■ ZAP Vulnerability Scan Report

Target: http://juice-shop.herokuapp.com/
Generated: 2025-04-09 22:32:26

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Information Disclosure - Suspicious Comments (Informational)

Description: The response appears to contain suspicious comments which may help an attacker.

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Information Disclosure - Suspicious Comments (Informational)

Description: The response appears to contain suspicious comments which may help an attacker.

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Hidden File Found (Medium)

Description: A sensitive file was identified as accessible or available. This may leak administrative, configuration, or

Mitigation: Block access to hidden/system files.

Vulnerability: Hidden File Found (Medium)

Description: A sensitive file was identified as accessible or available. This may leak administrative, configuration, or

Mitigation: Block access to hidden/system files.

Vulnerability: Hidden File Found (Medium)

Description: A sensitive file was identified as accessible or available. This may leak administrative, configuration, or

Mitigation: Block access to hidden/system files.

Vulnerability: Hidden File Found (Medium)

Description: A sensitive file was identified as accessible or available. This may leak administrative, configuration, or

Mitigation: Block access to hidden/system files.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: CSP: Failure to Define Directive with No Fallback (Medium)

Description: The Content Security Policy fails to define one of the directives that has no fallback. Missing/excluding t

Mitigation: Define fallback directives and test with CSP evaluators.

Vulnerability: CSP: Failure to Define Directive with No Fallback (Medium)

Description: The Content Security Policy fails to define one of the directives that has no fallback. Missing/excluding t

Mitigation: Define fallback directives and test with CSP evaluators.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 typ...
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ...
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig...
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the...
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the...
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig...
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig...
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 typo
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typo
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 typ

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)
Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the
Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: 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 type

Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 type
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain Misconfiguration (Medium)

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig

Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)
Description: A timestamp was disclosed by the application/web server. - Unix
Mitigation: Avoid exposing file modification timestamps.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: 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 typ
Mitigation: Define CSP with self and trusted sources only.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain Misconfiguration (Medium)
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfig
Mitigation: Use strict Access-Control-Allow-Origin headers.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)
Description: The page includes one or more script files from a third-party domain.
Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Cross-Domain JavaScript Source File Inclusion (Low)

Description: The page includes one or more script files from a third-party domain.

Mitigation: Avoid including scripts from external sources unnecessarily.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Modern Web Application (Informational)

Description: The application appears to be a modern web application. If you need to explore it automatically then the

Mitigation: No specific mitigation found. Follow OWASP guidelines.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.

Vulnerability: Timestamp Disclosure - Unix (Low)

Description: A timestamp was disclosed by the application/web server. - Unix

Mitigation: Avoid exposing file modification timestamps.