



Web Application Report

This report includes important security information about your web application.

Security Report

This report was created by IBM Security AppScan Standard 9.0.3.7 iFix005, Rules: 12742
Scan started: 4/8/2019 5:52:53 PM

Table of Contents

Introduction

- General Information
- Login Settings

Summary

- Issue Types
- Vulnerable URLs
- Fix Recommendations
- Security Risks
- Causes
- WASC Threat Classification

Issues Sorted by Issue Type

- Cross-Site Scripting **2**
- Body Parameters Accepted in Query **1**
- Cacheable SSL Page Found **39**
- Missing or insecure "Content-Security-Policy" header **5**
- Query Parameter in SSL Request **36**
- Unsafe third-party link (target="_blank") **6**
- Application Error **1**
- Application Test Script Detected **1**
- Client-Side (JavaScript) Cookie References **1**
- Integer Overflow **2**

Application Data

- Cookies
- JavaScripts

- Parameters
- Comments
- Visited URLs
- Failed Requests
- Filtered URLs

Introduction

This report contains the results of a web application security scan performed by IBM Security AppScan Standard.

High severity issues:	2
Low severity issues:	87
Informational severity issues:	5
Total security issues included in the report:	94
Total security issues discovered in the scan:	94

General Information

Scan file name: Activetenders_tender_080419

Scan started: 4/8/2019 5:52:53 PM

Test policy: Application-Only

Host 164.100.129.63

Port 0

Operating system: Unknown

Web server: Apache

Application server: Any

Login Settings

Login method: Recorded login

Concurrent logins: Enabled

JavaScript execution: Disabled

In-session detection: Enabled

In-session pattern:

Tracked or session ID cookies:

Tracked or session ID parameters:

Login sequence:

```
https://164.100.129.63/cppp8/  
https://164.100.129.63/cppp8/sites/all/themes/cppp/css/base/fonts/ro  
boto slab-regular-webfont.woff2  
https://164.100.129.63/cppp8/sites/all/themes/cppp/fonts/fontawesome  
-webfont.woff2?v=4.7.0  
https://164.100.129.63/cppp8/sites/all/themes/cppp/bootstrap/fonts/g  
lyphicons-halflings-regular.woff2  
https://164.100.129.63/cppp8/sites/default/files/orgname_json/orgnam  
e_json_data.json
```

https://164.100.129.63/cppp8/sites/default/files/dashboard_json/active_json_data.json
https://164.100.129.63/cppp8/sites/default/files/dashboard_json/open_json_data.json
https://164.100.129.63/cppp8/sites/default/files/dashboard_json/close_json_data.json
https://164.100.129.63/cppp8/sites/default/files/dashboard_json/totorg_json_data.json
https://164.100.129.63/cppp8/sites/default/files/dashboard_json/fin_yr_chart_data_live.json
https://164.100.129.63/cppp8/sites/default/files/dashboard_json/gepn icportals.json
https://164.100.129.63/cppp8/sites/default/files/dashboard_json/type wise_chart_data_live.json
https://164.100.129.63/cppp8/sites/default/files/dashboard_json/orgwise_chart_data_live.json
https://164.100.129.63/cppp8/sites/default/files/dashboard_json/fin_yr_aoc_chart_data_live.json

Summary

Issue Types 10

[TOC](#)

Issue Type		Number of Issues	
H	Cross-Site Scripting	2	
L	Body Parameters Accepted in Query	1	
L	Cacheable SSL Page Found	39	
L	Missing or insecure "Content-Security-Policy" header	5	
L	Query Parameter in SSL Request	36	
L	Unsafe third-party link (target="_blank")	6	
I	Application Error	1	
I	Application Test Script Detected	1	
I	Client-Side (JavaScript) Cookie References	1	
I	Integer Overflow	2	

Vulnerable URLs 48

[TOC](#)

URL		Number of Issues	
H	https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata	6	
H	https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata	4	
L	https://164.100.129.63/cppp8/core/assets/vendor/domready/ready.min.js	2	
L	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/data-min.js	2	
L	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/disable-selection-min.js	2	
L	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/focusable-min.js	2	
L	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/form-min.js	2	
L	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/ie-min.js	2	
L	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/jquery-1	2	

	-7-min.js		
L	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/keycode-min.js	2	
L	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/labels-min.js	2	
L	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/plugin-min.js	2	
L	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/safe-active-element-min.js	2	
L	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/safe-blur-min.js	2	
L	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/scroll-parent-min.js	2	
L	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/tabbable-min.js	2	
L	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/unique-id-min.js	2	
L	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/version-min.js	2	
L	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/widgets/datepicker-min.js	2	
L	https://164.100.129.63/cppp8/core/misc/drupal.init.js	2	
L	https://164.100.129.63/cppp8/core/misc/drupal.js	2	
L	https://164.100.129.63/cppp8/core/misc/drupalSettingsLoader.js	2	
L	https://164.100.129.63/cppp8/core/modules/locale/locale.datepicker.js	2	
L	https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata/byVFDsdWfYtJbJbmtnYjJZZ1VtRnBiSGRoZVhNPUExM2gxUld4bFkzUnlhV05oYkNCaGJtUWdUV0ZwYm5SbGJtRnVZMlVnVjI5eWEzTT1BMTNoMVltbGtYM04xWW0xcGMzTnBiMjVmWlcl1a1pHRjBaUT09QTEzaDFkR1ZrZEE9PQ==	2	
L	https://164.100.129.63/cppp8/sites/all/modules/appmodules/testmodules/latestactivecorrigendumsnew/js/latestactivecorrigendumsnew.js	2	
L	https://164.100.129.63/cppp8/sites/all/modules/appmodules/testmodules/latestactivetendersnew/js/latestactivetendersnew.js	2	
L	https://164.100.129.63/cppp8/sites/all/themes/cppp/bootstrap/js/boots-trap.min.js	2	
L	https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/c3.min.js	2	
L	https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/c3chart-slider.js	2	
L	https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/custom-common.js	2	
L	https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/d3.min.js	2	
L	https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/dncalendar.min.js	2	
L	https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/functions.js	3	
L	https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/general.js	2	
L	https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/jquery.b	2	

	ase64.min.js		
L	https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/pako.min.js	2	
L	https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/to-top.js	2	
L	https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/toggle.js	2	
L	https://164.100.129.63/cppp8/sites/default/files/orgname_json/orgname_json_data.json	2	
L	https://164.100.129.63/cppp8/sites/default/files/dashboard_json/active_json_data.json	1	
L	https://164.100.129.63/cppp8/sites/default/files/dashboard_json/close_json_data.json	1	
L	https://164.100.129.63/cppp8/sites/default/files/dashboard_json/open_json_data.json	1	
L	https://164.100.129.63/cppp8/sites/default/files/dashboard_json/totorg_json_data.json	1	
L	https://164.100.129.63/cppp8/core/assets/vendor/jquery/jquery.min.js	1	
L	https://164.100.129.63/cppp8/latestactivecorrigendumsnew	1	
L	https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata/byUTJWdWRISmhiQ0JRZFdKc2FXTWdWMji5YTNNZ1JHVndZWEowYldWdWRDQW9RMUJYUkNrPUExM2gxUTJsMmFXd2dWMji5YTNPUExM2gxWW1sa1gzTjFZbTFwYzNOcGlyNWZaVzVrWkdGMFpRPT1BMTNoMWRIbDA=	1	
L	https://164.100.129.63/cppp8/latestactivetendersnew	1	
I	https://164.100.129.63/cppp8/	1	

Fix Recommendations 9

TOC

Remediation Task		Number of Issues	
H	Review possible solutions for hazardous character injection	2	
L	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"	6	
L	Always use SSL and POST (body) parameters when sending sensitive information.	36	
L	Config your server to use the "Content-Security-Policy" header with secure policies	5	
L	Do not accept body parameters that are sent in the query string	1	
L	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.	39	
L	Remove business and security logic from the client side	1	
L	Remove test scripts from the server	1	
L	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions	3	

Security Risks 7

TOC

Risk		Number of Issues	
H	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user	2	
L	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations	45	
L	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.	12	
L	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted	36	
I	It is possible to gather sensitive debugging information	3	
I	It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords	1	
I	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side	1	






Causes 9

TOC

Cause		Number of Issues	
H	Sanitation of hazardous characters was not performed correctly on user input	2	
L	Insecure web application programming or configuration	6	
L	Sensitive information might have been cached by your browser	39	
L	Query parameters were passed over SSL, and may contain sensitive information	36	
L	The rel attribute in the link element is not set to "noopener noreferrer".	6	
I	Proper bounds checking were not performed on incoming parameter values	3	
I	No validation was done in order to make sure that user input matches the data type expected	3	
I	Temporary files were left in production environment	1	
I	Cookies are created at the client side	1	

