CybExplore Logo

Security Headers Report

Summary

Here is the summary of the security headers for the URL: http://192.168.0.156/

Header Information

Header	Purpose	Overview	Value	Recommendation	Statu
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.	False	N/A	Use 'SAM Prefe CSP 'fram ance direc
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.	False	N/A	Do n this h Use stron prote
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.	False	N/A	Set t to av type attac
Referrer-Policy	Controls the amount of referrer	Various policies such as 'no-referrer' or	False	N/A	Use refer simil

Header	Purpose	Overview	Value	Recommendation	Statu
	information sent with requests.	'strict-origin-when-cross-origin' limit referrer data exposure.			restri polic user
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.	True	text/html;charset=utf-8	Ensu head corre avoi type
Set-Cookie	Manages cookie security attributes to prevent attacks.	Attributes like 'Secure', 'HttpOnly', and 'SameSite' enhance cookie security.	False	N/A	Use 'Http 'Sam attrib prote
Strict-Transport-Security (HSTS)	Enforces HTTPS connections to prevent downgrade attacks.	Directs browsers to only connect over HTTPS, ensuring secure connections.	False	N/A	Set H a lon value enfo and down attac
Expect-CT	Enforces Certificate Transparency to prevent fraudulent certificates.	Requires certificates to be logged in public CT logs to detect misissued certificates.	False	N/A	Add to en Certi Trans and i certif secu
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.	False	N/A	Imple robus contr sourc mitig injec attac
	Controls which	Manages cross-origin	False	N/A	Conf head

Header	Purpose	Overview	Value	Recommendation	Statu
Access-Control-Allow-Origin	domains are allowed to access resources on the server.	resource sharing (CORS) by specifying allowed origins.			restri and unau cross requ
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.	False	N/A	Use enha secu isola brow conte
Cross-Origin-Embedder-Policy (COEP)	Prevents embedding of your content by third-party sites.	Protects your content from being embedded by unauthorized parties.	False	N/A	Imple COE preve unau embe enha secu
Cross-Origin-Resource-Policy (CORP)	Controls which origins can access resources from your site.	Manages access to your resources by different origins.	False	N/A	Use restri to yo reso preve unau acce
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.	False	N/A	Use Perm Polic mana acce enha secu
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.	False	N/A	Ensu disab enha priva
Server	Reveals information about the server	Exposing server details can assist attackers in identifying	True	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 obsc head preve revea

Header	Purpose	Overview	Value	Recommendation	Statu
	software used.	potential vulnerabilities.			serve detai
X-Powered-By	Indicates the technologies used by the server.	Revealing technology stack details can aid attackers in targeting specific vulnerabilities.	True	PHP/5.3.1	Rem obsc head prev techn stack discl
X-AspNet-Version	Reveals the version of ASP.NET used by the server.	Exposing ASP.NET version details can help attackers target known vulnerabilities.	False	N/A	Rem obsc head versi discl
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.	False	N/A	Rem obsc head prev discl
X-DNS-Prefetch-Control	Controls DNS prefetching behavior in browsers.	Disabling DNS prefetching can prevent some privacy concerns related to DNS lookups.	False	N/A	Set t to 'of prefe not n
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.	False	N/A	Be ca with to its depr and issue imple corre
X-Permitted-Cross-Domain-Policies	Controls cross-domain requests from Adobe	Helps manage permissions for cross-domain requests to prevent	False	N/A	Set t 'mas limit

Header	Purpose	Overview	Value	Recommendation	Statu
	Flash and other plugins.	unauthorized access.			doma perm
Clear-Site-Data	Clears site data (cookies, cache, storage) for a given site.	Useful for clearing sensitive data when security breaches are suspected.	False	N/A	Use with it ca user expe clear

Technology Stack Detection

Technology: