

## **Summary of Alerts**

Risk Level	Number of Alerts
<u>High</u>	2
Medium	2
Low	9
Informational	0

## **Alert Detail**

High (Medium)	SQL Injection
Description	SQL injection may be possible.
URL	https://csye6225-fall2018-chandwanid.me//transaction/8a8080cd67512ea401675137df450000/attachments?query=query%27+AND+%271%27%3D%271%27++
Metho d	POST
Para meter	query
Attack	query' OR '1'='1'
URL	https://csye6225-fall2018-chandwanid.me/transaction/8a8080cd67512ea401675137df450000?query=query%27+AND+%271%27%3D%271%27++
Metho d	GET
Para meter	query
Attack	query' AND '1'='1'
Instances	2
Solution	Do not trust client side input, even if there is client side validation in place.  In general, type check all data on the server side.  If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?'

If database Stored Procedures can be used, use them.  Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality!  Do not create dynamic SQL queries using simple string concatenation.  Escape all data received from the client.  Apply a 'whitelist' of allowed characters, or a 'blacklist' of disallowed characters in user input.  Apply the principle of least privilege by using the least privileged database user possible.  In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact.  Grant the minimum database access that is necessary for the application.  The page results were successfully manipulated using the boolean conditions [query' AND '1'='1' ] and [query' OR '1'='1' ]  The parameter value being modified was stripped from the HTML output for the purposes of the comparison  Data was NOT returned for the original parameter.
'exec immediate', or equivalent functionality!  Do not create dynamic SQL queries using simple string concatenation.  Escape all data received from the client.  Apply a 'whitelist' of allowed characters, or a 'blacklist' of disallowed characters in user input.  Apply the principle of least privilege by using the least privileged database user possible.  In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact.  Grant the minimum database access that is necessary for the application.  The page results were successfully manipulated using the boolean conditions [query' AND '1'='1' ] and [query' OR '1'='1' ]  The parameter value being modified was stripped from the HTML output for the purposes of the comparison
Escape all data received from the client.  Apply a 'whitelist' of allowed characters, or a 'blacklist' of disallowed characters in user input.  Apply the principle of least privilege by using the least privileged database user possible.  In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact.  Grant the minimum database access that is necessary for the application.  The page results were successfully manipulated using the boolean conditions [query' AND '1'='1' ] and [query' OR '1'='1' ]  The parameter value being modified was stripped from the HTML output for the purposes of the comparison
Apply a 'whitelist' of allowed characters, or a 'blacklist' of disallowed characters in user input.  Apply the principle of least privilege by using the least privileged database user possible.  In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact.  Grant the minimum database access that is necessary for the application.  The page results were successfully manipulated using the boolean conditions [query' AND '1'='1' ] and [query' OR '1'='1' ]  The parameter value being modified was stripped from the HTML output for the purposes of the comparison
Apply the principle of least privilege by using the least privileged database user possible.  In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact.  Grant the minimum database access that is necessary for the application.  The page results were successfully manipulated using the boolean conditions [query' AND '1'='1' ] and [query' OR '1'='1' ]  The parameter value being modified was stripped from the HTML output for the purposes of the comparison
In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact.  Grant the minimum database access that is necessary for the application.  The page results were successfully manipulated using the boolean conditions [query' AND '1'='1' ] and [query' OR '1'='1' ]  The parameter value being modified was stripped from the HTML output for the purposes of the comparison
eliminate SQL injection, but minimizes its impact.  Grant the minimum database access that is necessary for the application.  The page results were successfully manipulated using the boolean conditions [query' AND '1'='1' ] and [query' OR '1'='1' ]  The parameter value being modified was stripped from the HTML output for the purposes of the comparison
The page results were successfully manipulated using the boolean conditions [query' AND '1'='1' ] and [query' OR '1'='1' ]  The parameter value being modified was stripped from the HTML output for the purposes of the comparison
[query' AND '1'='1' ] and [query' OR '1'='1' ]  The parameter value being modified was stripped from the HTML output for the purposes of the comparison
Other information purposes of the comparison
Data was NOT returned for the original parameter
Data was 110 Frotanios for the original parameter.
The vulnerability was detected by successfully retrieving more data than originally returned, by manipulating the parameter
https://www.owasp.org/index.php/Top_10_2010-A1
Reference https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet
CWE ld 89
WASC Id 19
Source ID 1
High (Medium) SQL Injection
Description SQL injection may be possible.
https://csye6225-fall2018- URL chandwanid.me/transaction/765764578575758575674?query=query+AND+1% 3D1++
Method GET

