Valnara Security Scan Report

Scan Details:

Target URL: https://public-firing-range.appspot.com/
Scan Type: Passive Scan
Scan Depth: 5
Start Time: 2025-04-03 23:22:57
End Time: 2025-04-03 23:23:46

Risk Summary:

Medium Risk Vulnerabilities: 109
Low Risk Vulnerabilities: 1
Informational Risk Vulnerabilities: 55

Detailed Vulnerabilities:

Missing Anti-clickjacking Header
Risk Level: Medium
URL: https://public-firing-range.appspot.com/
Remediation: 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.

Re-examine Cache-control Directives
Risk Level: Informational
URL: https://public-firing-range.appspot.com/
Remediation: 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".

Content Security Policy (CSP) Header Not Set
Risk Level: Medium
URL: https://public-firing-range.appspot.com/
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Strict-Transport-Security Header Not Set
Risk Level: Low
URL: https://public-firing-range.appspot.com/
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/
Remediation: 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.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/robots.txt
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/sitemap.xml
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/index.html
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/leakedcookie/index.html
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/stricttransportsecurity/index.html
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/redirect/index.html
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/clickjacking/index.html
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/reverseclickjacking/
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/angular/index.html
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/reflected/index.html
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/escape/index.html
Remediation: 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.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/robots.txt

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/sitemap.xml
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/dom/index.html
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/tags/index.html
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/vulnerablelibraries/index.html
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/urldom/index.html
Remediation: 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.

Re-examine Cache-control Directives

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/index.html
Remediation: 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".

Re-examine Cache-control Directives

Risk Level: Informational
URL: https://public-firing-range.appspot.com/stricttransportsecurity/index.html
Remediation: 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".

Re-examine Cache-control Directives

Risk Level: Informational
URL: https://public-firing-range.appspot.com/leakedcookie/index.html
Remediation: 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".

Re-examine Cache-control Directives

Risk Level: Informational
URL: https://public-firing-range.appspot.com/redirect/index.html
Remediation: 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".

Re-examine Cache-control Directives

Risk Level: Informational
URL: https://public-firing-range.appspot.com/clickjacking/index.html
Remediation: 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".

Re-examine Cache-control Directives

Risk Level: Informational
URL: https://public-firing-range.appspot.com/reverseclickjacking/
Remediation: 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".

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/cors/index.html
Remediation: 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.

Re-examine Cache-control Directives

Risk Level: Informational
URL: https://public-firing-range.appspot.com/angular/index.html
Remediation: 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".

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/flashinjection/index.html

Remediation: 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.

Re-examine Cache-control Directives

Risk Level: Informational
URL: https://public-firing-range.appspot.com/vulnerablelibraries/index.html
Remediation: 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".

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/leakedcookie/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/stricttransportsecurity/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/redirect/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/reverseclickjacking/
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/clickjacking/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Re-examine Cache-control Directives

Risk Level: Informational
URL: https://public-firing-range.appspot.com/tags/index.html

Remediation: 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".

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/angular/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/vulnerablelibraries/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Re-examine Cache-control Directives

Risk Level: Informational
URL: https://public-firing-range.appspot.com/flashinjection/index.html
Remediation: 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".

Re-examine Cache-control Directives

Risk Level: Informational
URL: https://public-firing-range.appspot.com/cors/index.html
Remediation: 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".

Re-examine Cache-control Directives

Risk Level: Informational
URL: https://public-firing-range.appspot.com/urldom/index.html
Remediation: 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".

Re-examine Cache-control Directives

Risk Level: Informational
URL: https://public-firing-range.appspot.com/dom/index.html
Remediation: 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".

Re-examine Cache-control Directives

Risk Level: Informational
URL: https://public-firing-range.appspot.com/escape/index.html
Remediation: 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".

Re-examine Cache-control Directives

Risk Level: Informational

URL: https://public-firing-range.appspot.com/reflected/index.html
Remediation: 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".