WASC Threat Classification

TOC

Threat	Number of Issues	
Abuse of Functionality	6	
Cross-site Scripting	2	
Information Leakage	83	
Integer Overflows	2	
Predictable Resource Location	1	

Issues Sorted by Issue Type

H

Cross-Site Scripting 2

TOC

Issue 1 of 2

TOC

Cross-Site Scripting

Severity: **High**

CVSS Score: 7.5

URL: <https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata>

Entity: cpppdata (Page)

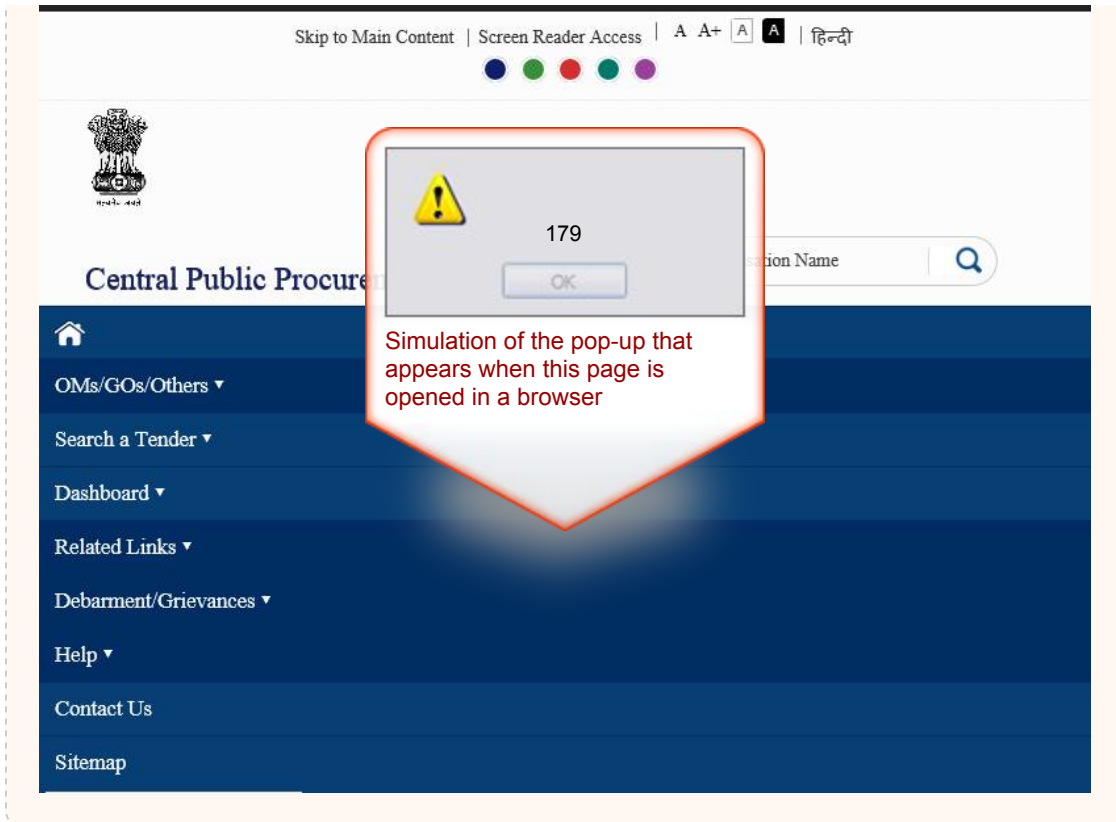
Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Sanitation of hazardous characters was not performed correctly on user input

Fix: Review possible solutions for hazardous character injection

Reasoning: The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

Test Response



Raw Test Response:

```
...
</div>
</div>
<div id="block-cppp-content" class="block block-system block-system-main-block">

    <div class="content">
        <form class="latestactivetendersnew-form" data-drupal-selector="latestactivetendersnew-
form"
action="https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata/"style=foo:expression(179+
{toString:alert}))!" method="post" id="latestactivetendersnew-form" accept-charset="UTF-8">
...

```

Cross-Site Scripting

Severity: **High**

CVSS Score: 7.5

URL: <https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata>

Entity: cpppdata (Page)

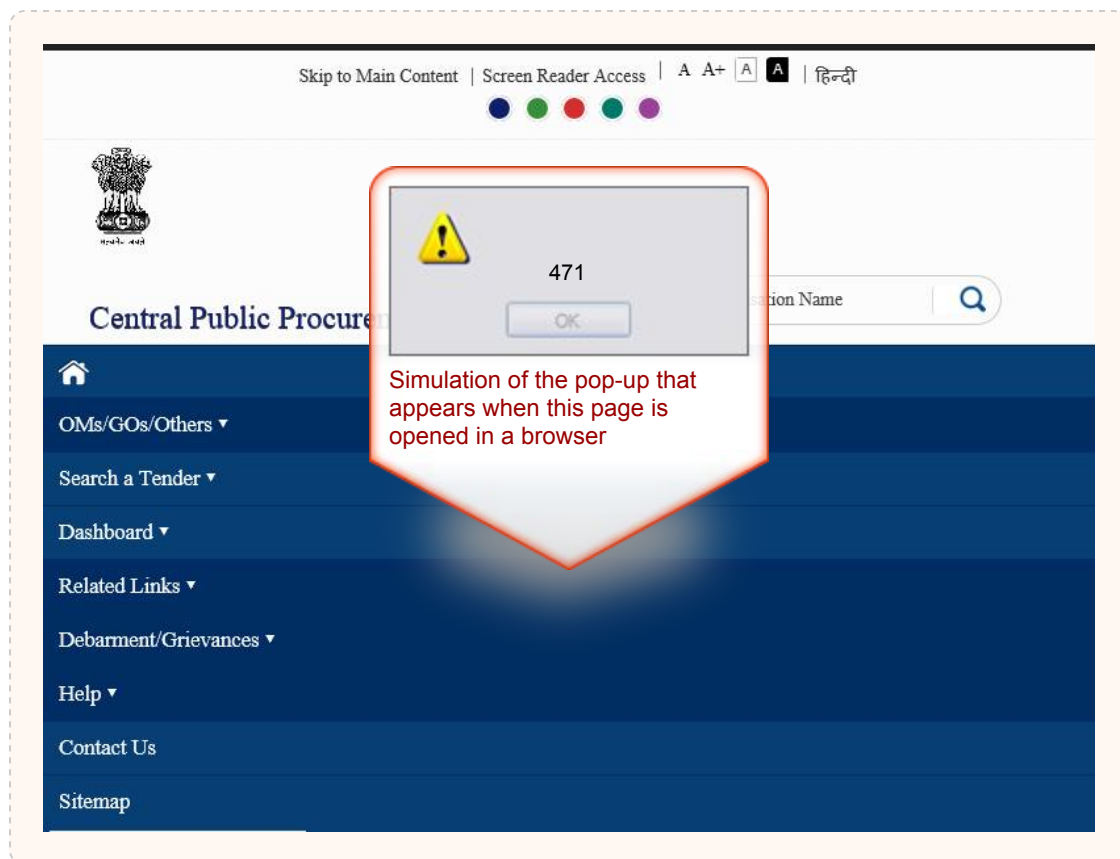
Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Sanitation of hazardous characters was not performed correctly on user input

Fix: Review possible solutions for hazardous character injection

Reasoning: The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

Test Response



Raw Test Response:

```
...
</div>
</div>
<div id="block-cppp-content" class="block block-system block-system-main-block">
```

```
<div class="content">
  <form class="latestactivecorrigendumsnew-form" data-drupal-
selector="latestactivecorrigendumsnew-form"
action="https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata/"style=foo:expression(4
71+{toString:alert}))!" method="post" id="latestactivecorrigendumsnew-form" accept-charset="UTF-
8">

  ...
```

Body Parameters Accepted in Query

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata>

Entity: cpppdata (Page)

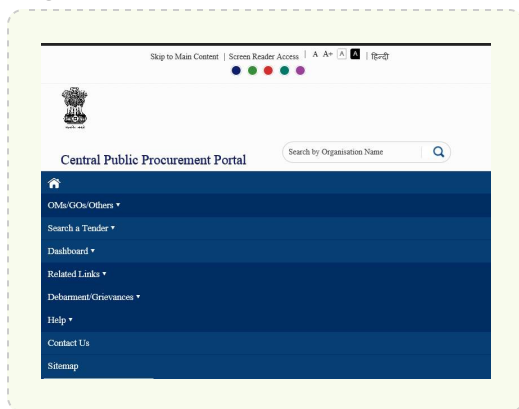
Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

