Security Scan Combined Report

Executive Summary

Scan Start Time:	2025-01-26 13:50:26
Scan End Time:	2025-01-26 13:51:57
Total Scan Duration:	89.95 seconds
Total URLs Scanned:	1
High Severity Vulnerabilities:	0
Medium Severity Vulnerabilities:	311
Low Severity Vulnerabilities:	1275

Detailed Scan Results

Target URL: https://chatgpt.com

Scan Duration:	89.95 seconds
URLs Crawled:	107
Attack Performed:	True
Attack Type:	All Attacks

High Severity Findings:	0
Medium Severity Findings:	311
Low Severity Findings:	1275

Crawled URLs:

#	URL
1	https://chatgpt.com/search$
2	https://chatgpt.com/share/178a557a-2fbd- 42af-9372-f136a021fb1e
3	https://chatgpt.com/shared-convos- sitemap.xml
4	https://chatgpt.com/share/820beb5d-bc69- 4920-bd47-fa2f435eeacf
5	https://chatgpt.com/share/ff3ca611-6076- 43c0-bd6c-3ed4c59620b1
6	https://chatgpt.com/sitemap.xml
7	https://chatgpt.com/share/29521a13-f504- 4a04-9aee-98f8d0765061
8	https://chatgpt.com/backend- anon/conversation$
9	https://chatgpt.com/share/9e7cd489-dae1- 4cc2-a759-7909f9c357fd
10	https://chatgpt.com/share/6703a341-184a- 49e8-8fd9-72da8b05d945
11	https://chatgpt.com/share/b4db8af6-d6c7- 4aa0-9533-f1a76416aeee

12	https://chatgpt.com/share/82ee15ea-66f1- 4de3-8abf-cf38fab7a581
13	https://chatgpt.com/
14	https://chatgpt.com/share/18621ffa-118b- 4947-92aa-f7653099e23a
15	https://chatgpt.com/share/6326fccf-2f48- 4bc4-ae10-35cd79b4b64e
16	https://chatgpt.com/share/c03b4298-dd7d- 4d3f-9d5d-8e1b70a0dcf7
17	https://chatgpt.com/backend-anon/
18	https://chatgpt.com/share/eb07b5c8-d10e- 4513-aae5-216e721f639e
19	https://chatgpt.com/g/
20	https://chatgpt.com/share/c4174d42-102a- 4845-83fd-e45dda1bef8f
21	https://chatgpt.com/share/74b2b80f-4681- 4cac-8404-c0e3e8e05e6a
22	https://chatgpt.com/share/0f774b12-db06- 48d8-b690-f3a1f2dd9fc8
23	https://chatgpt.com/share/e9920a58-7676- 4dc7-a961-447d95939298
24	https://chatgpt.com
25	https://chatgpt.com/robots.txt
26	https://chatgpt.com/share/da27a0b5-65f7- 4251-915f-a262263ef988
27	https://chatgpt.com/share/3ab3cba1-4112- 491b-9169-1f10c7056ec0
28	https://chatgpt.com/share/1804fb1c-ac21- 4b98-8faa-160c0789364f

29	https://chatgpt.com/share/bf7af7fa-0c11- 4489-8696-2822a4b39775
30	https://chatgpt.com/share/15db4bfb-58cf- 4a3c-a58c-0ff826dc757b
31	https://chatgpt.com/share/b4e40b1e-98aa- 493f-923a-f1006c6a12cd
32	https://chatgpt.com/share/840c4ef6-e33f- 4d42-b7fc-a11b10fb5f62
33	https://chatgpt.com/share/bb0c3537-bfd8- 4b6b-8a0e-5a7f1336365f
34	https://chatgpt.com/share/78b63b42-6ed7- 46ff-ab05-16845a39c98d
35	https://chatgpt.com/share/cbd31ba4-75a4- 4283-96b2-aa2a19c4e02b
36	https://chatgpt.com/auth/logout
37	https://chatgpt.com/share/c314aa1a-c678- 4ef1-b868-f54d20cb4fec
38	https://chatgpt.com/share/87d3a5df- cab4-4c9b-adad-e94a0ecb5964
39	https://chatgpt.com/share/57f795d0-609f- 4c9f-830a-ae7228f470fd
40	https://chatgpt.com/share/1caefae6-5d3a- 4932-b59a-4c5d21de0747
41	https://chatgpt.com/$
42	https://chatgpt.com/share/b1ec7b00-3ee0- 4819-8ad3-2947c1f6cac9
43	https://chatgpt.com/share/39a2bdcf-6951- 4403-9b38-03f46eb02601
44	https://chatgpt.com/share/86f4531e-7175- 4edf-971b-7333440bf2fb
45	https://chatgpt.com/share/d97714a8-50ff- 4875-b1a5-594f892957f5

