Security Scan Combined Report

Executive Summary

Scan Start Time:	2025-01-29 11:15:54
Scan End Time:	2025-01-29 11:16:32
Total Scan Duration:	38.27 seconds
Total URLs Scanned:	1
High Severity Vulnerabilities:	0
Medium Severity Vulnerabilities:	0
Low Severity Vulnerabilities:	1100

Detailed Scan Results

Target URL: https://coursera.org

Scan Duration:	38.27 seconds
URLs Crawled:	3
Attack Performed:	True
Attack Type:	All Attacks

High Severity Findings:	0
Medium Severity Findings:	0
Low Severity Findings:	1100

Crawled URLs:

#	URL
1	https://coursera.org
2	https://coursera.org/sitemap.xml
3	https://coursera.org/robots.txt

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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

Name:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 without SameSite Attribute
Risk Level:	Low

Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually 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:	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 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 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 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 without SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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 SameSite Attribute
Risk Level:	Low
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing 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:	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:	Timestamp Disclosure - Unix
Risk Level:	Low
Description:	A timestamp was disclosed by the application/web server. - Unix
Solution:	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Affected URL:	N/A

Name:	Timestamp Disclosure - Unix

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

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