WebAssure Scanner Report

Scan Information

Target URL: https://demo.owasp-juice.shop/

Scan Date: 2025-04-30 10:55:46

Executive Summary

OWASP ZAP Findings:

High Risk Issues: 0

Medium Risk Issues: 126

Low Risk Issues: 396

Informational Issues: 70

Nikto Findings:

High Risk Issues: 0

Medium Risk Issues: 1

Low Risk Issues: 5

Total Vulnerabilities: 7

WebAssure Scanner Report

OWASP ZAP Findings

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/assets/public/favicon_js.ico
Evidence: Access-Control-Allow-Origin: *

CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/runtime.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/robots.txt
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/sitemap.xml
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/

https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/sitemap.xml
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/polyfills.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/vendor.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/main.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/ftp/incident-support.kdbx
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/ftp/coupons_2013.md.bak
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

WebAssure Scanner Report

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/ftp/package.json.bak
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/ftp/eastere.gg
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for

instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/ftp/order_5267-e790c915f10a4e0b.pdf
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/ftp/suspicious_errors.yml
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/ftp/legal.md
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/ftp/eastere.gg
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/ftp/acquisitions.md
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/ftp/suspicious_errors.yml
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

URL: https://demo.owasp-juice.shop/ftp
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/ftp
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/build/routes/vendor.js
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/styles.css
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/favicon_js.ico
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the

Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/favicon_js.ico
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/build/routes/vendor.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/styles.css
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/layer.js:95:5
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/build/routes/fileServer.js:43:13
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:286:9
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/

https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:421:3
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/build/routes/styles.css
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:328:13
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/build/routes/fileServer.js:59:18
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS

headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/favicon_js.ico
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/index.js:145:39
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:280:10
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/favicon_js.ico
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/layer.js:95:5
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:286:9
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/build/routes/fileServer.js:43:13
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:421:3
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/build/routes/styles.css
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:328:13
Evidence: Access-Control-Allow-Origin: *

CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/build/routes/fileServer.js:59:18
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/build/routes/runtime.js
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/index.js:145:39

Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:280:10
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/ftp/announcement_encrypted.md
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/build/routes/runtime.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/styles.css
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/runtime.js
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS

headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/styles.css
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/runtime.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/styles.css
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types

are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/favicon_js.ico
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/assets/public/favicon_js.ico
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/styles.css
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/polyfills.js
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/vendor.js
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website

owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/runtime.js
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/polyfills.js
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/assets/public/favicon_js.ico
CWE ID: 693

Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/favicon_js.ico
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/assets/public/favicon_js.ico
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/vendor.js

CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/styles.css
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/runtime.js
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy

https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/polyfills.js
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/polyfills.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/assets/public/favicon_js.ico
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/vendor.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/runtime.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/polyfills.js

Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/assets/public/favicon_js.ico
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/vendor.js
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.

URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/vendor.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/styles.css
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/runtime.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/polyfills.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/assets/public/favicon_js.ico
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/vendor.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/main.js
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/runtime.js
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/main.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/runtime.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/vendor.js
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/styles.css
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website

owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/main.js
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/runtime.js
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/vendor.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/build/routes/main.js
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/build/routes/polyfills.js
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website

owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/polyfills.js
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/ftp/encrypt.pyc
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/main.js
CWE ID: 693

Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/styles.css
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/main.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/main.js

CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/runtime.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/polyfills.js
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of

attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:376:14
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/build/routes/polyfills.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/build/routes/main.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/polyfills.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/vendor.js
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/ftp/encrypt.pyc
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium

Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/main.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/main.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/polyfills.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and

video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:365:14
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:376:14
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/vendor.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).

Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:365:14
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/main.js
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/ftp/quarantine/juicy_malware_linux_amd_64.url
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for

instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/main.js
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/ftp/quarantine
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/ftp/quarantine
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/ftp/quarantine/juicy_malware_macos_64.url
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/ftp/quarantine/juicy_malware_windows_64.exe.url
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/ftp/quarantine/juicy_malware_linux_arm_64.url
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/styles.css
Evidence: Access-Control-Allow-Origin: *

CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
Confidence: High
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page ? covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
URL: https://demo.owasp-juice.shop/ftp/
CWE ID: 693
Reference: https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
https://w3c.github.io/webappsec-csp/
https://web.dev/articles/csp
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Finding: Cross-Domain Misconfiguration