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/stricttransportsecurity/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/leakedcookie/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/redirect/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/clickjacking/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/tags/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/reverseclickjacking/
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/flashinjection/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/escape/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/cors/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/reflected/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/vulnerablelibraries/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/dom/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/urldom/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/angular/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/leakedcookie/index.html
Remediation: 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.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/stricttransportsecurity/index.html

Remediation: 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.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/index.html
Remediation: 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.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/redirect/index.html
Remediation: 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.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/clickjacking/index.html
Remediation: 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.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/reverseclickjacking/
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/insecurethirdpartyscripts/index.html
Remediation: 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.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/tags/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/flashinjection/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/vulnerablelibraries/index.html
Remediation: 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.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/angular/index.html
Remediation: 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.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/cors/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/dom/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/urldom/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/escape/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/reflected/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Missing Anti-clickjacking Header

Risk Level: Medium

URL: https://public-firing-range.appspot.com/badscriptimport/index.html
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/mixedcontent/index.html
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/remoteinclude/index.html
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/documentwriteln
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/assign
Remediation: 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.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/tags/index.html
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/documentwrite
Remediation: 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.

Re-examine Cache-control Directives
Risk Level: Informational
URL: https://public-firing-range.appspot.com/insecurethirdpartyscripts/index.html
Remediation: 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".

X-Content-Type-Options Header Missing
Risk Level: Low
URL: https://public-firing-range.appspot.com/flashinjection/index.html
Remediation: 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.

Missing Anti-clickjacking Header
Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/function
Remediation: 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.

Missing Anti-clickjacking Header
Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location/assign
Remediation: 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.

X-Content-Type-Options Header Missing
Risk Level: Low
URL: https://public-firing-range.appspot.com/cors/index.html
Remediation: 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.

X-Content-Type-Options Header Missing
Risk Level: Low
URL: https://public-firing-range.appspot.com/urldom/index.html

Remediation: 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.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/dom/index.html
Remediation: 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.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/reflected/index.html
Remediation: 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.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/escape/index.html
Remediation: 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.

Re-examine Cache-control Directives

Risk Level: Informational
URL: https://public-firing-range.appspot.com/badscriptimport/index.html
Remediation: 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".

Re-examine Cache-control Directives

Risk Level: Informational
URL: https://public-firing-range.appspot.com/remoteinclude/index.html
Remediation: 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".

Re-examine Cache-control Directives

Risk Level: Informational
URL: https://public-firing-range.appspot.com/mixedcontent/index.html
Remediation: 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".

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/documentwriteln

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/insecurethirdpartyscripts/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/assign
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/documentwrite
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/innerHtml
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/setTimeout
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/onclickSetAttribute
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/onclickAddEventListener
Remediation: 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.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location/assign
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/function
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/eval
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/replace
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/inlineevent
Remediation: 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.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/badscriptimport/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/remoteinclude/index.html

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/mixedcontent/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/location.hash/documentwriteln
Remediation: This is an informational alert and so no changes are required.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/insecurethirdpartyscripts/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/location.hash/documentwrite
Remediation: This is an informational alert and so no changes are required.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/location.hash/assign
Remediation: This is an informational alert and so no changes are required.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/innerHtml
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/setTimeout
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/onclickSetAttribute
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/onclickAddEventListener
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/location/assign
Remediation: This is an informational alert and so no changes are required.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/location.hash/function
Remediation: This is an informational alert and so no changes are required.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/eval
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/replace
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/inlineevent
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/documentwriteln
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Private IP Disclosure

Risk Level: Low
URL: https://public-firing-range.appspot.com/badscriptimport/index.html
Remediation: Remove the private IP address from the HTTP response body. For comments, use JSP/ASP/PHP comment instead of HTML/JavaScript comment which can be seen by client browsers.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/remoteinclude/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Secure Pages Include Mixed Content (Including Scripts)

Risk Level: Medium
URL: https://public-firing-range.appspot.com/mixedcontent/index.html
Remediation: A page that is available over SSL/TLS must be comprised completely of content which is transmitted over SSL/TLS. The page must not contain any content that is transmitted over unencrypted HTTP. This includes content from third party sites.

