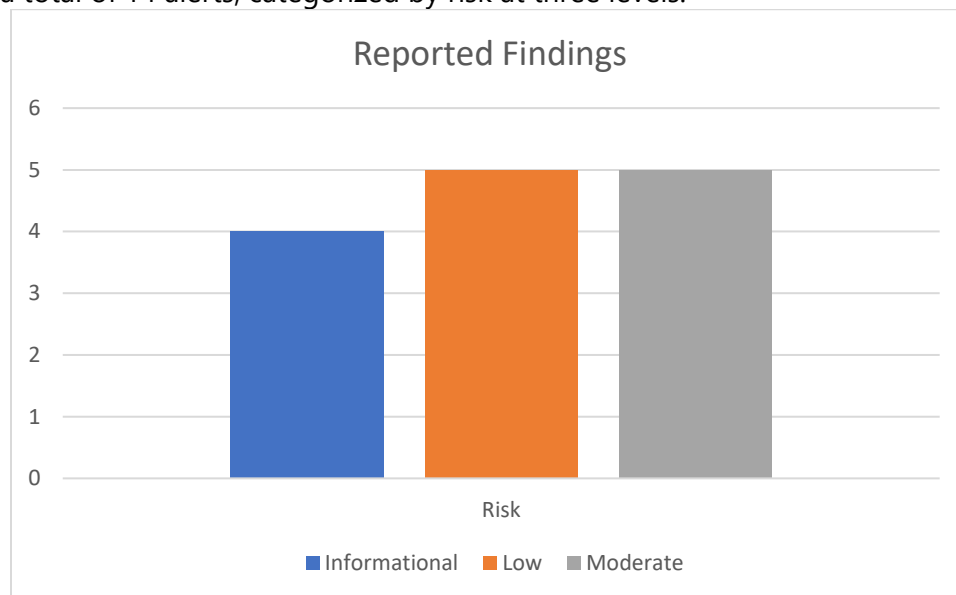


Image 6

- **Moderate Risk Alerts**

- Absence of Anti-CSRF Tokens

Risk: Medium

Confidence: Medium

Description: Missing Anti-CSRF tokens can allow attackers to perform actions on behalf of authenticated users without their consent.

Recommendation: Implement CSRF tokens in forms and state-changing requests to prevent cross-site request forgery attacks.

- Content Security Policy (CSP) Header Not Set

Risk: Medium

Confidence: Medium

Description: Lack of CSP header makes the site vulnerable to a range of attacks, including cross-site scripting (XSS).

Recommendation: Implement a robust Content Security Policy to mitigate XSS and data injection attacks.

- Cross-Domain Misconfiguration

Risk: Medium

Confidence: Medium

Description: Misconfigured cross-domain policies can allow unauthorized access to resources.

Recommendation: Review and properly configure cross-domain policies to restrict unauthorized resource sharing.

- Missing Anti-clickjacking Header

Risk: Medium

Confidence: High

Description: Absence of headers like X-Frame-Options or Content-Security-Policy can expose the site to clickjacking attacks.

Recommendation: Add anti-clickjacking headers to prevent framing by malicious websites.

- Vulnerable JS Library

Risk: Medium

Confidence: Low

Description: Using outdated JavaScript libraries with known vulnerabilities can be exploited by attackers.

Recommendation: Update all JavaScript libraries to the latest versions to mitigate security risks.