Risk Level: Medium
Confidence: Medium
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
URL: https://demo.owasp-juice.shop/ftp/
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

WebAssure Scanner Report

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/
Parameter: Reporting-Endpoints
Evidence: 1745990352
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/
Evidence: 1650485437

CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/assets/public/favicon_js.ico
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/runtime.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/assets/public/favicon_js.ico
Parameter: Reporting-Endpoints
Evidence: 1745990359
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/runtime.js
Parameter: Reporting-Endpoints
Evidence: 1745990359
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/robots.txt
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity

https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/robots.txt
Parameter: Reporting-Endpoints
Evidence: 1745990358
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/sitemap.xml
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/sitemap.xml
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/sitemap.xml
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html

https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/
Parameter: Reporting-Endpoints
Evidence: 1745990358
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/sitemap.xml
Parameter: Reporting-Endpoints
Evidence: 1745990358
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/sitemap.xml
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/sitemap.xml

Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/sitemap.xml
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/polyfills.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/polyfills.js
Parameter: Reporting-Endpoints
Evidence: 1745990359
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares

that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/vendor.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/vendor.js
Parameter: Reporting-Endpoints
Evidence: 1745990359
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/main.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/main.js
Parameter: Reporting-Endpoints

Evidence: 1745990359
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/main.js
Evidence: 1734944650
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/ftp/incident-support.kdbx
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk Level: Low
Confidence: High
Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
URL: https://demo.owasp-juice.shop/ftp/coupons_2013.md.bak
Evidence: Apache/2.4.63 (Unix)
CWE ID: 497
Reference: https://httpd.apache.org/docs/current/mod/core.html#servertokens
https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)
https://www.troyhunt.com/shhh-dont-let-your-response-headers/

Finding: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk Level: Low

Confidence: High
Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
URL: https://demo.owasp-juice.shop/ftp/package.json.bak
Evidence: Apache/2.4.63 (Unix)
CWE ID: 497
Reference: https://httpd.apache.org/docs/current/mod/core.html#servertokens
https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)
https://www.troyhunt.com/shhh-dont-let-your-response-headers/

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/ftp/coupons_2013.md.bak
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/ftp/package.json.bak
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix

Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/ftp/incident-support.kdbx
Parameter: Reporting-Endpoints
Evidence: 1745990365
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/ftp/order_5267-e790c915f10a4e0b.pdf
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/ftp/legal.md
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

URL: https://demo.owasp-juice.shop/ftp/acquisitions.md
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/ftp/eastere.gg
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/ftp/legal.md
Parameter: Reporting-Endpoints
Evidence: 1745990365
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/ftp/order_5267-e790c915f10a4e0b.pdf
Parameter: Reporting-Endpoints
Evidence: 1745990365
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

WebAssure Scanner Report

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/ftp/acquisitions.md
Parameter: Reporting-Endpoints
Evidence: 1745990365
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/ftp/suspicious_errors.yml
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/ftp/eastere.gg
Parameter: Reporting-Endpoints
Evidence: 1745990365
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/ftp/suspicious_errors.yml

Parameter: Reporting-Endpoints
Evidence: 1745990365
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/ftp
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/ftp
Parameter: Reporting-Endpoints
Evidence: 1745990359
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/styles.css
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium

Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/vendor.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/favicon_js.ico
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/styles.css
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/favicon_js.ico
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:286:9
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/layer.js:95:5
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/vendor.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:328:13
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/fileServer.js:43:13
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>

CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/styles.css
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/fileServer.js:59:18
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:421:3
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/favicon_js.ico
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/index.js:145:39
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:280:10
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:286:9
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/favicon_js.ico
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.

Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/layer.js:95:5
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/ftp/announcement_encrypted.md
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:328:13
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/fileServer.js:43:13
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low

Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/fileServer.js:59:18
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/styles.css
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:421:3
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/index.js:145:39
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by

end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/runtime.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:280:10
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/ftp/announcement_encrypted.md
Parameter: Reporting-Endpoints
Evidence: 1745990365
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/styles.css
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low

Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/runtime.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/build/routes/vendor.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/favicon_js.ico
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/styles.css

Parameter: Reporting-Endpoints
Evidence: 1745990366
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/favicon_js.ico
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/build/routes/fileServer.js:43:13
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/layer.js:95:5
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html

https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:328:13
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:286:9
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/vendor.js
Parameter: Reporting-Endpoints
Evidence: 1745990366
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

WebAssure Scanner Report

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/favicon_js.ico
Parameter: Reporting-Endpoints
Evidence: 1745990366
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/build/routes/styles.css
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:421:3
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High

Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/index.js:145:39
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/build/routes/fileServer.js:59:18
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:280:10
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low

Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/styles.css
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/layer.js:95:5
Parameter: Reporting-Endpoints
Evidence: 1745990366
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:328:13
Parameter: Reporting-Endpoints
Evidence: 1745990366
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/favicon_js.ico
Parameter: Reporting-Endpoints
Evidence: 1745990366
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low

Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/fileServer.js:43:13
Parameter: Reporting-Endpoints
Evidence: 1745990366
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:286:9
Parameter: Reporting-Endpoints
Evidence: 1745990366
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/vendor.js
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/favicon_js.ico
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares

that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/build/routes/runtime.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/styles.css
Parameter: Reporting-Endpoints
Evidence: 1745990366
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/fileServer.js:59:18
Parameter: Reporting-Endpoints
Evidence: 1745990366
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/index.js:145:39
Parameter: Reporting-Endpoints
Evidence: 1745990366
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

WebAssure Scanner Report

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:280:10
Parameter: Reporting-Endpoints
Evidence: 1745990366
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:421:3
Parameter: Reporting-Endpoints
Evidence: 1745990366
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/styles.css
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/styles.css
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/layer.js:95:5
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/fileServer.js:43:13
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/runtime.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/favicon_js.ico
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix

Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:286:9
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:328:13
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/vendor.js
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/favicon_js.ico
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/runtime.js

Parameter: Reporting-Endpoints
Evidence: 1745990366
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/styles.css
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/styles.css
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:421:3
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/index.js:145:39
Evidence: 1650485437
CWE ID: 497

Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/fileServer.js:59:18
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:280:10
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/styles.css
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/layer.js:95:5
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:328:13
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/favicon_js.ico
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:286:9
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/runtime.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix

Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/fileServer.js:43:13
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/vendor.js
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/favicon_js.ico
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/runtime.js
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/styles.css

Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:280:10
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:421:3
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/index.js:145:39
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/fileServer.js:59:18
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

WebAssure Scanner Report

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/layer.js:95:5
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:328:13
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/favicon_js.ico
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:286:9
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low

Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/fileServer.js:43:13
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/runtime.js
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/styles.css
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:280:10
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:421:3
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/index.js:145:39
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/fileServer.js:59:18
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/styles.css
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares

that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/runtime.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/runtime.js
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/styles.css
Parameter: Reporting-Endpoints
Evidence: 1745990367
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/styles.css
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/runtime.js
Parameter: Reporting-Endpoints
Evidence: 1745990367
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/assets/public/favicon_js.ico
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/favicon_js.ico
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/styles.css
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium

Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/styles.css
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/polyfills.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/vendor.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/polyfills.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/runtime.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/runtime.js
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/assets/public/favicon_js.ico
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/assets/public/favicon_js.ico
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/favicon_js.ico
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>

CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/vendor.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/styles.css
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/styles.css
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/polyfills.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/runtime.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/polyfills.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/assets/public/favicon_js.ico
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/vendor.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.

Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/runtime.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/polyfills.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/runtime.js
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/assets/public/favicon_js.ico
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/vendor.js

Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/vendor.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/styles.css
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/polyfills.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/runtime.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

WebAssure Scanner Report

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/styles.css
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/assets/public/favicon_js.ico
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/styles.css
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/runtime.js
Evidence: 1981395349
CWE ID: 497

Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/vendor.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/assets/public/favicon_js.ico
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/favicon_js.ico
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low

Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/styles.css
Parameter: Reporting-Endpoints
Evidence: 1745990367
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/polyfills.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/vendor.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/runtime.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/polyfills.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/assets/public/favicon_js.ico
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/styles.css
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/vendor.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/assets/public/favicon_js.ico
Parameter: Reporting-Endpoints
Evidence: 1745990367
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/favicon_js.ico
Parameter: Reporting-Endpoints
Evidence: 1745990367
CWE ID: 497

Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/polyfills.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/runtime.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/polyfills.js
Parameter: Reporting-Endpoints
Evidence: 1745990367
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/assets/public/favicon_js.ico
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/vendor.js
Parameter: Reporting-Endpoints
Evidence: 1745990367
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/styles.css
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/polyfills.js
Parameter: Reporting-Endpoints
Evidence: 1745990367
CWE ID: 497

Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/runtime.js
Parameter: Reporting-Endpoints
Evidence: 1745990367
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/assets/public/favicon_js.ico
Parameter: Reporting-Endpoints
Evidence: 1745990367
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/vendor.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose

exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/vendor.js
Parameter: Reporting-Endpoints
Evidence: 1745990367
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/styles.css
Parameter: Reporting-Endpoints
Evidence: 1745990367
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/assets/public/favicon_js.ico
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/favicon_js.ico
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/polyfills.js
Parameter: Reporting-Endpoints
Evidence: 1745990367
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/runtime.js
Parameter: Reporting-Endpoints
Evidence: 1745990367
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/main.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/styles.css
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/assets/public/favicon_js.ico

Parameter: Reporting-Endpoints
Evidence: 1745990367
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/polyfills.js
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/vendor.js
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/polyfills.js
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/runtime.js
Evidence: 1650485437
CWE ID: 497

Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/runtime.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/vendor.js
Parameter: Reporting-Endpoints
Evidence: 1745990367
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/assets/public/favicon_js.ico
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/assets/public/favicon_js.ico
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

WebAssure Scanner Report

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/favicon_js.ico
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/vendor.js
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/styles.css
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/polyfills.js
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low

Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/runtime.js
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/main.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/styles.css
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/polyfills.js
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/vendor.js
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/assets/public/favicon_js.ico
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/polyfills.js
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/runtime.js
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/runtime.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>

CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/assets/public/favicon_js.ico
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/vendor.js
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/assets/public/favicon_js.ico
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/favicon_js.ico
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/styles.css
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/vendor.js
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/polyfills.js
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/runtime.js
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix

Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/polyfills.js
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/vendor.js
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/assets/public/favicon_js.ico
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/runtime.js
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/polyfills.js

Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/vendor.js
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/assets/public/favicon_js.ico
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/vendor.js
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/styles.css
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

WebAssure Scanner Report

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/runtime.js
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/polyfills.js
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/main.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/assets/public/favicon_js.ico
Evidence: 1981395349
CWE ID: 497

Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/runtime.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/vendor.js
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/main.js
Parameter: Reporting-Endpoints
Evidence: 1745990367
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/vendor.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/runtime.js
Parameter: Reporting-Endpoints
Evidence: 1745990367
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/main.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/styles.css
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/main.js
Evidence: 1650485437

CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/runtime.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/vendor.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/runtime.js
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/polyfills.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

WebAssure Scanner Report

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/main.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/polyfills.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/ftp/encrypt.pyc
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/main.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>

CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/styles.css
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/main.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/main.js
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/main.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/runtime.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/polyfills.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/runtime.js
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/polyfills.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.

Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/main.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:376:14
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/polyfills.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/vendor.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/ftp/encrypt.pyc

Parameter: Reporting-Endpoints
Evidence: 1745990366
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/main.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/main.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/main.js
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/polyfills.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>

CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:365:14
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/runtime.js
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/vendor.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:376:14

Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/vendor.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/styles.css
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/main.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

WebAssure Scanner Report

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:365:14
Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/vendor.js
Parameter: Reporting-Endpoints
Evidence: 1745990367
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/runtime.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

URL: https://demo.owasp-juice.shop/app/build/routes/main.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/build/routes/polyfills.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/polyfills.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/styles.css
Parameter: Reporting-Endpoints

Evidence: 1745990367
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/main.js
Parameter: Reporting-Endpoints
Evidence: 1745990367
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/main.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/main.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

WebAssure Scanner Report

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/runtime.js
Parameter: Reporting-Endpoints
Evidence: 1745990368
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/polyfills.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/ftp/quarantine/juicy_malware_linux_amd_64.url
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low

Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/vendor.js
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/main.js
Parameter: Reporting-Endpoints
Evidence: 1745990368
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/polyfills.js
Parameter: Reporting-Endpoints
Evidence: 1745990368
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:376:14
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

WebAssure Scanner Report

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/polyfills.js
Parameter: Reporting-Endpoints
Evidence: 1745990367
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/vendor.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/main.js
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/styles.css
Evidence: 1650485437

CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/main.js
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/main.js
Parameter: Reporting-Endpoints
Evidence: 1745990367
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/main.js
Parameter: Reporting-Endpoints
Evidence: 1745990368
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/polyfills.js
Parameter: Reporting-Endpoints
Evidence: 1745990368

CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/runtime.js
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/vendor.js
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/ftp/quarantine/juicy_malware_linux_amd_64.url
Parameter: Reporting-Endpoints
Evidence: 1745990372
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:365:14
CWE ID: 319

Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:376:14
Parameter: Reporting-Endpoints
Evidence: 1745990366
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/polyfills.js
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/main.js
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low
Confidence: Medium
Description: The page includes one or more script files from a third-party domain.
Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/main.js

Parameter: //cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
CWE ID: 829

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/vendor.js
Parameter: Reporting-Endpoints
Evidence: 1745990367
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/polyfills.js
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/styles.css
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/main.js
Evidence: 2038834951
CWE ID: 497

Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/main.js
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/main.js
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/ftp/quarantine
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/runtime.js

Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/polyfills.js
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/vendor.js
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:365:14
Parameter: Reporting-Endpoints
Evidence: 1745990366
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/polyfills.js
Evidence: 2038834951
CWE ID: 497

Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/main.js
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:376:14
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/polyfills.js
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/vendor.js
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/styles.css
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/main.js
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/main.js
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/main.js
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix

Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/ftp/quarantine
Parameter: Reporting-Endpoints
Evidence: 1745990365
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/polyfills.js
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/runtime.js
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:365:14
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/ftp/quarantine/juicy_malware_macos_64.url
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:376:14
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/main.js
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/polyfills.js
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix

Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/vendor.js
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/polyfills.js
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/main.js
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/main.js
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low

Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/main.js
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/polyfills.js
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:365:14
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/ftp/quarantine/juicy_malware_macos_64.url
Parameter: Reporting-Endpoints
Evidence: 1745990372
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares

that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/ftp/quarantine/juicy_malware_windows_64.exe.url
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:376:14
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/main.js
Parameter: Reporting-Endpoints
Evidence: 1745990368
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/vendor.js
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/ftp/quarantine/juicy_malware_linux_arm_64.url
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:365:14
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/ftp/quarantine/juicy_malware_windows_64.exe.url
Parameter: Reporting-Endpoints
Evidence: 1745990372
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/main.js
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

WebAssure Scanner Report

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/ftp/quarantine/juicy_malware_linux_arm_64.url
Parameter: Reporting-Endpoints
Evidence: 1745990372
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/main.js
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/styles.css
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/main.js
Evidence: 1981395349

CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/styles.css
Parameter: Reporting-Endpoints
Evidence: 1745990359
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/styles.css
Evidence: 1701244813
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/styles.css
Evidence: 2033195021
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/styles.css
Evidence: 1839622642
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

WebAssure Scanner Report

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/styles.css
Evidence: 1680327869
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/styles.css
Evidence: 1863874346
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/styles.css
Evidence: 1917098446
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/styles.css
Evidence: 1818181818
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low

Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/styles.css
Evidence: 1650485437
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/styles.css
Evidence: 2038834951
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/styles.css
Evidence: 1981395349
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Strict-Transport-Security Header Not Set

Risk Level: Low
Confidence: High
Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
URL: https://demo.owasp-juice.shop/ftp/
CWE ID: 319
Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-community/Security_Headers
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
https://caniuse.com/stricttransportsecurity
https://datatracker.ietf.org/doc/html/rfc6797

Finding: Timestamp Disclosure - Unix

Risk Level: Low
Confidence: Low
Description: A timestamp was disclosed by the application/web server. - Unix
Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
URL: https://demo.owasp-juice.shop/ftp/
Parameter: Reporting-Endpoints
Evidence: 1745990372
CWE ID: 497
Reference: https://cwe.mitre.org/data/definitions/200.html

Finding: Re-examine Cache-control Directives

Risk Level: Informational
Confidence: Low
Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution: For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
URL: https://demo.owasp-juice.shop/
Parameter: cache-control
Evidence: public, max-age=0
CWE ID: 525
Reference:
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
https://grayduck.mn/2021/09/13/cache-control-recommendations/

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Re-examine Cache-control Directives