X-Content-Type-Options Header Missing

Risk Level: Low

URL: https://public-firing-range.appspot.com/insecurethirdpartyscripts/index.html
Remediation: 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.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/assign
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/documentwrite
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/location.hash/setTimeout
Remediation: This is an informational alert and so no changes are required.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/location.hash/innerHtml
Remediation: This is an informational alert and so no changes are required.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location/assign
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/function
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/location.hash/onclickSetAttribute
Remediation: This is an informational alert and so no changes are required.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/location.hash/eval
Remediation: This is an informational alert and so no changes are required.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/location.hash/onclickAddEventListener
Remediation: This is an informational alert and so no changes are required.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/location.hash/inlineevent
Remediation: This is an informational alert and so no changes are required.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/location.hash/replace
Remediation: This is an informational alert and so no changes are required.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/documentwriteln
Remediation: 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.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/badscriptimport/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/remoteinclude/index.html
Remediation: 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.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/mixedcontent/index.html
Remediation: This is an informational alert and so no changes are required.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/locationhref/documentwrite
Remediation: 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.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/documentwrite
Remediation: 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.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/assign
Remediation: 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.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/setTimeout
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/innerHtml
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/onclickSetAttribute
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/eval
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/onclickAddEventListener
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location/assign
Remediation: 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.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/function
Remediation: 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.

Strict-Transport-Security Header Not Set
Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/inlineevent
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set
Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/replace
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

X-Content-Type-Options Header Missing
Risk Level: Low
URL: https://public-firing-range.appspot.com/badscriptimport/index.html
Remediation: 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.

Missing Anti-clickjacking Header
Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/formaction
Remediation: 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.

Missing Anti-clickjacking Header
Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/URLUnencoded/documentwrite
Remediation: 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.

Strict-Transport-Security Header Not Set
Risk Level: Low
URL: https://public-firing-range.appspot.com/mixedcontent/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Content Security Policy (CSP) Header Not Set
Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/locationhref/documentwrite
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/jshref
Remediation: 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.

X-Content-Type-Options Header Missing
Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/setTimeout
Remediation: 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.

X-Content-Type-Options Header Missing
Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/innerHtml
Remediation: 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.

X-Content-Type-Options Header Missing
Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/onclickSetAttribute
Remediation: 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.

X-Content-Type-Options Header Missing
Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/onclickAddEventListener
Remediation: 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.

X-Content-Type-Options Header Missing
Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/eval
Remediation: 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.

X-Content-Type-Options Header Missing
Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/replace

Remediation: 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.

X-Content-Type-Options Header Missing
Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/inlineevent
Remediation: 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.

X-Content-Type-Options Header Missing
Risk Level: Low
URL: https://public-firing-range.appspot.com/mixedcontent/index.html
Remediation: 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.

Modern Web Application
Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/locationhref/documentwrite
Remediation: This is an informational alert and so no changes are required.

Content Security Policy (CSP) Header Not Set
Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/formaction
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set
Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/URLUnencoded/documentwrite
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set
Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/jshref
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Strict-Transport-Security Header Not Set
Risk Level: Low
URL: https://public-firing-range.appspot.com/address/locationhref/documentwrite
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Modern Web Application
Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/URLUnencoded/documentwrite

Remediation: This is an informational alert and so no changes are required.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/location.hash/formaction
Remediation: This is an informational alert and so no changes are required.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/location.hash/jshref
Remediation: This is an informational alert and so no changes are required.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/formaction
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/locationhref/documentwrite
Remediation: 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.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/URLUnencoded/documentwrite
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/jshref
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/formaction
Remediation: 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.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/jshref
Remediation: 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.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/URLUnencoded/documentwrite
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/documentURI/documentwrite
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/locationsearch/documentwrite
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location/innerHtml
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/stricttransportsecurity/hsts_missing
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location/documentwriteln
Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium

URL: https://public-firing-range.appspot.com/address/location/replace

Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium

URL: https://public-firing-range.appspot.com/address/location/documentwrite

Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium

URL: https://public-firing-range.appspot.com/address/location.hash/rangeCreateContextualFragment

Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium

URL: https://public-firing-range.appspot.com/address/location/eval

Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium

URL: https://public-firing-range.appspot.com/address/location/setTimeout

Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium

URL: https://public-firing-range.appspot.com/address/locationpathname/documentwrite

Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium

URL: https://public-firing-range.appspot.com/address/location/rangeCreateContextualFragment

Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium

URL: https://public-firing-range.appspot.com/redirect/meta?q=/

Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium

URL: https://public-firing-range.appspot.com/address/baseURI/documentwrite

Remediation: 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.

Missing Anti-clickjacking Header

Risk Level: Medium

URL: https://public-firing-range.appspot.com/address/URL/documentwrite

Remediation: 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.

