Valnara Security Scan Report

Scan Details:

Target URL: https://demo.testfire.net/
Scan Type: Passive Scan
Scan Depth: 5
Start Time: 2025-04-13 13:08:11
End Time: 2025-04-13 13:08:19

Risk Summary:

Medium Risk Vulnerabilities: 72
Low Risk Vulnerabilities: 132
Informational Risk Vulnerabilities: 41

Detailed Vulnerabilities:

Session Management Response Identified
Risk Level: Informational
URL: https://demo.testfire.net/
Remediation: This is an informational alert rather than a vulnerability and so there is nothing to fix.

Missing Anti-clickjacking Header
Risk Level: Medium
URL: https://demo.testfire.net/
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://demo.testfire.net/
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://demo.testfire.net/
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Cookie without SameSite Attribute
Risk Level: Low

URL: https://demo.testfire.net/
Remediation: Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Strict-Transport-Security Header Not Set
Risk Level: Low
URL: https://demo.testfire.net/
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://demo.testfire.net/
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://demo.testfire.net/sitemap.xml
Remediation: This is an informational alert rather than a vulnerability and so there is nothing to fix.

Session Management Response Identified
Risk Level: Informational
URL: https://demo.testfire.net/
Remediation: This is an informational alert rather than a vulnerability and so there is nothing to fix.

Session Management Response Identified
Risk Level: Informational
URL: https://demo.testfire.net/robots.txt
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://demo.testfire.net/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://demo.testfire.net/index.jsp?content=personal_checking.htm
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://demo.testfire.net/index.jsp?content=business_deposit.htm
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://demo.testfire.net/index.jsp?content=inside_contact.htm
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://demo.testfire.net/robots.txt
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Cookie without SameSite Attribute
Risk Level: Low
URL: https://demo.testfire.net/sitemap.xml
Remediation: Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Cookie without SameSite Attribute
Risk Level: Low
URL: https://demo.testfire.net/robots.txt
Remediation: Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/sitemap.xml
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Strict-Transport-Security Header Not Set
Risk Level: Low
URL: https://demo.testfire.net/sitemap.xml
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/robots.txt
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Strict-Transport-Security Header Not Set
Risk Level: Low

URL: https://demo.testfire.net/robots.txt
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://demo.testfire.net/index.jsp?content=business_retirement.htm
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://demo.testfire.net/index.jsp?content=personal_cards.htm
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://demo.testfire.net/
Remediation: This is an informational alert rather than a vulnerability and so there is nothing to fix.

Missing Anti-clickjacking Header
Risk Level: Medium
URL: https://demo.testfire.net/index.jsp?content=personal_other.htm
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://demo.testfire.net/index.jsp?content=inside_investor.htm
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://demo.testfire.net/index.jsp?content=business_deposit.htm
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://demo.testfire.net/index.jsp?content=personal.htm
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://demo.testfire.net/index.jsp?content=business_other.htm
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://demo.testfire.net/index.jsp?content=business_deposit.htm
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://demo.testfire.net/feedback.jsp
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://demo.testfire.net/index.jsp?content=personal_deposit.htm
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://demo.testfire.net/index.jsp?content=personal_checking.htm
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://demo.testfire.net/index.jsp?content=inside_about.htm

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.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=business_deposit.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Content Security Policy (CSP) Header Not Set
Risk Level: Medium
URL: https://demo.testfire.net/index.jsp?content=personal_checking.htm
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://demo.testfire.net/index.jsp?content=personal_loans.htm
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://demo.testfire.net/index.jsp
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://demo.testfire.net/index.jsp?content=business_deposit.htm
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://demo.testfire.net/login.jsp
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://demo.testfire.net/index.jsp?content=inside_contact.htm
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://demo.testfire.net/index.jsp?content=business_retirement.htm
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://demo.testfire.net/index.jsp?content=business_deposit.htm
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://demo.testfire.net/index.jsp?content=inside_contact.htm
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://demo.testfire.net/index.jsp?content=business_retirement.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=personal_checking.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Re-examine Cache-control Directives
Risk Level: Informational
URL: https://demo.testfire.net/index.jsp?content=personal.htm
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://demo.testfire.net/index.jsp?content=inside_about.htm
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://demo.testfire.net/index.jsp?content=personal_cards.htm
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://demo.testfire.net/feedback.jsp
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://demo.testfire.net/index.jsp?content=personal_deposit.htm
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://demo.testfire.net/index.jsp?content=personal_loans.htm
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://demo.testfire.net/survey_questions.jsp
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://demo.testfire.net/index.jsp?content=business_other.htm
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://demo.testfire.net/login.jsp
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://demo.testfire.net/index.jsp?content=personal_other.htm

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://demo.testfire.net/index.jsp?content=inside_investor.htm
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".