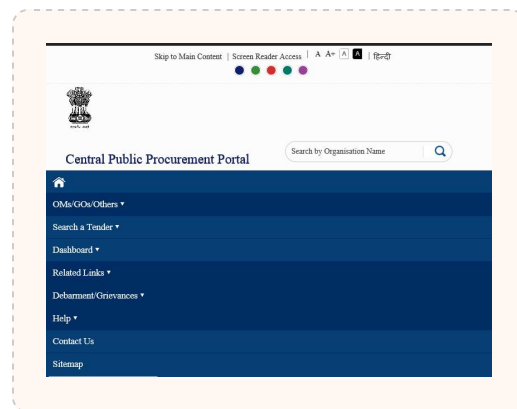
Fix: Do not accept body parameters that are sent in the query string

Reasoning: The test result seems to indicate a vulnerability because the Test Response is similar to the Original Response, indicating that the application processed body parameters that were submitted in the query

Original Response



Test Response



Cacheable SSL Page Found	
Severity:	Low
CVSS Score:	5.0
URL:	https://164.100.129.63/cppp8/sites/default/files/orgname_json/orgname_json_data.json
Entity:	orgname_json_data.json (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Fri, 09 Nov 2018 12:10:18 GMT
Connection: Keep-Alive
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 39498
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Keep-Alive: timeout=5, max=92
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "9a4a-57a3a3c111e80"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:14 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/json
...
```


Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/misc/drupalSettingsLoader.js>

Entity: drupalSettingsLoader.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 519
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "207-5848059b0e9c0"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:33 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

/**
...
```

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/domready/ready.min.js>

Entity: ready.min.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 485
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "1e5-5848059b0e9c0"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:27 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

/!!
...
```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/data-min.js>

Entity: data-min.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 405
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "195-5848059b0e9c0"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:43 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

/*! jQuery UI - v1.12.1 - 2017-03-31
...
```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata>

Entity: cpppdata (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
...
Access-Control-Allow-Origin: eprocure.gov.in
X-XSS-Protection: 1; mode=block
Connection: Keep-Alive
X-Drupal-Dynamic-Cache: HIT
Vary:
Keep-Alive: timeout=5, max=99
Date: Mon, 08 Apr 2019 12:07:15 GMT
Content-Type: text/html; charset=UTF-8
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Cache-Control: must-revalidate, no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules/content/ dc:
http://purl.org/dc/terms/ foaf: http://xmlns.com/foaf/0.1/ og: http://ogp.me/ns# rdfs:
http://www.w3.org/2000/01/rdf-schema# schema: http://schema.org/ sioc: http://rdfs.org/sioc/ns#
sioc: http://rdfs.org/sioc/types# skos: http://www.w3.org/2004/02/skos/core# xsd:
http://www.w3.org/2001/XMLSchema# ">
  <head>
    <meta charset="utf-8" />
    <meta name="MobileOptimized" content="width" />
    <meta name="HandheldFriendly" content="true" />
  ...
```

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/misc/drupal.js>

Entity: drupal.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 5313
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "14c1-5848059b0e9c0"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:34 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

/**
...
```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/disable-selection-min.js>

Entity: disable-selection-min.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 528
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "210-5848059b0e9c0"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:43 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

/*! jQuery UI - v1.12.1 - 2017-03-31
...
```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata>

Entity: cpppdata (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
...
Access-Control-Allow-Origin: eprocure.gov.in
X-XSS-Protection: 1; mode=block
Connection: Keep-Alive
X-Drupal-Dynamic-Cache: HIT
Vary:
Keep-Alive: timeout=5, max=92
Date: Mon, 08 Apr 2019 12:07:15 GMT
Content-Type: text/html; charset=UTF-8
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Cache-Control: must-revalidate, no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules/content/ dc:
http://purl.org/dc/terms/ foaf: http://xmlns.com/foaf/0.1/ og: http://ogp.me/ns# rdfs:
http://www.w3.org/2000/01/rdf-schema# schema: http://schema.org/ sioc: http://rdfs.org/sioc/ns#
sioc: http://rdfs.org/sioc/types# skos: http://www.w3.org/2004/02/skos/core# xsd:
http://www.w3.org/2001/XMLSchema# ">
  <head>
    <meta charset="utf-8" />
    <meta name="MobileOptimized" content="width" />
    <meta name="HandheldFriendly" content="true" />
  ...
```

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/misc/drupal.init.js>

Entity: drupal.init.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 409
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "199-5848059b0e9c0"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:41 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

/**
...
```


Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata/byVFdsdWFYTjBjbmtnYjJZZ1VtRnBiSGRoZVhNPUExM2gxUld4bFkzUnlhV05oYkNCaGJtUWdUV0ZwYm5SbGJtRnVZMlVnVjI5eWEzTT1BMTNoMVltbGtYM04xWW0xcGMzTnBiMjVmWlc1a1pHRjBaUT09QTEzaDFkR1ZrZEE9PQ==>

Entity: byVFdsdWFYTjBjbmtnYjJZZ1VtRnBiSGRoZVhNPUExM2gxUld4bFkzUnlhV05oYkNCaGJtUWdUV0ZwYm5SbGJtRnVZMlVnVjI5eWEzTT1BMTNoMVltbGtYM04xWW0xcGMzTnBiMjVmWlc1a1pHRjBaUT09QTEzaDFkR1ZrZEE9PQ== (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
...
Access-Control-Allow-Origin: eprocure.gov.in
X-XSS-Protection: 1; mode=block
Connection: Keep-Alive
X-Drupal-Dynamic-Cache: HIT
Vary:
Keep-Alive: timeout=5, max=96
Date: Mon, 08 Apr 2019 12:07:15 GMT
Content-Type: text/html; charset=UTF-8
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-inline' 'unsafe-eval'
Cache-Control: must-revalidate, no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules/content/ dc:
http://purl.org/dc/terms/ foaf: http://xmlns.com/foaf/0.1/ og: http://ogp.me/ns# rdfs:
http://www.w3.org/2000/01/rdf-schema# schema: http://schema.org/ sioc: http://rdfs.org/sioc/ns#
sioc: http://rdfs.org/sioc/types# skos: http://www.w3.org/2004/02/skos/core# xsd:
http://www.w3.org/2001/XMLSchema# ">
  <head>
    <meta charset="utf-8" />
    <meta name="MobileOptimized" content="width" />
    <meta name="HandheldFriendly" content="true" />
  ...
```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/safe-active-element-min.js>

Entity: safe-active-element-min.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 370
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "172-5848059b0e9c0"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:50 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

/*! jQuery UI - v1.12.1 - 2017-03-31
...
```

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/jquery-1-7-min.js>

Entity: jquery-1-7-min.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 1051
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "41b-5848059b0e9c0"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:46 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

/*! jQuery UI - v1.12.1 - 2017-03-31
...
```

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/form-min.js>

Entity: form-min.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 337
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "151-5848059b0e9c0"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:43 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

/*! jQuery UI - v1.12.1 - 2017-03-31
...
```

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/focusable-min.js>

Entity: focusable-min.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 868
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "364-5848059b0e9c0"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:48 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

/*! jQuery UI - v1.12.1 - 2017-03-31
...
```

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/labels-min.js>

Entity: labels-min.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 600
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "258-5848059b0e9c0"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:46 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

/*! jQuery UI - v1.12.1 - 2017-03-31
...
```

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/tabbable-min.js>

Entity: tabbable-min.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 377
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "179-5848059b0e9c0"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:47 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

/*! jQuery UI - v1.12.1 - 2017-03-31
...
```

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/scroll-parent-min.js>

Entity: scroll-parent-min.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 590
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "24e-5848059b0e9c0"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:47 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

/*! jQuery UI - v1.12.1 - 2017-03-31
...
```


Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/unique-id-min.js>

Entity: unique-id-min.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 481
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "1e1-5848059b0e9c0"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:48 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

/*! jQuery UI - v1.12.1 - 2017-03-31
...
```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/safe-blur-min.js>

Entity: safe-blur-min.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 328
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "148-5848059b0e9c0"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:52 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

/*! jQuery UI - v1.12.1 - 2017-03-31
...
```

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/version-min.js>

Entity: version-min.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 266
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "10a-5848059b0e9c0"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:49 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

/*! jQuery UI - v1.12.1 - 2017-03-31
...
```

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/themes/cppp/bootstrap/js/bootstrap.min.js>

Entity: bootstrap.min.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Fri, 09 Feb 2018 06:30:56 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 37046
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "90b6-564clabb84800"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:53 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

/*!
...
```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/ie-min.js>

Entity: ie-min.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 306
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "132-5848059b0e9c0"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:49 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

/*! jQuery UI - v1.12.1 - 2017-03-31
...
```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/modules/locale/locale.datepicker.js>

Entity: locale.datepicker.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 2095
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "82f-5848059b0e9c0"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:52 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

/**
...
```

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/keycode-min.js>

Entity: keycode-min.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 404
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "194-5848059b0e9c0"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:50 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

/*! jQuery UI - v1.12.1 - 2017-03-31
...
```