Session Management Response Identified

Risk Level: Informational

URL: https://public-firing-range.appspot.com/leakedcookie/leakedcookie

Remediation: This is an informational alert rather than a vulnerability and so there is nothing to fix.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium

URL: https://public-firing-range.appspot.com/address/locationsearch/documentwrite

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium

URL: https://public-firing-range.appspot.com/address/documentURI/documentwrite

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://public-firing-range.appspot.com/leakedcookie/leakedcookie
Remediation: 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.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/stricttransportsecurity/hsts_missing
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location.hash/rangeCreateContextualFragment
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/URL/documentwrite
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/locationpathname/documentwrite
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location/documentwrite
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/redirect/meta?q=/
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium
URL: https://public-firing-range.appspot.com/address/location/eval
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium

URL: https://public-firing-range.appspot.com/address/location/innerHtml

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium

URL: https://public-firing-range.appspot.com/address/location/setTimeout

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium

URL: https://public-firing-range.appspot.com/address/location/documentwriteln

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium

URL: https://public-firing-range.appspot.com/address/baseURI/documentwrite

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium

URL: https://public-firing-range.appspot.com/address/location/replace

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium

URL: https://public-firing-range.appspot.com/address/location/rangeCreateContextualFragment

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Modern Web Application

Risk Level: Informational

URL: https://public-firing-range.appspot.com/address/documentURI/documentwrite

Remediation: This is an informational alert and so no changes are required.

Modern Web Application

Risk Level: Informational

URL: https://public-firing-range.appspot.com/address/locationsearch/documentwrite

Remediation: This is an informational alert and so no changes are required.

Strict-Transport-Security Header Not Set

Risk Level: Low

URL: https://public-firing-range.appspot.com/stricttransportsecurity/hsts_missing

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium

URL: https://public-firing-range.appspot.com/leakedcookie/leakedcookie
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/locationpathname/documentwrite
Remediation: This is an informational alert and so no changes are required.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/URL/documentwrite
Remediation: This is an informational alert and so no changes are required.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/location.hash/rangeCreateContextualFragment
Remediation: This is an informational alert and so no changes are required.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/location/setTimeout
Remediation: This is an informational alert and so no changes are required.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/location/eval
Remediation: This is an informational alert and so no changes are required.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/location/innerHtml
Remediation: This is an informational alert and so no changes are required.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/location/documentwrite
Remediation: This is an informational alert and so no changes are required.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/location/documentwriteln
Remediation: This is an informational alert and so no changes are required.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/baseURI/documentwrite
Remediation: This is an informational alert and so no changes are required.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/redirect/meta?q=/
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/documentURI/documentwrite
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/locationsearch/documentwrite
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/location/replace
Remediation: This is an informational alert and so no changes are required.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/address/location/rangeCreateContextualFragment
Remediation: This is an informational alert and so no changes are required.

Cookie without SameSite Attribute

Risk Level: Low
URL: https://public-firing-range.appspot.com/leakedcookie/leakedcookie
Remediation: Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/stricttransportsecurity/hsts_missing
Remediation: 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.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/locationpathname/documentwrite
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/URL/documentwrite
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/rangeCreateContextualFragment
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low

URL: https://public-firing-range.appspot.com/address/location/setTimeout

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low

URL: https://public-firing-range.appspot.com/address/location/innerHtml

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low

URL: https://public-firing-range.appspot.com/address/baseURI/documentwrite

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low

URL: https://public-firing-range.appspot.com/address/location/documentwriteln

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

User Controllable HTML Element Attribute (Potential XSS)

Risk Level: Informational

URL: https://public-firing-range.appspot.com/redirect/meta?q=/

Remediation: Validate all input and sanitize output it before writing to any HTML attributes.

Strict-Transport-Security Header Not Set

Risk Level: Low

URL: https://public-firing-range.appspot.com/address/location/documentwrite

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low

URL: https://public-firing-range.appspot.com/address/location/eval

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low

URL: https://public-firing-range.appspot.com/address/location/replace

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Strict-Transport-Security Header Not Set

Risk Level: Low

URL: https://public-firing-range.appspot.com/address/location/rangeCreateContextualFragment

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

X-Content-Type-Options Header Missing

Risk Level: Low

URL: https://public-firing-range.appspot.com/address/documentURI/documentwrite
Remediation: 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.

X-Content-Type-Options Header Missing
Risk Level: Low
URL: https://public-firing-range.appspot.com/address/locationsearch/documentwrite
Remediation: 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.