Paramete r	query
Attack	query OR 1=1
Instances	1
Solution	Do not trust client side input, even if there is client side validation in place.  In general, type check all data on the server side.  If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?'  If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries.  If database Stored Procedures can be used, use them.  Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality!  Do not create dynamic SQL queries using simple string concatenation.  Escape all data received from the client.  Apply a 'whitelist' of allowed characters, or a 'blacklist' of disallowed characters in user input.  Apply the principle of least privilege by using the least privileged database user possible.  In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact.  Grant the minimum database access that is necessary for the application.
Other information	The page results were successfully manipulated using the boolean conditions [query AND 1=1 ] and [query OR 1=1 ]  The parameter value being modified was stripped from the HTML output for the purposes of the comparison  Data was NOT returned for the original parameter.  The vulnerability was detected by successfully retrieving more data than originally returned, by manipulating the parameter
	https://www.owasp.org/index.php/Top_10_2010-A1
Reference	
	https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet
CWE Id	89
WASC Id	19

Source ID	1
Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	https://csye6225-fall2018-chandwanid.me/transaction
Method	POST
Parameter	X-Frame-Options
URL	https://csye6225-fall2018-chandwanid.me/
Method	GET
Parameter	X-Frame-Options
Instances	2
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).
Reference	http://blogs.msdn.com/b/ie internals/archive/2010/03/30/combating-click jacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15
Source ID	3
Medium (Medium)	Application Error Disclosure
Description	This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.
URL	https://csye6225-fall2018-chandwanid.me//transaction/8a8080cd67512ea401675137df450000/attachment s
Method	POST
Evidenc e	HTTP/1.1 500
Instances	1
Solution	Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.
Reference	

CWE Id	200
WASC Id	13
Source ID	3
Low (Medium)	Incomplete or No Cache-control and Pragma HTTP Header Set
Description	The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.
URL	https://blocklists.settings.services.mozilla.com/v1/blocklist/3/%7Bec8030f7-c20a-464f-9b0e-13a3a9e97384%7D/60.2.0/Firefox/20180905211815/Linux_x86_64-gcc3/en-US/default/Linux%204.18.0-kali2-amd64%20(GTK%203.24.1%2Clibpulse%2012.2.0)/Kali/1.0/1/1/new/
Method	GET
Paramet er	Cache-Control
Instances	1
Solution	Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate; and that the pragma HTTP header is set with no-cache.
Reference	https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
CWE Id	525
WASC Id	13
Source ID	3
Low (Medium)	Incomplete or No Cache-control and Pragma HTTP Header Set
Description	The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.
URL	https://activity-stream-icons.services.mozilla.com/v1/icons.json.br
Method	GET
Paramet er	Cache-Control
Evidenc e	public,max-age=3600
Instances	1
Solution	Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate; and that the pragma HTTP header is set with no-cache.
Reference	$https://www.owasp.org/index.php/Session\_Management\_Cheat\_Sheet\#Web\_Content\_Caching$
CWE Id	525
WASC Id	13

Source ID	3
Low (Medium)	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://activity-stream-icons.services.mozilla.com/v1/icons.json.br
Method	GET
Parameter	X-Content-Type-Options
Instances	1
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.  If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed
	by the web application/web server to not perform MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.  At "High" threshold this scanner will not alert on client or server error responses.
	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx
Reference	https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
Source ID	3
Low (Medium)	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://csye6225-fall2018-chandwanid.me/
Method	GET
Parameter	X-Content-Type-Options