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/widgets/daterangepicker-min.js>

Entity: daterangepicker-min.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 36446
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "8e5e-5848059b0e9c0"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:53 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

/*! jQuery UI - v1.12.1 - 2017-03-31
...
```


Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/plugin-min.js>

Entity: plugin-min.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 561
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "231-5848059b0e9c0"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:50 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

/*! jQuery UI - v1.12.1 - 2017-03-31
...
```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/d3.min.js>

Entity: d3.min.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Mon, 04 Dec 2017 07:15:55 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 151733
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "250b5-55f7e7d39a0c0"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:58 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

!function(){function n(n){return n&&(n.ownerDocument||n.document||n).documentElement}function
t(n){return n&&
(n.ownerDocument&&n.ownerDocument.defaultView||n.document&&n||n.defaultView)}function e(n,t)...
```

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/customcommon.js>

Entity: customcommon.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Sat, 24 Nov 2018 10:53:26 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 31144
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "79a8-57b66e8ca3580"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:55 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

var $ = jQuery.noConflict();
...
```

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/toggle.js>

Entity: toggle.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Tue, 09 Feb 2016 11:04:09 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 417
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "1a1-52b5446d27c40"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:54 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

function hidePreHeader(){
...
```

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/general.js>

Entity: general.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Thu, 17 Jan 2019 12:58:11 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 15994
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "3e7a-57fa6f25c7ec0"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:55 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

/*-----*/
...
```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/pako.min.js>

Entity: pako.min.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Fri, 12 Oct 2018 10:26:53 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 46899
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "b733-5780586a9d540"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:59 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

!function(t){if("object"==typeof exports&&"undefined"!=typeof module)module.exports=t();else
if("function"==typeof define&&define.amd)define([],t);else{("undefined"!=typeof window?
window:"undefined"!=t...
```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/dncalendar.min.js>

Entity: dncalendar.min.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Mon, 06 Aug 2018 09:52:21 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 7274
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "1c6a-572c13bcb7f40"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:56 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

(function(a){a.fn.dnCalendar=function(n){var l=a(this);var b={};var d=new Date();var i=null;var
f=new Date();var e=function(q,s){var r=new Date(q,s-1,1);var o=new Date(q,s,0);var
p=r.getDay()+o.getDate...
```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/c3.min.js>

Entity: c3.min.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Thu, 17 Jan 2019 12:57:57 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 137277
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "2183d-57fa6f186df40"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:57 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

!function(a){"use strict";function b(a){this.owner=a}function c(a,b)
{if (Object.create)b.prototype=Object.create(a.prototype);else{var c=function()
{};c.prototype=a.prototype,b.prototype=new c}return b.p...
```


Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/functions.js>

Entity: functions.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Fri, 09 Feb 2018 09:29:46 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 318630
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "4dca6-564c42b471680"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:56 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

var $ = jQuery;
...
```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/jquery.base64.min.js>

Entity: jquery.base64.min.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Fri, 12 Oct 2018 10:26:32 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 1783
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "6f7-5780585696600"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:58 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

"use strict";jQuery.base64=(function($){var
_PADCHAR="=",_ALPHA="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/",_VERSION="
1.0";function _getbyte64(s,i){var idx=_ALPHA.indexOf(s.charA...
```

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/c3chartslider.js>

Entity: c3chartslider.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Mon, 06 Aug 2018 10:24:39 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 9488
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "2510-572claf4f07c0"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:59 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

$('.slider').each(function() {
  ...
```

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/to-top.js>

Entity: to-top.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Tue, 09 Feb 2016 11:04:09 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 316
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "13c-52b5446d27c40"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:08:02 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

jQuery(document).ready(function($) {
  ...
```

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/modules/appmodules/testmodules/latestactivecorrigendumsnew/js/latestactivecorrigendumsnew.js>

Entity: latestactivecorrigendumsnew.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Mon, 13 Aug 2018 10:57:20 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 377
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "179-5734ef5152400"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:08:01 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

var ddateToday = new Date();
...
```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/modules/appmodules/testmodules/latestactivetendersnew/js/atestactivetendersnew.js>

Entity: latestactivetendersnew.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Mon, 14 Jan 2019 13:42:01 GMT
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 726
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "2d6-57f6b3598fc40"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:08:02 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/javascript

var ddateToday = new Date();
...
```

L

Missing or insecure "Content-Security-Policy" header 5

TOC

Issue 1 of 5

TOC

Missing or insecure "Content-Security-Policy" header

Severity: **Low**

CVSS Score: 5.0

URL: https://164.100.129.63/cppp8/sites/default/files/dashboard_json/totorg_json_data.json

Entity: totorg_json_data.json (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "Content-Security-Policy" header with secure policies

Reasoning: AppScan detected that the Content-Security-Policy response header is missing or with an insecure policy, which increases exposure to various cross-site injection attacks

Raw Test Response:

```
...

Cookie: cookieWorked=yes;
SSESS196b5fb0ea7cfca9bfef1c5ca51a493=7QUXgoUc6yrlGytrAROpGbSurw5PuAmUQq8WhxtGroo;
li=https%3A%2F%2F164.100.129.63%2Fcppp8%2Flatestactivetendersnew
Connection: keep-alive
Host: 164.100.129.63
X-Requested-With: XMLHttpRequest
Content-Length: 0
Accept: */*
Accept-Language: en-US,en;q=0.5

HTTP/1.1 200 OK
Last-Modified: Mon, 20 Aug 2018 07:22:49 GMT
Connection: Keep-Alive
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 17
X-Frame-Options: DENY

...

X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Keep-Alive: timeout=5, max=95
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "11-573d8c6cce440"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:14 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/json

[
  {
    "totorg": 545
  }
]
```

...

Missing or insecure "Content-Security-Policy" header

Severity: Low

CVSS Score: 5.0

URL: https://164.100.129.63/cppp8/sites/default/files/dashboard_json/open_json_data.json

Entity: open_json_data.json (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "Content-Security-Policy" header with secure policies

Reasoning: AppScan detected that the Content-Security-Policy response header is missing or with an insecure policy, which increases exposure to various cross-site injection attacks

Raw Test Response:

...

```
Cookie: cookieWorked=yes;
SSESS196b5fb0ea7cfdca9bfef1c5ca51a493=7QUXgoUc6yrlGytrAROpGbSurw5PuAmUQq8WhxtGroo;
li=https%3A%2F%2F164.100.129.63%2Fcppp8%2Flatestactivetendersnew
Connection: keep-alive
Host: 164.100.129.63
X-Requested-With: XMLHttpRequest
Content-Length: 0
Accept: */*
Accept-Language: en-US,en;q=0.5
```

```
HTTP/1.1 200 OK
Last-Modified: Mon, 20 Aug 2018 07:22:49 GMT
Connection: Keep-Alive
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 16
X-Frame-Options: DENY
```

...

...

```
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Keep-Alive: timeout=5, max=99
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "10-573d8c6cce440"
```



```

Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:14 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/json

[
  {
    "open": 4608
  }
]

...

```

Issue 3 of 5

TOC

Missing or insecure "Content-Security-Policy" header

Severity: Low

CVSS Score: 5.0

URL: https://164.100.129.63/cppp8/sites/default/files/dashboard_json/active_json_data.json

Entity: active_json_data.json (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "Content-Security-Policy" header with secure policies

Reasoning: AppScan detected that the Content-Security-Policy response header is missing or with an insecure policy, which increases exposure to various cross-site injection attacks

Raw Test Response:

```

...

Cookie: cookieWorked=yes;
SSESS196b5fb0ea7cfdca9bfef1c5ca51a493=7QUXgoUc6yrlGytrAROpGbSurw5PuAmUQq8WhxtGroo;
li=https%3A%2F%2F164.100.129.63%2Fcppp8%2Flatestactivetendersnew
Connection: keep-alive
Host: 164.100.129.63
X-Requested-With: XMLHttpRequest
Content-Length: 0
Accept: */*
Accept-Language: en-US,en;q=0.5

HTTP/1.1 200 OK
Last-Modified: Mon, 20 Aug 2018 07:22:49 GMT
Connection: Keep-Alive
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 19
X-Frame-Options: DENY

```

```

...
...
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Keep-Alive: timeout=5, max=100
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "13-573d8c6cce440"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:15 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/json

[
  {
    "active": 37961
  }
]
...

```

Issue 4 of 5

TOC

Missing or insecure "Content-Security-Policy" header

Severity: Low

CVSS Score: 5.0

URL: https://164.100.129.63/cppp8/sites/default/files/orgname_json/orgname_json_data.json

Entity: orgname_json_data.json (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "Content-Security-Policy" header with secure policies

Reasoning: AppScan detected that the Content-Security-Policy response header is missing or with an insecure policy, which increases exposure to various cross-site injection attacks

Raw Test Response:

```

...