Cookie Without Secure Flag
Risk Level: Low
URL: https://public-firing-range.appspot.com/leakedcookie/leakedcookie
Remediation: Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

X-Content-Type-Options Header Missing
Risk Level: Low
URL: https://public-firing-range.appspot.com/address/locationpathname/documentwrite
Remediation: 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.

X-Content-Type-Options Header Missing
Risk Level: Low
URL: https://public-firing-range.appspot.com/address/URL/documentwrite
Remediation: 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.

X-Content-Type-Options Header Missing
Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location/setTimeout
Remediation: 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.

X-Content-Type-Options Header Missing
Risk Level: Low
URL: https://public-firing-range.appspot.com/address/location.hash/rangeCreateContextualFragment
Remediation: 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.

X-Content-Type-Options Header Missing

Risk Level: Low

URL: https://public-firing-range.appspot.com/address/location/innerHtml

Remediation: 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.

X-Content-Type-Options Header Missing

Risk Level: Low

URL: https://public-firing-range.appspot.com/address/baseURI/documentwrite

Remediation: 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.

X-Content-Type-Options Header Missing

Risk Level: Low

URL: https://public-firing-range.appspot.com/address/location/documentwrite

Remediation: 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.

X-Content-Type-Options Header Missing

Risk Level: Low

URL: https://public-firing-range.appspot.com/address/location/eval

Remediation: 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.

X-Content-Type-Options Header Missing

Risk Level: Low

URL: https://public-firing-range.appspot.com/redirect/meta?q=/

Remediation: 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.

X-Content-Type-Options Header Missing

Risk Level: Low

URL: https://public-firing-range.appspot.com/address/location/documentwriteln

Remediation: 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.

Session Management Response Identified

Risk Level: Informational

URL: https://public-firing-range.appspot.com/leakedcookie/leakedinresource

Remediation: This is an informational alert rather than a vulnerability and so there is nothing to fix.

X-Content-Type-Options Header Missing

Risk Level: Low

URL: https://public-firing-range.appspot.com/address/location/replace

Remediation: 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.

X-Content-Type-Options Header Missing

Risk Level: Low

URL: https://public-firing-range.appspot.com/address/location/rangeCreateContextualFragment

Remediation: 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.

Session Management Response Identified

Risk Level: Informational

URL: https://public-firing-range.appspot.com/leakedcookie/leakedinresource

Remediation: This is an informational alert rather than a vulnerability and so there is nothing to fix.

Strict-Transport-Security Header Not Set

Risk Level: Low

URL: https://public-firing-range.appspot.com/leakedcookie/leakedcookie

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Missing Anti-clickjacking Header

Risk Level: Medium

URL: https://public-firing-range.appspot.com/leakedcookie/leakedinresource

Remediation: 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.

X-Content-Type-Options Header Missing

Risk Level: Low

URL: https://public-firing-range.appspot.com/leakedcookie/leakedcookie

Remediation: 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.

Strict-Transport-Security Header Not Set

Risk Level: Low

URL: https://public-firing-range.appspot.com/leakedcookie/leakedcookie.js

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Content Security Policy (CSP) Header Not Set

Risk Level: Medium

URL: https://public-firing-range.appspot.com/leakedcookie/leakedinresource

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/leakedcookie/leakedcookie.js
Remediation: 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.

Cookie without SameSite Attribute

Risk Level: Low
URL: https://public-firing-range.appspot.com/leakedcookie/leakedinresource
Remediation: Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Cookie Without Secure Flag

Risk Level: Low
URL: https://public-firing-range.appspot.com/leakedcookie/leakedinresource
Remediation: Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

Modern Web Application

Risk Level: Informational
URL: https://public-firing-range.appspot.com/leakedcookie/leakedinresource
Remediation: This is an informational alert and so no changes are required.

Strict-Transport-Security Header Not Set

Risk Level: Low
URL: https://public-firing-range.appspot.com/leakedcookie/leakedinresource
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

X-Content-Type-Options Header Missing

Risk Level: Low
URL: https://public-firing-range.appspot.com/leakedcookie/leakedinresource
Remediation: 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.

Test Vulnerability

Risk Level: Low
URL: https://public-firing-range.appspot.com/
Remediation: This is a test vulnerability added to verify the results display is working.