URL	https://csye6225-fall2018-chandwanid.me/user
Method	GET
Parameter	X-Content-Type-Options
URL	https://csye6225-fall2018-chandwanid.me/transaction
Method	POST
Parameter	X-Content-Type-Options
Instances	3
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.  If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.  At "High" threshold this scanner will not alert on client or server error responses.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx
	https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	https://www.owasp.org/index.php/List_of_useful_HTTP_headers  16
CWE Id WASC Id	
	16
WASC Id	16 15
WASC Id Source ID	16 15 3
WASC Id Source ID Low (Medium)	16 15 3  Web Browser XSS Protection Not Enabled  Web Browser XSS Protection is not enabled, or is disabled by the configuration
WASC Id Source ID Low (Medium) Description	16 15 3  Web Browser XSS Protection Not Enabled  Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server  https://csye6225-fall2018-chandwanid.me//transaction/8a8080cd67512ea401675137df450000/attachment
WASC Id Source ID Low (Medium) Description URL	16 15 3  Web Browser XSS Protection Not Enabled  Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server  https://csye6225-fall2018-chandwanid.me//transaction/8a8080cd67512ea401675137df450000/attachment s
WASC Id Source ID  Low (Medium)  Description  URL  Method Paramet	16 15 3  Web Browser XSS Protection Not Enabled  Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server  https://csye6225-fall2018-chandwanid.me//transaction/8a8080cd67512ea401675137df450000/attachment s  POST
WASC Id Source ID Low (Medium)  Description  URL  Method Paramet er	16 15 3  Web Browser XSS Protection Not Enabled  Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server  https://csye6225-fall2018-chandwanid.me//transaction/8a8080cd67512ea401675137df450000/attachment s  POST  X-XSS-Protection
WASC Id Source ID  Low (Medium)  Description  URL  Method  Paramet er  URL	16 15 3  Web Browser XSS Protection Not Enabled  Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server  https://csye6225-fall2018-chandwanid.me//transaction/8a8080cd67512ea401675137df450000/attachment s  POST  X-XSS-Protection  https://csye6225-fall2018-chandwanid.me/
WASC Id Source ID Low (Medium)  Description  URL  Method Paramet er  URL  Method Paramet	16 15 3  Web Browser XSS Protection Not Enabled  Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server  https://csye6225-fall2018-chandwanid.me//transaction/8a8080cd67512ea401675137df450000/attachment s  POST  X-XSS-Protection  https://csye6225-fall2018-chandwanid.me/  GET

Method	POST
	POS1
Paramet er	X-XSS-Protection
URL	https://csye6225-fall2018-chandwanid.me/transaction/8a8080cd67512ea401675137df450000/attachment s
Method	POST
Paramet er	X-XSS-Protection
Instances	4
Solution	Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.
	The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it:
	X-XSS-Protection: 1; mode=block
	X-XSS-Protection: 1; report=http://www.example.com/xss
Other information	The following values would disable it:
	X-XSS-Protection: 0
	The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit).
	Note that this alert is only raised if the response body could potentially contain
	an XSS payload (with a text-based content type, with a non-zero length).
Reference	
Reference	an XSS payload (with a text-based content type, with a non-zero length).  https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Che
Reference CWE Id	an XSS payload (with a text-based content type, with a non-zero length).  https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Che at_Sheet
	an XSS payload (with a text-based content type, with a non-zero length).  https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Che at_Sheet  https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/
CWE Id	an XSS payload (with a text-based content type, with a non-zero length).  https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Che at_Sheet  https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/933
CWE Id WASC Id	an XSS payload (with a text-based content type, with a non-zero length).  https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Che at_Sheet  https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/933  14
CWE Id WASC Id Source ID	an XSS payload (with a text-based content type, with a non-zero length).  https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Che at_Sheet  https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/933  14 3
CWE Id WASC Id Source ID Low (Medium)	an XSS payload (with a text-based content type, with a non-zero length).  https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Che at_Sheet  https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/ 933  14  3  Incomplete or No Cache-control and Pragma HTTP Header Set  The cache-control and pragma HTTP header have not been set properly or are
CWE Id WASC Id Source ID Low (Medium) Description	an XSS payload (with a text-based content type, with a non-zero length).  https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Che at_Sheet  https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/ 933  14  3  Incomplete or No Cache-control and Pragma HTTP Header Set  The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.
CWE Id WASC Id Source ID Low (Medium) Description URL	an XSS payload (with a text-based content type, with a non-zero length).  https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Che at_Sheet  https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/ 933  14  3  Incomplete or No Cache-control and Pragma HTTP Header Set  The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.  https://csye6225-fall2018-chandwanid.me/user