Referer: https://164.100.129.63/
Cookie: li=https%3A%2F%2F164.100.129.63%2Fcppp8%2Flatestactivetendersnew; cookieWorked=yes;
SSESS196b5fb0ea7cfdca9bfef1c5ca51a493=7QUXgoUc6yrlGytrAROpGbSurw5PuAmUQq8WhxtGroo
Connection: keep-alive
Host: 164.100.129.63
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5

```

```

HTTP/1.1 200 OK
Last-Modified: Fri, 09 Nov 2018 12:10:18 GMT
Connection: Keep-Alive
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 39498
X-Frame-Options: DENY

...

...

X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Keep-Alive: timeout=5, max=92
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "9a4a-57a3a3c111e80"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:14 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/json

[
  {
    "organisationname": "15th Finance Commission"
  },
  {
    "organisationname": "36th International Geological Congress"
  },
  {
    "organisationname": "ABV- Indian Institute of Information Technology and Management"
  },
  ...
]

```

Missing or insecure "Content-Security-Policy" header

Severity: Low

CVSS Score: 5.0

URL: https://164.100.129.63/cppp8/sites/default/files/dashboard_json/close_json_data.json

Entity: close_json_data.json (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "Content-Security-Policy" header with secure policies

Reasoning: AppScan detected that the Content-Security-Policy response header is missing or with an insecure policy, which increases exposure to various cross-site injection attacks

Raw Test Response:

```
...

Cookie: cookieWorked=yes;
SSESS196b5fb0ea7cfdca9bfef1c5ca51a493=7QUXgoUc6yrlGytrAROpGbSurw5PuAmUQq8WhxtGroo;
li=https%3A%2F%2F164.100.129.63%2Fcppp8%2Flatestactivetendersnew
Connection: keep-alive
Host: 164.100.129.63
X-Requested-With: XMLHttpRequest
Content-Length: 0
Accept: */*
Accept-Language: en-US,en;q=0.5

HTTP/1.1 200 OK
Last-Modified: Mon, 20 Aug 2018 07:22:49 GMT
Connection: Keep-Alive
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Accept-Ranges: bytes
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 17
X-Frame-Options: DENY

...

X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Keep-Alive: timeout=5, max=86
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
ETag: "11-573d8c6cce440"
Access-Control-Allow-Methods: POST, GET
Date: Mon, 08 Apr 2019 12:07:15 GMT
Content-Security-Policy: default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval'
Content-Type: application/json

[
  {
    "close": 5430
  }
]

...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/domready/ready.min.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /cppp8/core/assets/vendor/domready/ready.min.js?v=1.0.8 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
...
```

Issue 2 of 36

[TOC](#)

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/jquery.base64.min.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```

...
GET /cppp8/sites/all/themes/cppp/js/custom/jquery.base64.min.js?v=8.6.13 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Fri, 12 Oct 2018 10:26:32 GMT

...

```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery/jquery.min.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```

...
GET /cppp8/core/assets/vendor/jquery/jquery.min.js?v=3.2.1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT

...

```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/d3.min.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /cppp8/sites/all/themes/cppp/js/custom/d3.min.js?v=8.6.13 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Last-Modified: Mon, 04 Dec 2017 07:15:55 GMT
```

...

Issue 5 of 36

[TOC](#)

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/misc/drupalSettingsLoader.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```

...
GET /cphp8/core/misc/drupalSettingsLoader.js?v=8.6.13 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cphp8/latestactivetendersnew/cphpdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT

...

```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cphp8/core/misc/drupal.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```

...
GET /cphp8/core/misc/drupal.js?v=8.6.13 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cphp8/latestactivetendersnew/cphpdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT

...

```


Query Parameter in SSL Request

Severity:	Low
CVSS Score:	5.0
URL:	https://164.100.129.63/cppp8/core/misc/drupal.init.js
Entity:	v (Parameter)
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Query parameters were passed over SSL, and may contain sensitive information
Fix:	Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /cppp8/core/misc/drupal.init.js?v=8.6.13 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
...
```

Issue 8 of 36

[TOC](#)

Query Parameter in SSL Request

Severity:	Low
CVSS Score:	5.0
URL:	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/data-min.js
Entity:	v (Parameter)
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Query parameters were passed over SSL, and may contain sensitive information
Fix:	Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```

...
GET /cppp8/core/assets/vendor/jquery.ui/ui/data-min.js?v=1.12.1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT

...

```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/disable-selection-min.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```

...
GET /cppp8/core/assets/vendor/jquery.ui/ui/disable-selection-min.js?v=1.12.1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT

...

```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/pako.min.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /cppp8/sites/all/themes/cppp/js/custom/pako.min.js?v=8.6.13 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Fri, 12 Oct 2018 10:26:53 GMT
...
```

Issue 11 of 36

[TOC](#)

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery/ui/ui/form-min.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```

...
GET /cphp8/core/assets/vendor/jquery.ui/ui/form-min.js?v=1.12.1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cphp8/latestactivetendersnew/cphpdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT

...

```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cphp8/sites/all/themes/cphp/js/custom/c3chartslider.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```

...
GET /cphp8/sites/all/themes/cphp/js/custom/c3chartslider.js?v=8.6.13 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cphp8/latestactivetendersnew/cphpdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Mon, 06 Aug 2018 10:24:39 GMT

...

```

Query Parameter in SSL Request

Severity:	Low
CVSS Score:	5.0
URL:	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/labels-min.js
Entity:	v (Parameter)
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Query parameters were passed over SSL, and may contain sensitive information
Fix:	Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /cppp8/core/assets/vendor/jquery.ui/ui/labels-min.js?v=1.12.1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
...
```

Issue 14 of 36

[TOC](#)

Query Parameter in SSL Request

Severity:	Low
CVSS Score:	5.0
URL:	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/scroll-parent-min.js
Entity:	v (Parameter)
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Query parameters were passed over SSL, and may contain sensitive information
Fix:	Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```

...
GET /cphp8/core/assets/vendor/jquery.ui/ui/scroll-parent-min.js?v=1.12.1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cphp8/latestactivetendersnew/cphpdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT

...

```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cphp8/core/assets/vendor/jquery.ui/ui/jquery-1-7-min.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```

...
GET /cphp8/core/assets/vendor/jquery.ui/ui/jquery-1-7-min.js?v=1.12.1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cphp8/latestactivetendersnew/cphpdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT

...

```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/tabbable-min.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /cppp8/core/assets/vendor/jquery.ui/ui/tabbable-min.js?v=1.12.1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
...
```

Issue 17 of 36

[TOC](#)

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/unique-id-min.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```

...
GET /cppp8/core/assets/vendor/jquery.ui/ui/unique-id-min.js?v=1.12.1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT

...

```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/modules/appmodules/testmodules/latestactivecorrigendumsnew/js/latestactivecorrigendumsnew.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```

...
GET
/cppp8/sites/all/modules/appmodules/testmodules/latestactivecorrigendumsnew/js/latestactivecorrigendumsnew.js?v=8.6.13 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Mon, 13 Aug 2018 10:57:20 GMT

...

```


Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/version-min.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /cppp8/core/assets/vendor/jquery.ui/ui/version-min.js?v=1.12.1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/to-top.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /cppp8/sites/all/themes/cppp/js/custom/to-top.js?v=8.6.13 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Tue, 09 Feb 2016 11:04:09 GMT

...
```

Issue 21 of 36

TOC

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/focusable-min.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /cppp8/core/assets/vendor/jquery.ui/ui/focusable-min.js?v=1.12.1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT

...
```

Query Parameter in SSL Request**Severity:** Low**CVSS Score:** 5.0**URL:** <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/ie-min.js>**Entity:** v (Parameter)**Risk:** It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted**Causes:** Query parameters were passed over SSL, and may contain sensitive information**Fix:** Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /cppp8/core/assets/vendor/jquery.ui/ui/ie-min.js?v=1.12.1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
...
```

Query Parameter in SSL Request**Severity:** Low**CVSS Score:** 5.0**URL:** <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/keycode-min.js>**Entity:** v (Parameter)**Risk:** It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted**Causes:** Query parameters were passed over SSL, and may contain sensitive information**Fix:** Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /cppp8/core/assets/vendor/jquery.ui/ui/keycode-min.js?v=1.12.1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT

...
```

Issue 24 of 36

TOC

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/plugin-min.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /cppp8/core/assets/vendor/jquery.ui/ui/plugin-min.js?v=1.12.1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT

...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/modules/appmodules/testmodules/latestactivetendersnew/js/latestactivetendersnew.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET
/cppp8/sites/all/modules/appmodules/testmodules/latestactivetendersnew/js/latestactivetendersnew.js?v=8.6.13 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Mon, 14 Jan 2019 13:42:01 GMT
...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/safe-active-element-min.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /cphp8/core/assets/vendor/jquery.ui/ui/safe-active-element-min.js?v=1.12.1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cphp8/latestactivetendersnew/cphpdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
```

...

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cphp8/core/assets/vendor/jquery.ui/ui/safe-blur-min.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /cphp8/core/assets/vendor/jquery.ui/ui/safe-blur-min.js?v=1.12.1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cphp8/latestactivetendersnew/cphpdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
```

...

