WebAssure Scanner Report

Scan Information

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

Scan Date: 2025-04-30 00:21:05

WebAssure Scanner Report

High and Medium Risk Findings

OWASP ZAP Findings:

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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/

Finding: Cross-Domain Misconfiguration (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/

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Cross-Domain Misconfiguration (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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Cross-Domain Misconfiguration (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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Cross-Domain Misconfiguration (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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Cross-Domain Misconfiguration (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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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

Finding: Cross-Domain Misconfiguration (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

Finding: Content Security Policy (CSP) Header Not Set (Medium)

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/

Finding: Cross-Domain Misconfiguration (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/

WebAssure Scanner Report

Nikto Findings:

ID: SSL

Finding: /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined.

References: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security