URL	https://csye6225-fall2018-chandwanid.me/
Method	GET
Paramet er	Cache-Control
URL	https://csye6225-fall2018-chandwanid.me/transaction
Method	POST
Paramet er	Cache-Control
Instances	3
Solution	Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate; and that the pragma HTTP header is set with no-cache.
Reference	$https://www.owasp.org/index.php/Session\_Management\_Cheat\_Sheet\#Web\_Content\_Caching$
CWE Id	525
WASC Id	13
Source ID	3
Low (Medium)	Web Browser XSS Protection Not Enabled
Description	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server
URL	http://csye6225-fall2018-chandwanid.me:443/user
Method	GET
Paramet er	X-XSS-Protection
	X-XSS-Protection  http://csye6225-fall2018-chandwanid.me:443/
er	
er URL	http://csye6225-fall2018-chandwanid.me:443/
er URL Method Paramet	http://csye6225-fall2018-chandwanid.me:443/ GET
er URL Method Paramet er	http://csye6225-fall2018-chandwanid.me:443/ GET  X-XSS-Protection
er URL Method Paramet er Instances	http://csye6225-fall2018-chandwanid.me:443/ GET  X-XSS-Protection  2 Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-

	The following values would disable it:
	X-XSS-Protection: 0
	The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit).
	Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).
Reference	https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Che at_Sheet
	https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/
CWE Id	933
WASC Id	14
Source ID	3
Low (Medium)	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://tracking-protection.cdn.mozilla.net/except-flashallow-digest256/1490633678
Method	GET
Parameter	X-Content-Type-Options
URL	https://tracking-protection.cdn.mozilla.net/block-flash-digest256/1496263270
Method	GET
Parameter	X-Content-Type-Options
URL	https://tracking-protection.cdn.mozilla.net/except-flash-digest256/1494877265
	ф
Method	GET
Method Parameter	
	GET
Parameter	GET X-Content-Type-Options
Parameter URL	GET  X-Content-Type-Options  https://tracking-protection.cdn.mozilla.net/base-track-digest256/1541603465
Parameter URL Method	GET  X-Content-Type-Options  https://tracking-protection.cdn.mozilla.net/base-track-digest256/1541603465  GET
Parameter URL Method Parameter	GET  X-Content-Type-Options  https://tracking-protection.cdn.mozilla.net/base-track-digest256/1541603465  GET  X-Content-Type-Options  https://tracking-protection.cdn.mozilla.net/allow-flashallow-
Parameter URL Method Parameter URL	GET  X-Content-Type-Options  https://tracking-protection.cdn.mozilla.net/base-track-digest256/1541603465  GET  X-Content-Type-Options  https://tracking-protection.cdn.mozilla.net/allow-flashallow-digest256/1490633678

URL	https://tracking-protection.cdn.mozilla.net/mozstd-trackwhite-digest256/1541603465
Method	GET
Parameter	X-Content-Type-Options
URL	https://tracking-protection.cdn.mozilla.net/except-flashsubdocdigest256/1517935265
Method	GET
Parameter	X-Content-Type-Options
URL	https://tracking-protection.cdn.mozilla.net/block-flashsubdocdigest256/1512160865
Method	GET
Parameter	X-Content-Type-Options
Instances	8
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.
	If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.
	At "High" threshold this scanner will not alert on client or server error responses.
	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx
Reference	https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
Source ID	3
Low (Medium)	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content
	type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	
URL Method	content type (if one is set), rather than performing MIME-sniffing.  https://shavar.services.mozilla.com/downloads?client=navclient-auto-