46	https://chatgpt.com/share/6877d667-aa55- 43c8-971b-f080ecba7856
47	https://chatgpt.com/share/3ae9227a-5f85- 4516-af41-ea30ecc6b72e
48	https://chatgpt.com/share/8e092129-201b- 4eba-9010-585c1c9b18ee
49	https://chatgpt.com/share/d0795192-1068- 466b-afa7-80c450eb4ef0
50	https://chatgpt.com/share/509f963e-83c6- 40ff-9e9f-d44d7cb45358
51	https://chatgpt.com/share/0651c30f-ca81- 42d1-9390-532bfa4ad52c
52	https://chatgpt.com/share/f814afa5-a9e6- 4a82-b016-71d7d7af15c6
53	https://chatgpt.com/public-api/
54	https://chatgpt.com/share/2e09e44d-76a2- 47fb-8391-b04d1bc36008
55	https://chatgpt.com/share/7c025ade-a90a- 42cf-aaa8-cd47eda7c036
56	https://chatgpt.com/share/97cb4979-6393- 4a7b-9910-44e2bfa69401
57	https://chatgpt.com/share/dadd4e69-aabb- 4081-bb30-5c82479150ea
58	https://chatgpt.com/share/bb083213-e0fd- 4491-a82a-738be2ae76c4
59	https://chatgpt.com/share/9e52dd18-d1c0- 4872-b4ec-fe9448bd83f4
60	https://chatgpt.com/share/f0d00336-9535- 42cf-82c2-d54ae5dfe082
61	https://chatgpt.com/images/
62	https://chatgpt.com/share/64bb6a74-9357- 4ac2-a7ae-a26d2d206627

63	https://chatgpt.com/share/2c03942d-c42a- 43dc-9bec-04064fed5c21
64	https://chatgpt.com/share/9e446a95-8e47- 4c40-8d63-dd016d7c66f4
65	https://chatgpt.com/share/77f6237f-6bf8- 4e8e-8648-be34ccdcc52d
66	https://chatgpt.com/share/212c4130-96cb- 4217-91fd-08eb4380405f
67	https://chatgpt.com/share/f556a7c2-73db- 4c0b-b784-ac6ee09a3db6
68	https://chatgpt.com/share/ddd27ba7-50de- 48d1-ac0c-51bf794c4025
69	https://chatgpt.com/share/d3040658-12ed- 41fc-87f4-fec8a70c3344
70	https://chatgpt.com/share/a6fa9f47-c411- 46f6-8f8b-12f2930fa710
71	https://chatgpt.com/share/2f43a3b3-33f2- 42d7-b89b-63a86c4a155b
72	https://chatgpt.com/share/91fcc4d0-ebc4- 44d0-8fce-6c1167dfd46f
73	https://chatgpt.com/share/6c675e7c-61ed- 4202-a570-95c31a3e67f3
74	https://chatgpt.com/auth/login
75	https://chatgpt.com/share/6572c20a-aa76- 475b-bbea-d0af6c23ffc1
76	https://chatgpt.com/share/b3c31a0d-7314- 47c0-b194-313366d90131
77	https://chatgpt.com/share/fad4fb79-a7d8- 45f0-b28d-decd3f5bff55
78	https://chatgpt.com/share/2e0c7813-d324- 445e-a09e-12379123704e
79	https://chatgpt.com/share/16e2a811-2ffe- 412c-b730-b055e059254c