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/modules/locale/locale.datepicker.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /cppp8/core/modules/locale/locale.datepicker.js?v=8.6.13 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT
...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/widgets/datepicker-min.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /cppp8/core/assets/vendor/jquery.ui/ui/widgets/datepicker-min.js?v=1.12.1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Wed, 20 Mar 2019 06:01:19 GMT

...
```

Query Parameter in SSL Request	
Severity:	Low
CVSS Score:	5.0
URL:	https://164.100.129.63/cppp8/sites/all/themes/cppp/bootstrap/js/bootstrap.min.js
Entity:	v (Parameter)
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Query parameters were passed over SSL, and may contain sensitive information
Fix:	Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /cppp8/sites/all/themes/cppp/bootstrap/js/bootstrap.min.js?v=8.6.13 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Fri, 09 Feb 2018 06:30:56 GMT

...
```


Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/toggle.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /cppp8/sites/all/themes/cppp/js/custom/toggle.js?v=8.6.13 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Tue, 09 Feb 2016 11:04:09 GMT
...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/general.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over

SSL.

Original Request

```
...
GET /cppp8/sites/all/themes/cppp/js/custom/general.js?v=8.6.13 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Thu, 17 Jan 2019 12:58:11 GMT

...
```

Issue 33 of 36

TOC

Query Parameter in SSL Request

Severity:	Low
CVSS Score:	5.0
URL:	https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/functions.js
Entity:	v (Parameter)
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Query parameters were passed over SSL, and may contain sensitive information
Fix:	Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /cppp8/sites/all/themes/cppp/js/custom/functions.js?v=8.6.13 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Fri, 09 Feb 2018 09:29:46 GMT

...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/themes/cppp8/js/custom/dncalendar.min.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /cppp8/sites/all/themes/cppp8/js/custom/dncalendar.min.js?v=8.6.13 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Mon, 06 Aug 2018 09:52:21 GMT
...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/themes/cppp8/js/custom/customcommon.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /cppp8/sites/all/themes/cppp/js/custom/customcommon.js?v=8.6.13 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Sat, 24 Nov 2018 10:53:26 GMT

...
```

Issue 36 of 36

TOC

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/c3.min.js>

Entity: v (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /cppp8/sites/all/themes/cppp/js/custom/c3.min.js?v=8.6.13 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Thu, 17 Jan 2019 12:57:57 GMT

...
```

Unsafe third-party link (target="_blank")**Severity:** Low**CVSS Score:** 5.0**URL:** <https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata/byVFdsdWFYTjBjbmtnYjJZZ1VtRnBiSGRoZVhNPUEXM2gxUld4bFkzUnlhV05oYkNCaGJtUWdUV0ZwYm5SbGJtRnVZMlVnVjI5eWEzTT1BMTNoMVltbGtYM04xWW0xcGMzTnBiMjVmWlc1a1pHRjBaUT09QTEzaDFkR1ZrZEE9PQ==>**Entity:** byVFdsdWFYTjBjbmtnYjJZZ1VtRnBiSGRoZVhNPUEXM2gxUld4bFkzUnlhV05oYkNCaGJtUWdUV0ZwYm5SbGJtRnVZMlVnVjI5eWEzTT1BMTNoMVltbGtYM04xWW0xcGMzTnBiMjVmWlc1a1pHRjBaUT09QTEzaDFkR1ZrZEE9PQ== (Page)**Risk:** It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.**Causes:** The rel attribute in the link element is not set to "noopener noreferrer".**Fix:** Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"**Reasoning:** The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object**Raw Test Response:**

```

...
<li class="first leaf menu-mlid-595"><a target="_blank" title="Unified Analytics"
href="https://eprocure.gov.in/eprocdashboard/conreport"> Unified
Analytics</a></li>

<li class="first leaf menu-mlid-595"><a target="_blank" title="Key Performance Indicators"
href="https://eprocure.gov.in/eprocdashboard/index"> Key
Performance Indicators</a></li>

<li class="first leaf menu-mlid-595"><a target="_blank" title="Descriptive Analytics"
href="https://eprocure.gov.in/eprocdashboard/dashbd1">
Descriptive Analytics</a></li>
...

...
.../newwindow_external.gif" alt = " New Window External"></a></li>
<li class="first leaf menu-mlid-595"><a target="_blank" href="http://goidirectory.gov.in "
title="Government of India Web Directory : External Website that opens in a new window">GoI
Directory&nbsp;
<ul>
<li><a target="_blank" href="http://www.digitalindia.gov.in"><img title="Digital India (External
Site that opens in a new wi...
```

...

Unsafe third-party link (target="_blank")

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata>

Entity: cpppdata (Page)

Risk: It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: The rel attribute in the link element is not set to "noopener noreferrer".

Fix: Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Raw Test Response:

```
...

<li class="first leaf menu-mlid-595"><a target="_blank" title="Unified Analytics"
href="https://eprocure.gov.in/eprocdashboard/conreport"> Unified
Analytics</a></li>

<li class="first leaf menu-mlid-595"><a target="_blank" title="Key Performance Indicators"
href="https://eprocure.gov.in/eprocdashboard/index"> Key
Performance Indicators</a></li>

<li class="first leaf menu-mlid-595"><a target="_blank" title="Descriptive Analytics"
href="https://eprocure.gov.in/eprocdashboard/dashbd1">
Descriptive Analytics</a></li>
...

.../newwindow_external.gif" alt = " New Window External"></a></li>
<li class="first leaf menu-mlid-595"><a target="_blank" href="http://goidirectory.gov.in "
title="Government of India Web Directory : External Website that opens in a new window">GoI
Directory&nbsp;
<ul>
<li><a target="_blank" href="http://www.digitalindia.gov.in"><img title="Digital India (External
Site that opens in a new wi...

...
```

Unsafe third-party link (target="_blank")**Severity:** Low**CVSS Score:** 5.0**URL:** <https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata>**Entity:** cpppdata (Page)**Risk:** It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.**Causes:** The rel attribute in the link element is not set to "noopener noreferrer".**Fix:** Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Raw Test Response:

```
...

<li class="first leaf menu-mlid-595"><a target="_blank" title="Unified Analytics"
href="https://eprocure.gov.in/eprocdashboard/conreport"> Unified
Analytics</a></li>

<li class="first leaf menu-mlid-595"><a target="_blank" title="Key Performance Indicators"
href="https://eprocure.gov.in/eprocdashboard/index"> Key
Performance Indicators</a></li>

<li class="first leaf menu-mlid-595"><a target="_blank" title="Descriptive Analytics"
href="https://eprocure.gov.in/eprocdashboard/dashbdl">
Descriptive Analytics</a></li>
...

...
.../newwindow_external.gif" alt = " New Window External"></a></li>
<li class="first leaf menu-mlid-595"><a target="_blank" href="http://goirectory.gov.in "
title="Government of India Web Directory : External Website that opens in a new window">GoI
Directory&nbsp;
<ul>
<li><a target="_blank" href="http://www.digitalindia.gov.in"><img title="Digital India (External
Site that opens in a new wi...

...
```

Unsafe third-party link (target="_blank")**Severity:** Low**CVSS Score:** 5.0**URL:** <https://164.100.129.63/cppp8/latestactivecorrigendumsnew>**Entity:** latestactivecorrigendumsnew (Page)**Risk:** It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.**Causes:** The rel attribute in the link element is not set to "noopener noreferrer".**Fix:** Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"**Reasoning:** The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object**Raw Test Response:**

```

...
<li class="first leaf menu-mlid-595"><a target="_blank" title="Unified Analytics"
href="https://eprocure.gov.in/eprocdashboard/conreport"> Unified
Analytics</a></li>

<li class="first leaf menu-mlid-595"><a target="_blank" title="Key Performance Indicators"
href="https://eprocure.gov.in/eprocdashboard/index"> Key
Performance Indicators</a></li>

<li class="first leaf menu-mlid-595"><a target=" blank" title="Descriptive Analytics"
href="https://eprocure.gov.in/eprocdashboard/dashbd1">
Descriptive Analytics</a></li>
...

...
.../newwindow_external.gif" alt = " New Window External"></a></li>
<li class="first leaf menu-mlid-595"><a target="_blank" href="http://goidirectory.gov.in "
title="Government of India Web Directory : External Website that opens in a new window">GoI
Directory&nbsp;
<ul>
<li><a target="_blank" href="http://www.digitalindia.gov.in"><img title="Digital India (External
Site that opens in a new wi...

...