Secure Pages Include Mixed Content
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=inside_contact.htm
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.

Re-examine Cache-control Directives
Risk Level: Informational
URL: https://demo.testfire.net/index.jsp
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://demo.testfire.net/index.jsp?content=personal_checking.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=business_retirement.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Content Security Policy (CSP) Header Not Set
Risk Level: Medium
URL: https://demo.testfire.net/index.jsp
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://demo.testfire.net/feedback.jsp
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://demo.testfire.net/index.jsp?content=personal_cards.htm

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://demo.testfire.net/index.jsp?content=inside_about.htm
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://demo.testfire.net/index.jsp?content=personal.htm
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://demo.testfire.net/index.jsp?content=inside_investor.htm
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://demo.testfire.net/index.jsp?content=personal_other.htm
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://demo.testfire.net/login.jsp
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://demo.testfire.net/index.jsp?content=personal_loans.htm
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://demo.testfire.net/index.jsp?content=business_other.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=inside_contact.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Content Security Policy (CSP) Header Not Set
Risk Level: Medium
URL: https://demo.testfire.net/index.jsp?content=personal_deposit.htm

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://demo.testfire.net/survey_questions.jsp
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://demo.testfire.net/index.jsp?content=business_retirement.htm
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://demo.testfire.net/index.jsp?content=personal_checking.htm
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.

Absence of Anti-CSRF Tokens

Risk Level: Medium
URL: https://demo.testfire.net/feedback.jsp
Remediation: Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

Server Leaks Version Information via "Server" HTTP Response Header Field

Risk Level: Low
URL: https://demo.testfire.net/index.jsp
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Server Leaks Version Information via "Server" HTTP Response Header Field

Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=personal_cards.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=inside_about.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Absence of Anti-CSRF Tokens
Risk Level: Medium
URL: https://demo.testfire.net/login.jsp
Remediation: Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

Strict-Transport-Security Header Not Set
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=inside_contact.htm
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://demo.testfire.net/index.jsp?content=personal_other.htm
Remediation: This is an informational alert and so no changes are required.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=personal.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=business_other.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Content Security Policy (CSP) Header Not Set
Risk Level: Medium
URL: https://demo.testfire.net/survey_questions.jsp
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Server Leaks Version Information via "Server" HTTP Response Header Field

Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=personal_loans.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=inside_investor.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=personal_deposit.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

X-Content-Type-Options Header Missing
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=business_retirement.htm
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://demo.testfire.net/index.jsp?content=business_cards.htm
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://demo.testfire.net/index.jsp
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://demo.testfire.net/index.jsp?content=business_insurance.htm
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.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/feedback.jsp

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Strict-Transport-Security Header Not Set
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=personal_cards.htm
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://demo.testfire.net/index.jsp?content=inside_about.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=personal_other.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Information Disclosure - Suspicious Comments
Risk Level: Informational
URL: https://demo.testfire.net/login.jsp
Remediation: Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.

Strict-Transport-Security Header Not Set
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=personal.htm
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://demo.testfire.net/index.jsp?content=business_other.htm
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://demo.testfire.net/index.jsp?content=inside_contact.htm
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://demo.testfire.net/index.jsp?content=personal_loans.htm
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://demo.testfire.net/index.jsp?content=inside_investor.htm
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://demo.testfire.net/index.jsp?content=personal_deposit.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Re-examine Cache-control Directives
Risk Level: Informational
URL: https://demo.testfire.net/index.jsp?content=business_cards.htm
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://demo.testfire.net/index.jsp?content=inside.htm
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.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/survey_questions.jsp
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