Parameter	X-Content-Type-Options
Instances	1
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.  If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.  At "High" threshold this scanner will not alert on client or server error responses.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
Source ID	3



## **Summary of Alerts**

Risk Level	Number of Alerts
<u>High</u>	0
<u>Medium</u>	1
Low	8
Informational	0

## **Alert Detail**

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	https://csye6225-fall2018-bhargavan.me/transaction
Method	POST

Parameter	X-Frame-Options
Instances	1
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).
Reference	http://blogs.msdn.com/b/ie internals/archive/2010/03/30/combating-click jacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15
Source ID	3
Low (Medium)	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://tracking-protection.cdn.mozilla.net/except-flashallow-digest256/1490633678
Method	GET
Parameter	X-Content-Type-Options
URL	https://tracking-protection.cdn.mozilla.net/block-flash-digest256/1496263270
Method	GET
Parameter	X-Content-Type-Options
URL	https://tracking-protection.cdn.mozilla.net/except-flash-digest256/1494877265
Method	GET
Parameter	X-Content-Type-Options
URL	https://tracking-protection.cdn.mozilla.net/base-track-digest256/1541603465
Method	GET
Parameter	X-Content-Type-Options
URL	https://tracking-protection.cdn.mozilla.net/allow-flashallow-digest256/1490633678
Method	GET
Parameter	X-Content-Type-Options
URL	https://tracking-protection.cdn.mozilla.net/mozstd-trackwhite-digest256/1541603465

Method	GET
Parameter	X-Content-Type-Options
URL	https://tracking-protection.cdn.mozilla.net/except-flashsubdocdigest256/1517935265
Method	GET
Parameter	X-Content-Type-Options
URL	https://tracking-protection.cdn.mozilla.net/block-flashsubdocdigest256/1512160865
Method	GET
Parameter	X-Content-Type-Options
Instances	8
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.  If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed
	by the web application/web server to not perform MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.  At "High" threshold this scanner will not alert on client or server error
	responses.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	
	16
WASC Id	15
WASC Id Source ID	
	15
Source ID	15 3
Source ID  Low (Medium)	X-Content-Type-Options Header Missing  The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared
Source ID  Low (Medium)  Description	X-Content-Type-Options Header Missing  The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.  https://shavar.services.mozilla.com/downloads?client=navclient-auto-
Source ID  Low (Medium)  Description  URL	X-Content-Type-Options Header Missing  The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.  https://shavar.services.mozilla.com/downloads?client=navclient-auto-ffox&appver=60.2&pver=2.2