```


Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	https://164.100.129.63/cppp8/latestactivetendersnew
Entity:	latestactivetendersnew (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target=" blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Raw Test Response:

```

...
<li class="first leaf menu-mlid-595"><a target="_blank" title="Unified Analytics"
href="https://eprocure.gov.in/eprocdashboard/conreport"> Unified
Analytics</a></li>

<li class="first leaf menu-mlid-595"><a target="_blank" title="Key Performance Indicators"
href="https://eprocure.gov.in/eprocdashboard/index"> Key
Performance Indicators</a></li>

<li class="first leaf menu-mlid-595"><a target="_blank" title="Descriptive Analytics"
href="https://eprocure.gov.in/eprocdashboard/dashbdl1">
Descriptive Analytics</a></li>
...
...
.../newwindow_external.gif" alt = " New Window External"></a></li>
<li class="first leaf menu-mlid-595"><a target="_blank" href="http://goindirectory.gov.in"
title="Government of India Web Directory : External Website that opens in a new window">GoI
Directory&nbsp;
<ul>
<li><a target="_blank" href="http://www.digitalindia.gov.in"><img title="Digital India (External
Site that opens in a new wi...

...

```

Unsafe third-party link (target="_blank")

Severity: **Low**

CVSS Score: 5.0

URL: <https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata/byUTJWdWRISmhiQ0JRZFdKc2FXTWdWMjl5YTNNZ1JHVndZWEowYldWdWRDQW9RMUJYUkNrPUExM2gxUTJsMmFXd2dWMjl5YTNNPUExM2gxWW1sa1gzTjFZbTFwYzNOcGlyNWZaVzVrWkdGMFpRPT1BMTNoMWRl bDA=>

Entity: byUTJWdWRISmhiQ0JRZFdKc2FXTWdWMjl5YTNNZ1JHVndZWEowYldWdWRDQW9RMUJYUkNrPUExM2gxUTJsMmFXd2dWMjl5YTNNPUExM2gxWW1sa1gzTjFZbTFwYzNOcGlyNWZaVzVrWkdGMFpRPT1BMTNoMWRl bDA= (Page)

Risk: It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: The rel attribute in the link element is not set to "noopener noreferrer".

Fix: Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Raw Test Response:

```
...

<li class="first leaf menu-mlid-595"><a target="_blank" title="Unified Analytics"
href="https://eprocure.gov.in/eprocdashboard/conreport"> Unified
Analytics</a></li>

<li class="first leaf menu-mlid-595"><a target="_blank" title="Key Performance Indicators"
href="https://eprocure.gov.in/eprocdashboard/index"> Key
Performance Indicators</a></li>

<li class="first leaf menu-mlid-595"><a target="_blank" title="Descriptive Analytics"
href="https://eprocure.gov.in/eprocdashboard/dashbd1">
Descriptive Analytics</a></li>
...

.../newwindow_external.gif" alt = " New Window External"></a></li>
<li class="first leaf menu-mlid-595"><a target="_blank" href="http://goindirectory.gov.in "
title="Government of India Web Directory : External Website that opens in a new window">GoI
Directory&nbsp;
<ul>
<li><a target="_blank" href="http://www.digitalindia.gov.in"><img title="Digital India (External
Site that opens in a new wi...

...
```

Issue 1 of 1

TOC

Application Error**Severity:** Informational**CVSS Score:** 0.0**URL:** <https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata>**Entity:** s_short (Parameter)**Risk:** It is possible to gather sensitive debugging information**Causes:** Proper bounds checking were not performed on incoming parameter values
No validation was done in order to make sure that user input matches the data type expected**Fix:** Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions**Reasoning:** The application has responded with an error message, indicating an undefined state that may expose sensitive information.**Raw Test Response:**

```

...
GET
/cppp8/latestactivecorrigendumsnew/cpppdata/byUTJWdWRISmhiQ0JRZFdKc2FXTWdWMj15YTNNZ1JHvndZWEowYld
WdWRDQW9RMUJYUkNrPUExM2gxUTJsMmFXd2dWMj15YTNNPUExM2gxQTEzaDFkSGww HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Referer: https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata
Cookie: cookieWorked=yes;
SSESS196b5fb0ea7cfdca9bfef1c5ca51a493=7QUXgoUc6yrlGytrAROpGbSurw5PuAmUQq8WhxtGroo;
li=https%3A%2F%2F164.100.129.63%2Fcppp8%2Fatestactivecorrigendumsnew
Host: 164.100.129.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.0 500 500 Service unavailable (with message)
Connection: close
X-XSS-Protection: 1; mode=block
Server: Apache
Access-Control-Max-Age: 1000
Access-Control-Allow-Origin: eprocure.gov.in
Content-Length: 74
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
...

```

Application Test Script Detected

Severity:	Informational
CVSS Score:	0.0
URL:	https://164.100.129.63/cppp8/
Entity:	test (Page)
Risk:	It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords
Causes:	Temporary files were left in production environment
Fix:	Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

...

Referer: https://164.100.129.63/
Cookie: cookieWorked=yes; SSESS1
96b5fb0ea7cfdca9bfef1c5ca51a493=
7QUXgoUc6yrlGytrAROpGbSurw5PuAmU
Qq8WhxtGroo
Connection: keep-alive
Host: 164.100.129.63
X-Requested-With: XMLHttpRequest
Accept: /*/*
Accept-Language: en-US,en;q=0.5

HTTP/1.1 200 OK
Expires: Sun, 19 Nov 1978 05:00:
00 GMT
Vary:
Content-Security-Policy: default
-src *; style-src 'self' 'unsafe
-inline'; script-src 'self' 'uns
afe-inline' 'unsafe-eval'
Access-Control-Allow-Methods: PO
ST, GET
X-XSS-Protection: 1; mode=block
Keep-Alive: timeout=5, max=35
X-Frame-Options: DENY
X-Frame-Options: SAMEORIGIN
Link: <https://164.100.129.63/cp
pp8/test>; rel="alternate"; href
lang="en"

...

...
000/01/rdf-schema# schema: http
://schema.org/ sioc: http://rdf
s.org/sioc/ns# sioc: http://rd
fs.org/sioc/types# skos: http:/
/www.w3.org/2004/02/skos/core#
xsd: http://www.w3.org/2001/XMLS
chema# ">
<head>
 <meta charset="utf-8" />
 <meta name="MobileOptimized" con
tent="width" />
 <meta name="HandheldFriendly" co
ntent="true" />
 <meta name="viewport" content="w
idth=device-width, initial-scale
=1" />
 <meta http-equiv="x-ua-compatibl
e" content="ie=edge" />
 <meta name="referrer" content="o
rigin" />
 <link rel="shortcut icon" href=" "
/cppp8/sites/default/files/favic
on.ico" type="image/vnd.microsof
t.icon" />
 <link rel="alternate" hreflang="

```

GET /cphp8/test HTTP/1.1
User-Agent: Mozilla/5.0 (Windows
NT 6.1; Win64; x64; rv:62.0) Gec
ko/20100101 Firefox/62.0
Referer: https://164.100.129.63/
Cookie: cookieWorked=yes; SSESS1
96b5fb0ea7cfdca9bfeffc5ca51a493=
7QUXgoUc6yrlGytrAROpGbSurw5PuAmU
Qq8WhxtGroo
Connection: keep-alive
Host: 164.100.129.63
X-Requested-With: XMLHttpRequest
Accept: */*
Accept-Language: en-US,en;q=0.5

```

```

en" href="https://164.100.129.63
/cphp8/test" />
<link rel="canonical" href="/cphp
8/test" />
<link rel="shortlink" href="/cphp
8/node/1" />
<link rel="revision" href="/cphp
8/test" />

```

```

<title>Test | Tenders Portal
of Government of India | Governm
ent eTenders</title>

```

```

<style media="all">
@import url("/cphp8/core/assets/
vendor/normalize-css/normalize.c
ss?ppn28w");
@import url("/cphp8/core/misc/no
rmalize-fixes.css?ppn28w");
@import url("/cphp8/core/themes/
stable/css/system/components/aja
x-progress.module.css?ppn28w");
@import url("/cphp8/core/themes/
stable/css/system/components/ali
gn.module.css?ppn28w");
@import url("/cphp8/core/themes/
stable/css/system/components/aut
ocomplete-loading.module.css?ppn
28w");
@import url("/cphp8/core/themes/
stable/css/system/components/fie
ldgroup.module.css?ppn28w");
@import url("/cphp8/core/themes/
stable/css/system/components/con
tainer-inline.module.css?ppn28w"
);
@import url("/cphp8/core/themes/
stable/css/system/components/cle
arfix.module.css?ppn28w");
...
...