X-Content-Type-Options Header Missing
Risk Level: Low
URL: https://demo.testfire.net/index.jsp
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://demo.testfire.net/feedback.jsp
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://demo.testfire.net/index.jsp?content=inside_about.htm
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://demo.testfire.net/index.jsp?content=personal_cards.htm
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://demo.testfire.net/index.jsp?content=business_insurance.htm
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://demo.testfire.net/index.jsp?content=personal_other.htm
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://demo.testfire.net/index.jsp?content=business_other.htm
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://demo.testfire.net/index.jsp?content=personal.htm
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.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/login.jsp
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Missing Anti-clickjacking Header
Risk Level: Medium
URL: https://demo.testfire.net/status_check.jsp
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://demo.testfire.net/index.jsp?content=business_cards.htm
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://demo.testfire.net/survey_questions.jsp
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://demo.testfire.net/index.jsp?content=personal_loans.htm
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://demo.testfire.net/index.jsp?content=personal_deposit.htm
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://demo.testfire.net/index.jsp?content=inside_investor.htm
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://demo.testfire.net/index.jsp?content=inside.htm
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://demo.testfire.net/cgi.exe
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://demo.testfire.net/index.jsp?content=business_insurance.htm

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://demo.testfire.net/feedback.jsp
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://demo.testfire.net/index.jsp?content=personal_savings.htm
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://demo.testfire.net/default.jsp?content=security.htm
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://demo.testfire.net/index.jsp?content=personal_other.htm
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://demo.testfire.net/login.jsp
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://demo.testfire.net/index.jsp?content=personal_investments.htm
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://demo.testfire.net/subscribe.jsp

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://demo.testfire.net/status_check.jsp
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://demo.testfire.net/survey_questions.jsp
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://demo.testfire.net/index.jsp?content=inside_careers.htm
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://demo.testfire.net/index.jsp?content=inside.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Server Leaks Version Information via "Server" HTTP Response Header Field

Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=business_cards.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Missing Anti-clickjacking Header

Risk Level: Medium
URL: https://demo.testfire.net/index.jsp?content=business_lending.htm
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://demo.testfire.net/index.jsp?content=privacy.htm
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.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/cgi.exe
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=business_insurance.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Missing Anti-clickjacking Header
Risk Level: Medium
URL: https://demo.testfire.net/index.jsp?content=inside_press.htm
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://demo.testfire.net/index.jsp?content=personal_savings.htm
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".

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/default.jsp?content=security.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Missing Anti-clickjacking Header
Risk Level: Medium
URL: https://demo.testfire.net/index.jsp?content=business.htm
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://demo.testfire.net/login.jsp

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://demo.testfire.net/status_check.jsp
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://demo.testfire.net/index.jsp?content=personal_investments.htm
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://demo.testfire.net/subscribe.jsp
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://demo.testfire.net/swagger/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://demo.testfire.net/index.jsp?content=business_cards.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Re-examine Cache-control Directives

Risk Level: Informational
URL: https://demo.testfire.net/index.jsp?content=inside_careers.htm
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".

Modern Web Application

Risk Level: Informational
URL: https://demo.testfire.net/index.jsp?content=inside.htm
Remediation: This is an informational alert and so no changes are required.

Re-examine Cache-control Directives

Risk Level: Informational
URL: https://demo.testfire.net/index.jsp?content=business_lending.htm
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://demo.testfire.net/index.jsp?content=privacy.htm
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://demo.testfire.net/cgi.exe
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://demo.testfire.net/index.jsp?content=business_insurance.htm
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://demo.testfire.net/index.jsp?content=personal_savings.htm
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://demo.testfire.net/default.jsp?content=security.htm
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://demo.testfire.net/subscribe.jsp
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://demo.testfire.net/index.jsp?content=inside_press.htm
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://demo.testfire.net/index.jsp?content=business.htm

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://demo.testfire.net/index.jsp?content=personal_investments.htm
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://demo.testfire.net/index.jsp?content=security.htm
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.

Server Leaks Version Information via "Server" HTTP Response Header Field

Risk Level: Low
URL: https://demo.testfire.net/status_check.jsp
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Re-examine Cache-control Directives

Risk Level: Informational
URL: https://demo.testfire.net/swagger/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://demo.testfire.net/index.jsp?content=inside_careers.htm
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://demo.testfire.net/index.jsp?content=business_cards.htm
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://demo.testfire.net/index.jsp?content=privacy.htm
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://demo.testfire.net/index.jsp?content=business_lending.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=inside.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

X-Content-Type-Options Header Missing
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=business_insurance.htm
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.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/images/header_pic.jpg
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/images/home1.jpg
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=personal_savings.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Absence of Anti-CSRF Tokens
Risk Level: Medium
URL: https://demo.testfire.net/subscribe.jsp
Remediation: Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate

functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

Content Security Policy (CSP) Header Not Set
Risk Level: Medium
URL: https://demo.testfire.net/index.jsp?content=inside_press.htm
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://demo.testfire.net/index.jsp?content=business.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Cross-Domain JavaScript Source File Inclusion
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=personal_investments.htm
Remediation: Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

