Security Scan Report for https://www.saucedemo.com/

Summary

Severity	Count
High	0
Medium	6
Low	7
Informational	32

Detailed Findings

Finding: Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://janarthananpalanivel.vercel.app/
Description: The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.

Finding: Re-examine Cache-control Directives

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

Finding: Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://janarthananpalanivel.vercel.app/

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

Finding: Cross-Domain Misconfiguration

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

Finding: Cross-Domain JavaScript Source File Inclusion

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

Finding: Modern Web Application

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

Finding: Retrieved from Cache

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app/
Description: The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
Solution: Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store,

must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.

Finding: X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://janarthananpalanivel.vercel.app/
Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution: Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

Finding: Modern Web Application

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

Finding: Strict-Transport-Security Header Not Set

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

Finding: Timestamp Disclosure - Unix

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

Finding: Timestamp Disclosure - Unix

Risk Level: Low
URL: https://janarthananpalanivel.vercel.app/

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

Finding: User Agent Fuzzer

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app/
Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Solution:

Finding: User Agent Fuzzer

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app
Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Solution:

Finding: User Agent Fuzzer

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app/
Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Solution:

Finding: User Agent Fuzzer

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app
Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Solution:

Finding: User Agent Fuzzer

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app/
Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Solution:

Finding: User Agent Fuzzer

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app
Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Solution:

Finding: User Agent Fuzzer

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app/
Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Solution:

Finding: User Agent Fuzzer

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app
Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Solution:

Finding: User Agent Fuzzer

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app/
Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Solution:

Finding: User Agent Fuzzer

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app
Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Solution:

Finding: User Agent Fuzzer

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app/

Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Solution:

Finding: User Agent Fuzzer

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app
Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Solution:

Finding: User Agent Fuzzer

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app/
Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Solution:

Finding: User Agent Fuzzer

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app
Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Solution:

Finding: User Agent Fuzzer

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app/
Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Solution:

Finding: User Agent Fuzzer

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app
Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Solution:

Finding: User Agent Fuzzer

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app/
Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Solution:

Finding: User Agent Fuzzer

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app
Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Solution:

Finding: User Agent Fuzzer

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app
Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Solution:

Finding: User Agent Fuzzer

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app/
Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Solution:

Finding: User Agent Fuzzer

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app
Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Solution:

Finding: User Agent Fuzzer

Risk Level: Informational

URL: https://janarthananpalanivel.vercel.app/
Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Solution:

Finding: User Agent Fuzzer

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app
Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Solution:

Finding: User Agent Fuzzer

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app/
Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Solution:

Finding: Retrieved from Cache

Risk Level: Informational
URL: https://janarthananpalanivel.vercel.app/
Description: The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
Solution: Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.

Finding: Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://www.saucedemo.com/
Description: The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use

SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.

Finding: Re-examine Cache-control Directives

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

Finding: Content Security Policy (CSP) Header Not Set

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

Finding: Cross-Domain Misconfiguration

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

Finding: Modern Web Application

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

Finding: Retrieved from Cache

Risk Level: Informational
URL: https://www.saucedemo.com/
Description: The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
Solution: Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.

Finding: Strict-Transport-Security Header Not Set

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

Finding: X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://www.saucedemo.com/
Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution: Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.