Instances	1
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.  If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.  At "High" threshold this scanner will not alert on client or server error responses.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
Source ID	3
Low (Medium)	Incomplete or No Cache-control and Pragma HTTP Header Set
Description	The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.
URL	https://blocklists.settings.services.mozilla.com/v1/blocklist/3/%7Bec8030f7-c20a-464f-9b0e-13a3a9e97384%7D/60.2.0/Firefox/20180905211815/Linux_x86_64-gcc3/en-US/default/Linux%204.18.0-kali2-amd64%20(GTK%203.24.1%2Clibpulse%2012.2.0)/Kali/1.0/1/1/new/
URL Method	https://blocklists.settings.services.mozilla.com/v1/blocklist/3/%7Bec8030f7-c20a-464f-9b0e-13a3a9e97384%7D/60.2.0/Firefox/20180905211815/Linux_x86_64-gcc3/en-US/default/Linux%204.18.0-kali2-
	https://blocklists.settings.services.mozilla.com/v1/blocklist/3/%7Bec8030f7-c20a-464f-9b0e-13a3a9e97384%7D/60.2.0/Firefox/20180905211815/Linux_x86_64-gcc3/en-US/default/Linux%204.18.0-kali2-amd64%20(GTK%203.24.1%2Clibpulse%2012.2.0)/Kali/1.0/1/1/new/
Method Paramet	https://blocklists.settings.services.mozilla.com/v1/blocklist/3/%7Bec8030f7-c20a-464f-9b0e-13a3a9e97384%7D/60.2.0/Firefox/20180905211815/Linux_x86_64-gcc3/en-US/default/Linux%204.18.0-kali2-amd64%20(GTK%203.24.1%2Clibpulse%2012.2.0)/Kali/1.0/1/1/new/GET
Method Paramet er	https://blocklists.settings.services.mozilla.com/v1/blocklist/3/%7Bec8030f7-c20a-464f-9b0e-13a3a9e97384%7D/60.2.0/Firefox/20180905211815/Linux_x86_64-gcc3/en-US/default/Linux%204.18.0-kali2-amd64%20(GTK%203.24.1%2Clibpulse%2012.2.0)/Kali/1.0/1/1/new/GET  Cache-Control
Method Paramet er Instances	https://blocklists.settings.services.mozilla.com/v1/blocklist/3/%7Bec8030f7-c20a-464f-9b0e-13a3a9e97384%7D/60.2.0/Firefox/20180905211815/Linux_x86_64-gcc3/en-US/default/Linux%204.18.0-kali2-amd64%20(GTK%203.24.1%2Clibpulse%2012.2.0)/Kali/1.0/1/1/new/ GET  Cache-Control  1  Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate; and that the pragma HTTP header is set with no-
Method Paramet er Instances Solution	https://blocklists.settings.services.mozilla.com/v1/blocklist/3/%7Bec8030f7-c20a-464f-9b0e-13a3a9e97384%7D/60.2.0/Firefox/20180905211815/Linux_x86_64-gcc3/en-US/default/Linux%204.18.0-kali2-amd64%20(GTK%203.24.1%2Clibpulse%2012.2.0)/Kali/1.0/1/1/new/GET  Cache-Control  Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate; and that the pragma HTTP header is set with no-cache.  https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Co
Method Paramet er Instances Solution Reference	https://blocklists.settings.services.mozilla.com/v1/blocklist/3/%7Bec8030f7-c20a-464f-9b0e-13a3a9e97384%7D/60.2.0/Firefox/20180905211815/Linux_x86_64-gcc3/en-US/default/Linux%204.18.0-kali2-amd64%20(GTK%203.24.1%2Clibpulse%2012.2.0)/Kali/1.0/1/1/new/GET  Cache-Control  Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate; and that the pragma HTTP header is set with no-cache.  https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
Method Paramet er Instances Solution Reference CWE Id	https://blocklists.settings.services.mozilla.com/v1/blocklist/3/%7Bec8030f7-c20a-464f-9b0e-13a3a9e97384%7D/60.2.0/Firefox/20180905211815/Linux_x86_64-gcc3/en-US/default/Linux%204.18.0-kali2-amd64%20(GTK%203.24.1%2Clibpulse%2012.2.0)/Kali/1.0/1/1/new/  GET  Cache-Control  Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate; and that the pragma HTTP header is set with no-cache.  https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching  525
Method Paramet er Instances Solution Reference CWE Id WASC Id	https://blocklists.settings.services.mozilla.com/v1/blocklist/3/%7Bec8030f7-c20a-464f-9b0e-13a3a9e97384%7D/60.2.0/Firefox/20180905211815/Linux_x86_64-gcc3/en-US/default/Linux%204.18.0-kali2-amd64%20(GTK%203.24.1%2Clibpulse%2012.2.0)/Kali/1.0/1/1/new/  GET  Cache-Control  1  Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate; and that the pragma HTTP header is set with no-cache.  https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching 525  13