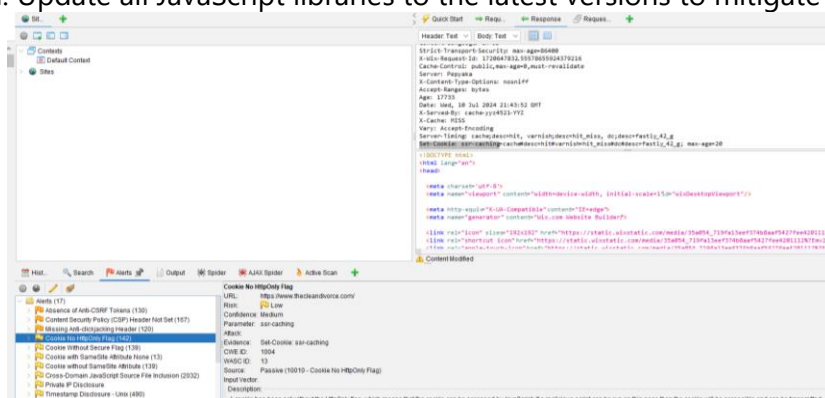


Image 7

Low Risk Alerts

- Cookie No HttpOnly Flag

Risk: Low

Confidence: High

Description: Cookies without HttpOnly flag can be accessed via JavaScript, potentially exposing sensitive information.

Recommendation: Set the HttpOnly flag on cookies to prevent client-side scripts from accessing them.

- Cookie Without Secure Flag

Risk: Low

Confidence: High

Description: Cookies without Secure flag can be transmitted over unencrypted connections, exposing them to interception.

Recommendation: Set the Secure flag on cookies to ensure they are only sent over HTTPS.

- Strict-Transport-Security Header Not Set

Risk: Low

Confidence: Medium

Description: Missing HSTS header can allow attackers to intercept communications over unencrypted channels.

Recommendation: Implement the Strict-Transport-Security header to enforce secure connections.

- X-Content-Type-Options Header Missing

Risk: Low

Confidence: Medium

Description: Absence of this header can lead to MIME type sniffing vulnerabilities.

Recommendation: Set the X-Content-Type-Options header to 'nosniff' to prevent MIME type sniffing.

- Private IP Disclosure

Risk: Low

Confidence: Low

Description: Disclosure of internal IP addresses can provide attackers with additional information about the internal network.

Recommendation: Remove or obfuscate private IP addresses from publicly accessible responses.

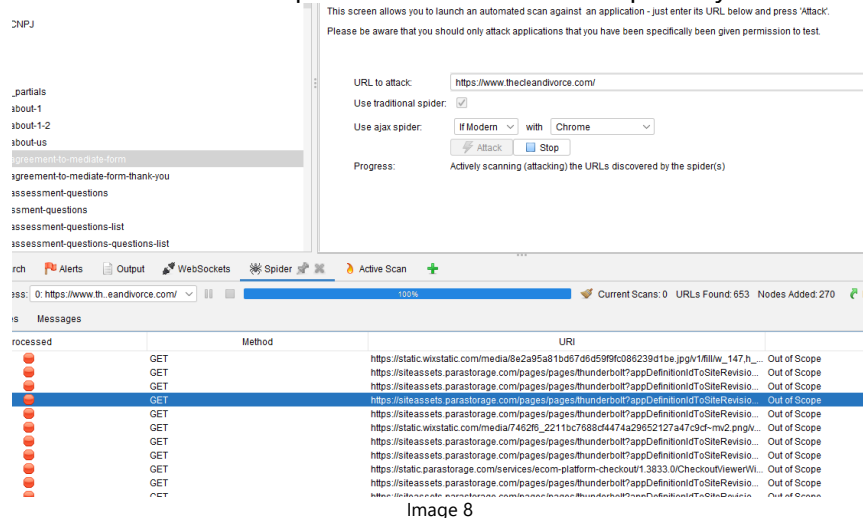


Image 8

Informational Alerts

- Information Disclosure - Suspicious Comments

Risk: Informational

Confidence: High

Description: Comments in the source code may disclose sensitive information or implementation details.

Recommendation: Review and remove any sensitive information from comments in the code.

- Loosely Scoped Cookie

Risk: Informational

Confidence: Medium

Description: Cookies that are scoped too broadly can be accessed by subdomains or other parts of the site unnecessarily.

Recommendation: Scope cookies as narrowly as possible to limit their accessibility.

- Re-examine Cache-control Directives

Risk: Informational

Confidence: Medium

Description: Inadequate cache-control directives can lead to sensitive information being stored in caches.

Recommendation: Implement appropriate cache-control directives to prevent sensitive data from being cached.

