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	Value
X-Frame-Options	{'Purpose': 'Prevents clickjacking by controlling whether a browser should be allowed to render a page in a frame or iframe.', 'Overview': "Can be set to 'DENY' or 'SAMEORIGIN'. 'DENY' blocks all framing, while 'SAMEORIGIN' allows framing from the same origin.", 'Present': False, 'Value': 'N/A', 'Recommendation': "Use 'DENY' or 'SAMEORIGIN'. Prefer using CSP with 'frame-ancestors' directive.", 'Vulnerable': 'Yes'}
X-XSS-Protection	{'Purpose': "Provides basic protection against XSS attacks by enabling browser's XSS filters.", 'Overview': "Can be set to '1; mode=block' to block pages when an XSS attack is detected, or '0' to disable XSS filtering.", 'Present': False, 'Value': 'N/A', 'Recommendation': 'Do not rely on this header. Use CSP for stronger XSS protection.', 'Vulnerable': 'Yes'}
X-Content-Type-Options	{'Purpose': 'Prevents browsers from interpreting files as a different MIME type than specified.', 'Overview': "Setting this to 'nosniff' ensures the browser respects the specified Content-Type header.", 'Present': False, 'Value': 'N/A', 'Recommendation': "Set to 'nosniff' to avoid MIME type sniffing attacks.", 'Vulnerable': 'Yes'}
Referrer-Policy	{'Purpose': 'Controls the amount of referrer information sent with requests.', 'Overview': "Various policies such as 'no-referrer' or 'strict-origin-when-cross-origin' limit referrer data exposure.", 'Present': False, 'Value': 'N/A', 'Recommendation': "Use 'no-referrer' or a similar restrictive policy to protect user privacy.", 'Vulnerable': 'Yes'}
Content-Type	{'Purpose': 'Specifies the MIME type of the content being sent, guiding proper interpretation by the browser.', 'Overview': 'Ensures the content is interpreted correctly, avoiding MIME type confusion attacks.', 'Present': True, 'Value': 'text/

Header	Value
	html;charset=utf-8', 'Recommendation': 'Ensure this header is set correctly to avoid MIME type confusion.', 'Vulnerable': 'No'}
Set-Cookie	{'Purpose': 'Manages cookie security attributes to prevent attacks.', 'Overview': "Attributes like 'Secure', 'HttpOnly', and 'SameSite' enhance cookie security.", 'Present': False, 'Value': 'N/A', 'Recommendation': "Use 'Secure', 'HttpOnly', and 'SameSite' attributes to protect cookies.", 'Vulnerable': 'Yes'}
Strict-Transport-Security (HSTS)	{'Purpose': 'Enforces HTTPS connections to prevent downgrade attacks.', 'Overview': 'Directs browsers to only connect over HTTPS, ensuring secure connections.', 'Present': False, 'Value': 'N/A', 'Recommendation': 'Set HSTS with a long max-age value to enforce HTTPS and prevent downgrade attacks.', 'Vulnerable': 'Yes'}
Expect-CT	{'Purpose': 'Enforces Certificate Transparency to prevent fraudulent certificates.', 'Overview': 'Requires certificates to be logged in public CT logs to detect misissued certificates.', 'Present': False, 'Value': 'N/A', 'Recommendation': 'Add this header to enforce Certificate Transparency and improve certificate security.', 'Vulnerable': 'Yes'}
Content-Security-Policy (CSP)	{'Purpose': 'Mitigates various attacks by controlling the sources of content that a page can load.', 'Overview': 'Specifies allowed sources for content, reducing risks of XSS and other content injection attacks.', 'Present': False, 'Value': 'N/A', 'Recommendation': 'Implement a robust CSP to control content sources and mitigate code injection attacks.', 'Vulnerable': 'Yes'}
Access-Control-Allow-Origin	{'Purpose': 'Controls which domains are allowed to access resources on the server.', 'Overview': 'Manages cross-origin resource sharing (CORS) by specifying allowed origins.', 'Present': False, 'Value': 'N/A', 'Recommendation': 'Configure this header to restrict access and prevent unauthorized cross-origin requests.', 'Vulnerable': 'Yes'}
Cross-Origin-Opener-Policy (COOP)	{'Purpose': 'Isolates browsing contexts to prevent potential cross-origin attacks.', 'Overview': 'COOP ensures content is isolated from other origins, reducing attack vectors.', 'Present': False, 'Value': 'N/A', 'Recommendation': 'Use COOP to enhance security and isolate your browsing context.', 'Vulnerable': 'Yes'}
Cross-Origin-Embedder-Policy (COEP)	{'Purpose': 'Prevents embedding of your content by third-party sites.', 'Overview': 'Protects your content from being embedded by unauthorized parties.', 'Present': False, 'Value': 'N/A', 'Recommendation': 'Implement COEP to prevent unauthorized embedding and enhance security.', 'Vulnerable': 'Yes'}

Header	Value
Cross-Origin-Resource-Policy (CORP)	{'Purpose': 'Controls which origins can access resources from your site.', 'Overview': 'Manages access to your resources by different origins.', 'Present': False, 'Value': 'N/A', 'Recommendation': 'Use CORP to restrict access to your resources and prevent unauthorized access.', 'Vulnerable': 'Yes'}
Permissions-Policy	{'Purpose': 'Controls which features and APIs can be used by a site or its subframes.', 'Overview': 'Restricts access to sensitive features and APIs based on origin.', 'Present': False, 'Value': 'N/A', 'Recommendation': 'Use Permissions-Policy to manage feature access and enhance security.', 'Vulnerable': 'Yes'}
FLoC (Federated Learning of Cohorts)	{'Purpose': 'Controls whether FLoC is used for interest-based advertising.', 'Overview': 'Disabling FLoC helps protect user privacy by avoiding interest-based tracking.', 'Present': False, 'Value': 'N/A', 'Recommendation': 'Ensure FLoC is disabled to enhance privacy.', 'Vulnerable': 'Yes'}
Server	{'Purpose': 'Reveals information about the server software used.', 'Overview': 'Exposing server details can assist attackers in identifying potential vulnerabilities.', 'Present': True, 'Value': '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', 'Recommendation': 'Hide or obscure this header to prevent revealing server software details.', 'Vulnerable': 'No'}
X-Powered-By	{'Purpose': 'Indicates the technologies used by the server.', 'Overview': 'Revealing technology stack details can aid attackers in targeting specific vulnerabilities.', 'Present': True, 'Value': 'PHP/5.3.1', 'Recommendation': 'Remove or obscure this header to prevent technology stack disclosure.', 'Vulnerable': 'No'}
X-AspNet-Version	{'Purpose': 'Reveals the version of ASP.NET used by the server.', 'Overview': 'Exposing ASP.NET version details can help attackers target known vulnerabilities.', 'Present': False, 'Value': 'N/A', 'Recommendation': 'Remove or obscure this header to avoid version disclosure.', 'Vulnerable': 'Yes'}
X-AspNetMvc-Version	{'Purpose': 'Indicates the version of ASP.NET MVC used by the server.', 'Overview': 'Revealing ASP.NET MVC version details can aid attackers in targeting vulnerabilities.', 'Present': False, 'Value': 'N/A', 'Recommendation': 'Remove or obscure this header to prevent version disclosure.', 'Vulnerable': 'Yes'}
X-DNS-Prefetch-	{'Purpose': 'Controls DNS prefetching behavior in browsers.', 'Overview': 'Disabling DNS prefetching can prevent some

Header	Value
	'Value': 'N/A', 'Recommendation': "Set this header to 'off' if DNS prefetching is not needed.", 'Vulnerable': 'Yes'}
Public-Key-Pins (HPKP)	{'Purpose': 'Enforces public key pinning to prevent man-in-the-middle (MITM) attacks using fraudulent certificates.', 'Overview': 'HPKP is deprecated but was used to pin server public keys to prevent MITM attacks.', 'Present': False, 'Value': 'N/A', 'Recommendation': 'Be cautious with HPKP due to its deprecation and potential issues if not implemented correctly.', 'Vulnerable': 'Yes'}
X-Permitted-Cross-Domain-Policies	{'Purpose': 'Controls cross-domain requests from Adobe Flash and other plugins.', 'Overview': 'Helps manage permissions for cross-domain requests to prevent unauthorized access.', 'Present': False, 'Value': 'N/A', 'Recommendation': "Set to 'none' or 'master-only' to limit cross-domain permissions.", 'Vulnerable': 'Yes'}
Clear-Site-Data	{'Purpose': 'Clears site data (cookies, cache, storage) for a given site.', 'Overview': 'Useful for clearing sensitive data when security breaches are suspected.', 'Present': False, 'Value': 'N/A', 'Recommendation': 'Use this header with caution, as it can impact user experience by clearing data.', 'Vulnerable': 'Yes'}

Technology Stack

- Technology
- Details