Risk Level: Informational
Confidence: Low
Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution: For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
URL: https://demo.owasp-juice.shop/robots.txt
Parameter: cache-control

CWE ID: 525
Reference:
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
https://grayduck.mn/2021/09/13/cache-control-recommendations/

Finding: Re-examine Cache-control Directives

Risk Level: Informational
Confidence: Low
Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution: For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
URL: https://demo.owasp-juice.shop/sitemap.xml
Parameter: cache-control
Evidence: public, max-age=0
CWE ID: 525
Reference:
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
https://grayduck.mn/2021/09/13/cache-control-recommendations/

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/sitemap.xml
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Information Disclosure - Suspicious Comments

Risk Level: Informational
Confidence: Low
Description: The response appears to contain suspicious comments which may help an attacker.
Solution: Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
URL: https://demo.owasp-juice.shop/vendor.js
Evidence: Query
CWE ID: 615

Finding: Information Disclosure - Suspicious Comments

Risk Level: Informational
Confidence: Low
Description: The response appears to contain suspicious comments which may help an attacker.

Solution: Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
URL: https://demo.owasp-juice.shop/main.js
Evidence: query
CWE ID: 615

Finding: Re-examine Cache-control Directives

Risk Level: Informational
Confidence: Low
Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution: For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
URL: https://demo.owasp-juice.shop/ftp/legal.md
Parameter: cache-control
Evidence: public, max-age=0
CWE ID: 525
Reference:
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
https://grayduck.mn/2021/09/13/cache-control-recommendations/

Finding: Re-examine Cache-control Directives

Risk Level: Informational
Confidence: Low
Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution: For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
URL: https://demo.owasp-juice.shop/ftp/acquisitions.md
Parameter: cache-control
Evidence: public, max-age=0
CWE ID: 525
Reference:
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
https://grayduck.mn/2021/09/13/cache-control-recommendations/

Finding: Re-examine Cache-control Directives

Risk Level: Informational
Confidence: Low
Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution: For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".

URL: https://demo.owasp-juice.shop/ftp
Parameter: cache-control
CWE ID: 525
Reference:
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
https://grayduck.mn/2021/09/13/cache-control-recommendations/

Finding: Re-examine Cache-control Directives

Risk Level: Informational
Confidence: Low
Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution: For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
URL: https://demo.owasp-juice.shop/app/build/routes/fileServer.js:59:18
Parameter: cache-control
Evidence: public, max-age=0
CWE ID: 525
Reference:
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
https://grayduck.mn/2021/09/13/cache-control-recommendations/

Finding: Re-examine Cache-control Directives

Risk Level: Informational
Confidence: Low
Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution: For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
URL: https://demo.owasp-juice.shop/app/build/routes/fileServer.js:43:13
Parameter: cache-control
Evidence: public, max-age=0
CWE ID: 525
Reference:
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
https://grayduck.mn/2021/09/13/cache-control-recommendations/

Finding: Re-examine Cache-control Directives

Risk Level: Informational
Confidence: Low
Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

Solution: For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:286:9
Parameter: cache-control
Evidence: public, max-age=0
CWE ID: 525
Reference:
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
https://grayduck.mn/2021/09/13/cache-control-recommendations/

Finding: Re-examine Cache-control Directives

Risk Level: Informational
Confidence: Low
Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution: For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:421:3
Parameter: cache-control
Evidence: public, max-age=0
CWE ID: 525
Reference:
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
https://grayduck.mn/2021/09/13/cache-control-recommendations/

Finding: Re-examine Cache-control Directives

Risk Level: Informational
Confidence: Low
Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution: For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/layer.js:95:5
Parameter: cache-control
Evidence: public, max-age=0
CWE ID: 525
Reference:
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
https://grayduck.mn/2021/09/13/cache-control-recommendations/

Finding: Re-examine Cache-control Directives

Risk Level: Informational
Confidence: Low

Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution: For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:328:13
Parameter: cache-control
Evidence: public, max-age=0
CWE ID: 525
Reference:
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
https://grayduck.mn/2021/09/13/cache-control-recommendations/

Finding: Re-examine Cache-control Directives

Risk Level: Informational
Confidence: Low
Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution: For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:280:10
Parameter: cache-control
Evidence: public, max-age=0
CWE ID: 525
Reference:
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
https://grayduck.mn/2021/09/13/cache-control-recommendations/

