This QID reports the absence of the following <A HREF="https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers" TARGET="_blank">HTTP headers</A> according to <A HREF="https://cwe.mitre.org/data/definitions/693.html" TARGET="_blank">CWE-693: Protection Mechanism Failure</A>:

X-Frame-Options: This HTTP response header improves the protection of web applications against clickjacking attacks. Clickjacking, also known as a "UI redress attack", allows an attacker to use multiple transparent or opaque layers to trick a targeted user into clicking on a button or link on another page when they were intending to click on the the top level page.

X-XSS-Protection: This HTTP header enables the browser built-in Cross-Site Scripting (XSS) filter to prevent cross-site scripting attacks. X-XSS-Protection: 0; disables this functionality.

X-Content-Type-Options: This HTTP header prevents attacks based on MIME-type mismatch. The only possible value is nosniff. If your server returns X-Content-Type-Options: nosniff in the response, the browser will refuse to load the styles and scripts in case they have an incorrect MIME-type.

Content-Security-Policy: This HTTP header helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS), packet sniffing attacks and data injection attacks.

Strict-Transport-Security: The HTTP Strict-Transport-Security response header (HSTS) is a security feature that lets a web site tell browsers that it should only be communicated with using HTTPS, instead of using HTTP.

QID Detection Logic:

This unauthenticated QID looks for the presence of the following HTTP responses:

Valid directives for X-Frame-Options are:

X-Frame-Options: DENY - The page cannot be displayed in a frame, regardless of the site attempting to do so.

X-Frame-Options: SAMEORIGIN - The page can only be displayed in a frame on the same origin as the page itself.

X-Frame-Options: ALLOW-FROM RESOURCE-URL - The page can only be displayed in a frame on the specified origin.

Content-Security-Policy: frame-ancestors - This directive specifies valid parents that may embed a page using frame, iframe, object, embed, or applet

Valid directives for X-XSS-Protections are:

X-XSS-Protection: 1 - Enables XSS filtering (usually default in browsers). If a cross-site scripting attack is detected, the browser will sanitize the page (remove the unsafe parts).

X-XSS-Protection: 1; mode=block - Enables XSS filtering. Rather than sanitizing the page, the browser will prevent rendering of the page if an attack is detected.

X-XSS-Protection: 1; report=URI - Enables XSS filtering. If a cross-site scripting attack is detected, the browser will sanitize the page and report the violation. This uses the functionality of the CSP report-uri directive to send a report.

X-XSS-Protection: 0 disables this directive and hence is also treated as not detected.

A valid directive for X-Content-Type-Options: nosniff

A valid directive for Content-Security-Policy: <policy-directive>; <policy-directive>

A valid HSTS directive Strict-Transport-Security: max-age=<expire-time>; [; includeSubDomains][; preload]

NOTE: All report-only directives (where applicable) are considered invalid.