Security Scan Combined Report

Executive Summary

Scan Start Time:	2024-12-17 21:13:06
Scan End Time:	2024-12-17 21:13:30
Total Scan Duration:	24.05 seconds
Total URLs Scanned:	1
High Severity Vulnerabilities:	0
Medium Severity Vulnerabilities:	176
Low Severity Vulnerabilities:	264

Detailed Scan Results

Target URL: http://vulnweb.com

Scan Duration:	24.05 seconds
URLs Crawled:	4
Attack Performed:	True
Attack Type:	All Attacks

High Severity Findings:	0
Medium Severity Findings:	176
Low Severity Findings:	264

Crawled URLs:

#	URL
1	http://vulnweb.com
2	http://vulnweb.com/acunetix-logo.png
3	http://vulnweb.com/sitemap.xml
4	http://vulnweb.com/robots.txt

Detected Vulnerabilities:

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing

Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set

Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

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

Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.

Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.

Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.

Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.

Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.

Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.

Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.

Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.

Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.

Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.

Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.

Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.

Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.

Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.

Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low

Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low
Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Missing Anti-clickjacking Header
Risk Level:	Medium
Description:	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	Content Security Policy (CSP) Header Not Set
Risk Level:	Medium

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A

Name:	Server Leaks Version Information via "Server" HTTP Response Header Field
Risk Level:	Low
Description:	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Solution:	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Affected URL:	N/A

Name:	X-Content-Type-Options Header Missing
Risk Level:	Low

Description:	The Anti-MIME-Sniffing header X-Content-Type- Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Solution:	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.
Affected URL:	N/A