Finding: Re-examine Cache-control Directives

Risk Level: Informational
Confidence: Low
Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution: For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/index.js:145:39
Parameter: cache-control
Evidence: public, max-age=0
CWE ID: 525
Reference:
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
https://grayduck.mn/2021/09/13/cache-control-recommendations/

Finding: Re-examine Cache-control Directives

Risk Level: Informational
Confidence: Low
Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution: For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
URL: https://demo.owasp-juice.shop/ftp/announcement_encrypted.md
Parameter: cache-control
Evidence: public, max-age=0
CWE ID: 525
Reference:
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
https://grayduck.mn/2021/09/13/cache-control-recommendations/

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/styles.css
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/build/routes/vendor.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/favicon_js.ico
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

WebAssure Scanner Report

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/favicon_js.ico
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/layer.js:95:5
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:286:9
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/build/routes/fileServer.js:43:13
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:328:13

Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/build/routes/fileServer.js:59:18
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:421:3
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/build/routes/styles.css
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/index.js:145:39
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the

Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:280:10
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/build/routes/runtime.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/styles.css
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/runtime.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/styles.css
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/assets/public/favicon_js.ico
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/favicon_js.ico
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/polyfills.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/vendor.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/polyfills.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>

CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/runtime.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/assets/public/favicon_js.ico
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/vendor.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/styles.css
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/runtime.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/polyfills.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/assets/public/favicon_js.ico
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/vendor.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/main.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational

Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/runtime.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Re-examine Cache-control Directives

Risk Level: Informational
Confidence: Low
Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution: For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:376:14
Parameter: cache-control
Evidence: public, max-age=0
CWE ID: 525
Reference:
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
https://grayduck.mn/2021/09/13/cache-control-recommendations/

Finding: Re-examine Cache-control Directives

Risk Level: Informational
Confidence: Low
Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution: For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:365:14
Parameter: cache-control
Evidence: public, max-age=0
CWE ID: 525
Reference:
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
https://grayduck.mn/2021/09/13/cache-control-recommendations/

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.

URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/vendor.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/assets/public/main.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/styles.css
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/runtime.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/build/routes/main.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium

Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/build/routes/polyfills.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/serve-index/polyfills.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/main.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/assets/public/main.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Re-examine Cache-control Directives

Risk Level: Informational
Confidence: Low
Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution: For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
URL: https://demo.owasp-juice.shop/ftp/quarantine
Parameter: cache-control

CWE ID: 525
Reference:
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
https://grayduck.mn/2021/09/13/cache-control-recommendations/

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/polyfills.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:376:14
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/vendor.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/node_modules/express/lib/router/index.js:365:14
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/app/build/routes/assets/public/main.js
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: -1

Finding: Re-examine Cache-control Directives

Risk Level: Informational
Confidence: Low
Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution: For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
URL: https://demo.owasp-juice.shop/ftp/
Parameter: cache-control
CWE ID: 525
Reference:
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
https://grayduck.mn/2021/09/13/cache-control-recommendations/

Finding: Modern Web Application

Risk Level: Informational
Confidence: Medium
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution: This is an informational alert and so no changes are required.
URL: https://demo.owasp-juice.shop/ftp/
Evidence: ftp
CWE ID: -1

WebAssure Scanner Report

Nikto Findings

Finding ID: HEADER

Message: /: Retrieved via header: 1.1 heroku-router.
Method: GET

Finding ID: HEADER

Message: /: Retrieved access-control-allow-origin header: *.
Method: GET

Finding ID: HEADER

Message: /:X-Frame-Options header is deprecated and was replaced with the Content-Security-Policy HTTP header with the frame-ancestors directive instead.
Method: GET
References: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Finding ID: HEADER

Message: /: Uncommon header(s) 'reporting-endpoints' found, with contents: heroku-nel="https://nel.heroku.com/reports?s=l6OfOlHLakee2TKZUInZGssGtjLYaSA0JJ8iz1lNq9o%3D&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&ts=1745990202".
Method: GET

Finding ID: HEADER

Message: /: Uncommon header(s) 'x-recruiting' found, with contents: /#/jobs.
Method: GET

Finding ID: SSL

Message: /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined.
Method: GET
References: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security

Finding ID: MISC

Message: : Server banner changed from 'Heroku' to 'Apache/2.4.63 (Unix)'.
Method: GET