- Session Management Response Identified

Risk: Informational

Confidence: Low

Description: Session management mechanisms identified in responses may provide insights into session handling.

Recommendation: Ensure session management is secure and review session handling practices.

4. Risk Assessment

The vulnerabilities to analyze, were categorized into medium, low and informational levels, without present of any critical score, who pose the highest risk to the organization and require immediate attention. Medium vulnerabilities also need to be addressed in the mid-term to reduce the risk of exploitation.

5. Clean Divorce Risk Tolerance

The overall risk posture of the domain should be significantly compromised due to the identified vulnerabilities. The presence of outdated scan engines, unprotected services, and insecure SSL/TLS configurations on critical systems poses a high risk of exploitation and potential compromise of sensitive data.

In that order, these risks do not Align with The Clean Divorce Tolerance, as they expose critical systems to a high likelihood of exploitation. That likely dictates a need for addresses to the Host site (WIX), to mitigate these vulnerabilities and reduce the risk to an acceptable level.

6. Recommendations to Mitigate

As not every vulnerability can be remediated, which is where mitigation comes in. Based on the severity and potential impact of the vulnerabilities, Clearly the WIX IT Response team should be aware of the potential impact of these vulnerabilities on The Clean Divorce domain operations, and the importance of implementing the following recommendations provided:

Mitigation strategies to have in mind not only for escalation to the WIX team but also in the event of a potential migration to another platform. It is important to have these strategies in mind and report them as a first step.

Strengthening Security Measures:

- Implement multi-factor authentication across all systems.
- Regularly update and patch all software and hardware components.

Enhancing Monitoring and Response:

- Establish a continuous monitoring system to detect and respond to threats in real-time.
- Conduct regular security audits and vulnerability assessments.
- Regularly monitor server logs for unusual or suspicious User Agent strings.
- **Monitor and Remove Sensitive Comments:** Periodically audit code for comments that may disclose sensitive information and remove them.

User Training and Awareness:

- Conduct periodic training sessions to educate users about common security threats and best practices.
- Develop and distribute security awareness materials to keep security top-of-mind.

Data Protection and Backup:

- Ensure regular backups of all critical data and systems.
- Implement strong encryption protocols for data at rest and in transit.

Secondary measures to have in mind.

Implement Security Headers: Add necessary security headers like CSP, X-Frame-Options, and HSTS to improve overall security.

Use Secure Cookies: Ensure all cookies use the Secure and HttpOnly flags to protect them during transmission and from client-side access.

Regular Updates: Keep all software, libraries, and dependencies updated to the latest versions to mitigate known vulnerabilities.

Review and Harden Configurations: Regularly review and tighten security configurations, including cross-domain policies and cookie scopes.

Review User Agent Handling: Ensure that the application does not expose sensitive information or functionality based on different User Agents.

Update Security Policies and Conduct Manual Reviews.

By addressing these vulnerabilities and following the recommendations, you can enhance the security posture of The Clean Divorce website, and protect it from potential cyber threats.

7. Conclusion

Implementing to mid-term specially, the recommended security measures for protecting The Clean Divorce's web page, can help to enhance its security posture and safeguard its operations against potential threats, supporting future growth as well.

8. References

Article Name	URL
Creating a Culture of Security	https://www.nist.gov/blogs/manufacturing-innovation-blog/creating-culture-security
11 Identity & Access Management (IAM) Best Practices in 2024	https://www.strongdm.com/blog/iam-best-practices#:~:text=One%20of%20the%20most%20common,interfering%20with%20users%27%20daily%20workflows
What Are Network Security Basics?	https://www.trendmicro.com/en_us/what-is/network-security/network-security-basics.html
Fundamentals of Cyber Security for Canada's CI Community	https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/index-en.aspx
Cybersecurity Framework 1.1 Components	https://www.nist.gov/cyberframework/cybersecurity-framework-components

Appendix

- Zap reports
- Shodan Report
- TCD Cybersecurity Infographic
- Read me file