80	https://chatgpt.com/share/e799c12f-0865- 406f-9000-4523fd09a478
81	https://chatgpt.com/share/c2cfc5c4-4648- 4b54-8330-35597c960379
82	https://chatgpt.com/share/31265a1c-94ad- 42f4-bef5-daca31be3b8c
83	https://chatgpt.com/backend- anon/sentinel/
84	https://chatgpt.com/share/011b8169-b122- 45d9-9e94-ac14af26f424
85	https://chatgpt.com/share/033f2231-fa10- 4c48-885c-990f54ba17fa
86	https://chatgpt.com/auth/
87	https://chatgpt.com/share/afda7698-c915- 427c-8f52-020b1cb4988b
88	https://chatgpt.com/share/0cf558a8-2708- 4d7a-92ea-26a875124d65
89	https://chatgpt.com/share/1ed652e9-e8a7- 4430-b89f-96fe3a2fb0f7
90	https://chatgpt.com/share/ed2c604f-0153- 4d42-9838-d8fe56522a60
91	https://chatgpt.com/share/2d1c7db0-cf56- 4d36-888d-a1d01d795aa6
92	https://chatgpt.com/share/da70d36e-fe5b- 4fe6-bc84-e3277949b864
93	https://chatgpt.com/share/09b22266-67fd- 4edd-b03a-cb438d633362
94	https://chatgpt.com/share/2e0f975c-8f7b- 412c-b483-03cfa2beff44
95	https://chatgpt.com/share/08389979-70b7- 4626-b639-c23c04829be5
96	https://chatgpt.com/share/df043e41-d7c2- 4f7e-a513-27bdc65749ae

97	https://chatgpt.com/share/
98	https://chatgpt.com/share/af8f48bb-6ddf- 4c75-9310-37058180b1ef
99	https://chatgpt.com/gpts$
100	https://chatgpt.com/share/17313117-1968- 425f-86b3-a0d1192012f3
101	https://chatgpt.com/share/9fb6737a-7f30- 4fa0-b170-70127ae77ffc
102	https://chatgpt.com/share/ebf3c33e-3c91- 49e3-8f41-9e2977115d92
103	https://chatgpt.com/share/00ba92ea- ecf1-451d-b8db-783303ebee10
104	https://chatgpt.com/api/share/og/
105	https://chatgpt.com/share/6f6ddd82-7a90- 477d-8f96-3e59c5ef1352
106	https://chatgpt.com/share/eedeae77-348c- 420c-9cbb-f684672a7c7d
107	https://chatgpt.com/share/107078ad-9a69- 4623-9834-a33546e5e9c7

Detected Vulnerabilities:

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives

Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.

Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified

Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.

Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified

Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.

Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified

Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.

Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified

Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.

Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified

Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.

Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified

Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.

Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified

Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.

Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified

Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.

Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified

Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.

Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified

Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.

Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified

Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.

Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified

Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.

Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified

Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.

Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified

Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.

Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified

Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational

Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".

Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low

Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low

Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives

Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low

Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low

Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives

Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational

Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".

Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low

Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low

Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives

Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational

Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".

Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low

Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low

Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives

Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational

Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".

Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low

Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low

Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives

Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive

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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag

Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low

Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low

Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational

Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive

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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag

Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low

Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low

Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational

Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive

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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag

Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low

Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low

Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational

Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive

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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag

Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low

Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low

Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational

Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive

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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag

Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low

Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low

Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational

Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational

Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational

Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified

Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational

Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational

Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational

Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.

Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low

Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational

Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low

Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational

Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low

Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational

Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational

Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	Re-examine Cache-control Directives
Risk Level:	Informational
Description:	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Solution:	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low
Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None

Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Retrieved from Cache
Risk Level:	Informational
Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal or user- specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution:	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Session Management Response Identified
Risk Level:	Informational
Description:	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Solution:	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments

Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Notices
Risk Level:	Low
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: Wildcard Directive
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	CSP: style-src unsafe-inline
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 (but not limited to) 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 properly configured to set the Content-Security-Policy header.
Affected URL:	N/A

Name:	Cookie No HttpOnly Flag
Risk Level:	Low

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Solution:	Ensure that the HttpOnly flag is set for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Affected URL:	N/A

Name:	Cookie with SameSite Attribute None
Risk Level:	Low
Description:	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Affected URL:	N/A

Name:	Cookie Without Secure Flag
Risk Level:	Low
Description:	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Solution:	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix

Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low

Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Information Disclosure - Suspicious Comments
Risk Level:	Informational
Description:	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
Solution:	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Modern Web Application
Risk Level:	Informational
Description:	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Solution:	This is an informational alert and so no changes are required.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A