Security Headers Report for http://192.168.0.156

Security Headers

Header	Purpose	Overview	Present	Value	Recommenda
X-Frame-Options	Prevents clickjacking by controlling whether a browser should be allowed to render a page in a frame or iframe.	Can be set to 'DENY' or 'SAMEORIGIN'. 'DENY' blocks all framing, while 'SAMEORIGIN' allows framing from the same origin.	No	N/A	Use 'DENY' or 'SAMEORIGIN Prefer using C with 'frame-ancestors' directive.
X-XSS-Protection	Provides basic protection against XSS attacks by enabling browser's XSS filters.	Can be set to '1; mode=block' to block pages when an XSS attack is detected, or '0' to disable XSS filtering.	No	N/A	Do not rely on header. Use CS for stronger X protection.
X-Content-Type-Options	Prevents browsers from interpreting files as a different MIME type than specified.	Setting this to 'nosniff' ensures the browser respects the specified Content-Type header.	No	N/A	Set to 'nosniff' avoid MIME ty sniffing attack
Referrer-Policy	Controls the amount of referrer information sent with requests.	Various policies such as 'no-referrer' or 'strict-origin-when-cross-origin'	No	N/A	Use 'no-referr or a similar restrictive pol to protect user privacy.

		limit referrer data exposure.			
Content-Type	Specifies the MIME type of the content being sent, guiding proper interpretation by the browser.	Ensures the content is interpreted correctly, avoiding MIME type confusion attacks.	Yes	text/html;charset=utf-8	Ensure this header is set correctly to av MIME type confusion.
Set-Cookie	Manages cookie security attributes to prevent attacks.	Attributes like 'Secure', 'HttpOnly', and 'SameSite' enhance cookie security.	No	N/A	Use 'Secure', 'HttpOnly', an 'SameSite' attributes to protect cookie
Strict-Transport-Security (HSTS)	Enforces HTTPS connections to prevent downgrade attacks.	Directs browsers to only connect over HTTPS, ensuring secure connections.	No	N/A	Set HSTS with long max-age value to enfor HTTPS and prevent downgrade attacks.
Expect-CT	Enforces Certificate Transparency to prevent fraudulent certificates.	Requires certificates to be logged in public CT logs to detect misissued certificates.	No	N/A	Add this heade enforce Certifi Transparency improve certificate security.
Content-Security-Policy (CSP)	Mitigates various attacks by controlling the sources of content that a page can load.	Specifies allowed sources for content, reducing risks of XSS and other content injection attacks.	No	N/A	Implement a robust CSP to control conter sources and mitigate code injection attac
Access-Control-	Controls which domains are	Manages cross-origin resource	No	N/A	Configure this header to rest access and

Allow-Origin	allowed to access resources on the server.	sharing (CORS) by specifying allowed origins.			prevent unauthorized cross-origin requests.
Cross-Origin-Opener-Policy (COOP)	Isolates browsing contexts to prevent potential cross-origin attacks.	COOP ensures content is isolated from other origins, reducing attack vectors.	No	N/A	Use COOP to enhance secur and isolate yo browsing cont
Cross-Origin-Embedder-Policy (COEP)	Prevents embedding of your content by third-party sites.	Protects your content from being embedded by unauthorized parties.	No	N/A	Implement CO to prevent unauthorized embedding an enhance secur
Cross-Origin-Resource-Policy (CORP)	Controls which origins can access resources from your site.	Manages access to your resources by different origins.	No	N/A	Use CORP to restrict access your resource and prevent unauthorized access.
Permissions-Policy	Controls which features and APIs can be used by a site or its subframes.	Restricts access to sensitive features and APIs based on origin.	No	N/A	Use Permissio Policy to mana feature access enhance secur
FLoC (Federated Learning of Cohorts)	Controls whether FLoC is used for interest-based advertising.	Disabling FLoC helps protect user privacy by avoiding interest-based tracking.	No	N/A	Ensure FLoC i disabled to enhance priva
Server	Reveals information about the server software used.	Exposing server details can assist attackers in identifying potential vulnerabilities.	Yes	Apache/2.2.14 (Unix) DAV/2 mod_ssl/2.2.14 OpenSSL/ 0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1	Hide or obscu this header to prevent revea server softwar details.

X-Powered-By	Indicates the technologies used by the server.	Revealing technology stack details can aid attackers in targeting specific vulnerabilities.	Yes	PHP/5.3.1	Remove or obscure this header to prev technology sta disclosure.
X-AspNet-Version	Reveals the version of ASP.NET used by the server.	Exposing ASP.NET version details can help attackers target known vulnerabilities.	No	N/A	Remove or obscure this header to avoi version disclosure.
X-AspNetMvc-Version	Indicates the version of ASP.NET MVC used by the server.	Revealing ASP.NET MVC version details can aid attackers in targeting vulnerabilities.	No	N/A	Remove or obscure this header to prev version disclosure.
X-DNS-Prefetch-Control	Controls DNS prefetching behavior in browsers.	Disabling DNS prefetching can prevent some privacy concerns related to DNS lookups.	No	N/A	Set this heade 'off' if DNS prefetching is needed.
Public-Key-Pins (HPKP)	Enforces public key pinning to prevent man-in-the-middle (MITM) attacks using fraudulent certificates.	HPKP is deprecated but was used to pin server public keys to prevent MITM attacks.	No	N/A	Be cautious w HPKP due to it deprecation a potential issue not implemen correctly.
X-Permitted-Cross-Domain-Policies	Controls cross-domain requests from Adobe Flash and other plugins.	Helps manage permissions for cross-domain requests to prevent	No	N/A	Set to 'none' o 'master-only' t limit cross-domain permissions.

		unauthorized access.				
Clear-Site-Data	Clears site data (cookies, cache, storage) for a given site.	Useful for clearing sensitive data when security breaches are suspected.	No	N/A		Use this heade with caution, a can impact us experience by clearing data.

Technology Stack Detection

Technology: Caching

- Apache server detected from Server header.
- PHP detected from X-Powered-By header.
- Cache-Control header detected.
- Expires header detected.
- Pragma header detected.