Strict-Transport-Security Header Not Set
Risk Level: Low
URL: https://demo.testfire.net/status_check.jsp
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://demo.testfire.net/swagger/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://demo.testfire.net/index.jsp?content=security.htm
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://demo.testfire.net/index.jsp?content=inside.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=inside_careers.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=business_lending.htm

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=privacy.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/images/home2.jpg
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Strict-Transport-Security Header Not Set
Risk Level: Low
URL: https://demo.testfire.net/images/header_pic.jpg
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://demo.testfire.net/index.jsp?content=personal_savings.htm
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://demo.testfire.net/images/home1.jpg
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://demo.testfire.net/search.jsp?query=ZAP
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.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/subscribe.jsp
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Secure Pages Include Mixed Content (Including Scripts)
Risk Level: Medium
URL: https://demo.testfire.net/index.jsp?content=personal_investments.htm
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://demo.testfire.net/status_check.jsp
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.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=inside_press.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=business.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Modern Web Application
Risk Level: Informational
URL: https://demo.testfire.net/swagger/index.html
Remediation: This is an informational alert and so no changes are required.

Content Security Policy (CSP) Header Not Set
Risk Level: Medium
URL: https://demo.testfire.net/index.jsp?content=security.htm
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://demo.testfire.net/index.jsp?content=inside_careers.htm
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://demo.testfire.net/index.jsp?content=business_lending.htm
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://demo.testfire.net/images/home2.jpg
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://demo.testfire.net/index.jsp?content=privacy.htm

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://demo.testfire.net/index.jsp?content=inside.htm
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://demo.testfire.net/images/header_pic.jpg
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://demo.testfire.net/images/home1.jpg
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://demo.testfire.net/index.jsp?content=personal_savings.htm
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://demo.testfire.net/subscribe.jsp
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Re-examine Cache-control Directives
Risk Level: Informational
URL: https://demo.testfire.net/search.jsp?query=ZAP
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".

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=personal_investments.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/swagger/index.html
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Strict-Transport-Security Header Not Set
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=inside_press.htm
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://demo.testfire.net/index.jsp?content=business.htm
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://demo.testfire.net/images/home2.jpg
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://demo.testfire.net/index.jsp?content=business_lending.htm
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://demo.testfire.net/index.jsp?content=inside_careers.htm
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.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/doLogin
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/style.css

Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=security.htm
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

X-Content-Type-Options Header Missing
Risk Level: Low
URL: https://demo.testfire.net/index.jsp?content=privacy.htm
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.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/images/logo.gif
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Content Security Policy (CSP) Header Not Set
Risk Level: Medium
URL: https://demo.testfire.net/search.jsp?query=ZAP
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/images/pf_lock.gif
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

X-Content-Type-Options Header Missing
Risk Level: Low
URL: https://demo.testfire.net/subscribe.jsp
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.

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/images/home3.jpg
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Strict-Transport-Security Header Not Set
Risk Level: Low
URL: https://demo.testfire.net/swagger/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://demo.testfire.net/index.jsp?content=personal_investments.htm
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://demo.testfire.net/index.jsp?content=inside_press.htm
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://demo.testfire.net/index.jsp?content=business.htm
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://demo.testfire.net/style.css
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://demo.testfire.net/index.jsp?content=security.htm
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://demo.testfire.net/images/logo.gif
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://demo.testfire.net/images/pf_lock.gif
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://demo.testfire.net/images/home3.jpg

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

Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level: Low
URL: https://demo.testfire.net/search.jsp?query=ZAP
Remediation: Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

X-Content-Type-Options Header Missing
Risk Level: Low
URL: https://demo.testfire.net/swagger/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://demo.testfire.net/index.jsp?content=personal_investments.htm
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://demo.testfire.net/style.css
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://demo.testfire.net/index.jsp?content=security.htm
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://demo.testfire.net/images/logo.gif
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://demo.testfire.net/images/pf_lock.gif

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://demo.testfire.net/search.jsp?query=ZAP
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://demo.testfire.net/images/home3.jpg
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://demo.testfire.net/search.jsp?query=ZAP
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://demo.testfire.net/
Remediation: This is a test vulnerability added to verify the results display is working.