URL	https://activity-stream-icons.services.mozilla.com/v1/icons.json.br
Method	GET
Paramet er	Cache-Control
Evidenc e	public,max-age=3600
Instances	1
Solution	Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate; and that the pragma HTTP header is set with no-cache.
Reference	$https://www.owasp.org/index.php/Session\_Management\_Cheat\_Sheet\#Web\_Content\_Caching$
CWE Id	525
WASC Id	13
Source ID	3
Low (Medium)	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://activity-stream-icons.services.mozilla.com/v1/icons.json.br
Method	GET
Parameter	X-Content-Type-Options
Instances	1
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.  If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed
	by the web application/web server to not perform MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.
	At "High" threshold this scanner will not alert on client or server error responses.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx
	https://www.owasp.org/index.php/List_of_useful_HTTP_headers

	16
WASC Id	15
Source ID	3
Low (Medium)	Incomplete or No Cache-control and Pragma HTTP Header Set
Description	The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.
URL	https://csye6225-fall2018-bhargavan.me/transaction
Method	POST
Paramet er	Cache-Control
URL	https://csye6225-fall2018-bhargavan.me/user
Method	GET
Paramet er	Cache-Control
Instances	2
Solution	Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate; and that the pragma HTTP header is set with no-cache.
Reference	$https://www.owasp.org/index.php/Session\_Management\_Cheat\_Sheet\#Web\_Content\_Caching$
CWE Id	525
WASC Id	13
Source ID	3
Low (Medium)	Web Browser XSS Protection Not Enabled
Description	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server
URL	https://csye6225-fall2018-bhargavan.me/transaction
Method	POST
Paramet er	X-XSS-Protection
	https://csye6225-fall2018-bhargavan.me/transaction/64838762894632846239/attachments
URL	Shargavarimie, transaction, o receive 200 receive recognition in onte
URL Method	POST
Method Paramet	POST
Description  URL  Method  Paramet er	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server  https://csye6225-fall2018-bhargavan.me/transaction  POST  X-XSS-Protection  https://csye6225-fall2018-

	The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it:
	X-XSS-Protection: 1; mode=block
	X-XSS-Protection: 1; report=http://www.example.com/xss
Other information	The following values would disable it:
	X-XSS-Protection: 0
	The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit).
	Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).
Reference	https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Che at_Sheet
	https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/
CWE Id	933
WASC Id	14
Source ID	3
Source ID  Low (Medium)	3  X-Content-Type-Options Header Missing
Low (Medium)	X-Content-Type-Options Header Missing  The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared
Low (Medium)  Description	X-Content-Type-Options Header Missing  The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Low (Medium)  Description  URL	X-Content-Type-Options Header Missing  The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.  https://csye6225-fall2018-bhargavan.me/user
Low (Medium)  Description  URL  Method	X-Content-Type-Options Header Missing  The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.  https://csye6225-fall2018-bhargavan.me/user  GET
Low (Medium)  Description  URL  Method  Parameter	X-Content-Type-Options Header Missing  The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.  https://csye6225-fall2018-bhargavan.me/user  GET  X-Content-Type-Options
Low (Medium)  Description  URL  Method  Parameter  URL	X-Content-Type-Options Header Missing  The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.  https://csye6225-fall2018-bhargavan.me/user  GET  X-Content-Type-Options  https://csye6225-fall2018-bhargavan.me/transaction
Low (Medium)  Description  URL  Method  Parameter  URL  Method	X-Content-Type-Options Header Missing  The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.  https://csye6225-fall2018-bhargavan.me/user  GET  X-Content-Type-Options  https://csye6225-fall2018-bhargavan.me/transaction  POST
Low (Medium)  Description  URL  Method  Parameter  URL  Method  Parameter	X-Content-Type-Options Header Missing  The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.  https://csye6225-fall2018-bhargavan.me/user  GET  X-Content-Type-Options  https://csye6225-fall2018-bhargavan.me/transaction  POST  X-Content-Type-Options

	If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.  At "High" threshold this scanner will not alert on client or server error responses.
	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx
Reference	https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
Source ID	3