```

```

<li class="first expanded active
menu-mlid-1232"><a href="https:/
/164.100.129.63/cphp8/latestacti
vetendersnew"> Latest Active Tenders</a></l
i>

```

```

<li class="first expanded active
menu-mlid-1232"><a href="https:/
/164.100.129.63/cphp8/latestacti
vecorrigendumsnew"> Active Corrigendums</a>

```

```

</li>
...

...

    <div class="region region-content">

<div id="block-cppp-page-title"
class="block block-core block-page-title-block">

    <div class="content">

        <h1 class="page-title"><span property="schema:name" class="field field--name-title field--type-string field--label-hidden">Test</span>
</h1>

    </div>
</div>
<div id="block-cppp-content" class="block block-system block-system-main-block">

    <div class="content">

<article data-history-node-id="1" role="article" about="/cppp8/test" typeof="schema:Article" class="node node--type-article node--view-mode-full clearfix">
    <header>

        <span property="schema:name" content="Test" class="rdf-meta hidden"></span>
        <span property="schema:interactionCount" content="UserComments:0" class="rdf-meta hidden"></span>
        ...
        ...

    <div class="node__content clearfix">

        <div property="schema:text" class="clearfix text-formatted field field--name-body field--type-text-with-summary field--label-hidden field__item"><h3 align="center">XML REST TEST - DEMO</h3></div>
        <section rel="schema:comment"

```

```
nt" class="field field--name-comment field--type-comment field--label-hidden comment-wrapper">
```

```
...
```

```
...
```

```
<script src="/cppp8/core/assets/vendo...
```

I Client-Side (JavaScript) Cookie References 1

TOC

Issue 1 of 1

TOC

Client-Side (JavaScript) Cookie References

Severity: Informational

CVSS Score: 0.0

URL: <https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/functions.js>

Entity: var \$ = jQuery; (Page)

Risk: The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side

Causes: Cookies are created at the client side

Fix: Remove business and security logic from the client side

Reasoning: AppScan found a reference to cookies in the JavaScript.

Original Response

```
...
var a=c;if(t==0)return b;if((t/d)==1)return b+c;if(!p)p=d*0.3;if(a<Math.abs(c)){a=c;var
s=p/4}else var s=p/(2*Math.PI)*Math.asin(c/a);return a*Math.pow(2,-10*t)*Math.sin((t*d-s)*
(2*Math.PI)/p)+c+b},e...

/*! jquery.cookie v1.4.1 | MIT */
jQuery.cookie=function(name,value,options){if(typeof value!='undefined'){options=options||
{};if(value===null){value='';options=options||{};options.expires=...

//jQuery.marquee
(function(){var e=jQuery,f="jQuery.pause",d=1,b=e.fn.animate,a={};function c(){return new
Date().getTime()}e.fn.animate=function(k,h,j,i){var g=e.speed(h,j,i);g.complete=g.old;return
this.each(function()

...
...

```



```

1.70158;return c*(t/=d)*t*((s+1)*t-s)+b},easeOutBack:function(x,t,b,c,d,s)
{if(s==undefined)s=1.70158;return c*((t=t/d-1)*t*
((s+1)*t+s)+1)+b},easeInOutBack:function(x,t,b,c,d,s){if(s==undefined)s=1.701...

/*! jquery.cookie v1.4.1 | MIT */
...main=options.domain?'; domain='+options.domain:'';var secure=options.secure?';
secure:'';document.cookie=
[name,'',encodeURIComponent(value),expires,path,domain,secure].join('');}else{var
cookieValue=null;i...

//jQuery.marquee
(function(){var e=jQuery,f="jQuery.pause",d=1,b=e.fn.animate,a={};function c(){return new
Date().getTime()}e.fn.animate=function(k,h,j,i){var g=e.speed(h,j,i);g.complete=g.old;return
this.each(function...

...

...
g=d("style");0!==g.length?g.filter(":last").append(f):d("head").append("<style>"+f+"
</style>");B(c[0],"AnimationIteration",function()
{b.trigger("finished")});B(c[0],"AnimationEnd",function(){v();b.tri...
g.pause);b.bind("resume",g.resume);a.pauseOnHover&&b.bind("mouseenter
mouseleave",g.toggle);e&&a.allowCss3Support?
v():b.timer=setTimeout(v,a.delayBeforeStart)}});d.fn.marquee.defaults={allowCss3Suppo...

// Access Script

...tTime(expireDate.getTime()+days*24*60*60*1E3);expires="";
expires="+expireDate.toGMTString()}document.cookie=name+"="+value+expires+";
path=/"},read:function(name){var nameEQ=name+"=";var ca=document.cookie.spl...

...

```

I Integer Overflow 2

TOC

Issue 1 of 2

TOC

Integer Overflow

Severity: Informational

CVSS Score: 0.0

URL: <https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata>

Entity: captcha_sid (Parameter)

Risk: It is possible to gather sensitive debugging information

Causes: Proper bounds checking were not performed on incoming parameter values
No validation was done in order to make sure that user input matches the data type expected

Fix: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that

Raw Test Response:

Issue 2 of 2

Integer Overflow

CVSS Score: 0.0

Entity: captcha_sid (Parameter)

Causes: Proper bounds checking were not performed on incoming parameter values
No validation was done in order to make sure that user input matches the data type expected

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Raw Test Response:

4/9/2019

```
HTTP/1.1 500 500 Service unavailable (with message)
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Content-Length: 68
Content-language: en
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept,
client-security-token
Server: Apache
X-Frame-Options: DENY
X-Frame-Options: SAMEORIGIN
Access-Control-Allow-Methods: POST, GET
Access-Control-Max-Age: 1000
```

98

Application Data

Visited URLs 51

TOC

URL
https://164.100.129.63/cppp8/sites/default/files/dashboard_json/active_json_data.json
https://164.100.129.63/cppp8/sites/default/files/dashboard_json/open_json_data.json
https://164.100.129.63/cppp8/sites/default/files/dashboard_json/close_json_data.json
https://164.100.129.63/cppp8/sites/default/files/dashboard_json/totorg_json_data.json
https://164.100.129.63/cppp8/latestactivetendersnew
https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata
https://164.100.129.63/cppp8/latestactivecorrigendumsnew
https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata
https://164.100.129.63/cppp8/core/assets/vendor/domready/ready.min.js?v=1.0.8
https://164.100.129.63/cppp8/core/assets/vendor/jquery/jquery.min.js?v=3.2.1
https://164.100.129.63/cppp8/core/misc/drupalSettingsLoader.js?v=8.6.13
https://164.100.129.63/cppp8/core/misc/drupal.js?v=8.6.13
https://164.100.129.63/cppp8/core/misc/drupal.init.js?v=8.6.13
https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/data-min.js?v=1.12.1
https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/disable-selection-min.js?v=1.12.1
https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/form-min.js?v=1.12.1
https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/labels-min.js?v=1.12.1
https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/jquery-1-7-min.js?v=1.12.1
https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/scroll-parent-min.js?v=1.12.1
https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/tabbable-min.js?v=1.12.1
https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/unique-id-min.js?v=1.12.1
https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/version-min.js?v=1.12.1
https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/focusable-min.js?v=1.12.1
https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/ie-min.js?v=1.12.1
https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/keycode-min.js?v=1.12.1
https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/plugin-min.js?v=1.12.1
https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/safe-active-element-min.js?v=1.12.1
https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/safe-blur-min.js?v=1.12.1
https://164.100.129.63/cppp8/core/modules/locale/locale.datepicker.js?v=8.6.13
https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/widgets/datepicker-min.js?v=1.12.1
https://164.100.129.63/cppp8/sites/all/themes/cppp/bootstrap/js/bootstrap.min.js?v=8.6.13

<https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/toggle.js?v=8.6.13>
<https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/functions.js?v=8.6.13>
<https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/general.js?v=8.6.13>
<https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/customcommon.js?v=8.6.13>
<https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/dncalendar.min.js?v=8.6.13>
https://164.100.129.63/cppp8/sites/default/files/orgname_json/orgname_json_data.json
https://164.100.129.63/cppp8/sites/default/files/dashboard_json/active_json_data.json
https://164.100.129.63/cppp8/sites/default/files/dashboard_json/open_json_data.json
https://164.100.129.63/cppp8/sites/default/files/dashboard_json/close_json_data.json
https://164.100.129.63/cppp8/sites/default/files/dashboard_json/totorg_json_data.json
<https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata>
<https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/c3.min.js?v=8.6.13>
<https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata>
<https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/d3.min.js?v=8.6.13>
<https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/jquery.base64.min.js?v=8.6.13>
<https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/pako.min.js?v=8.6.13>
<https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/c3chartslider.js?v=8.6.13>
<https://164.100.129.63/cppp8/sites/all/modules/appmodules/testmodules/latestactivecorrigendumsnew/js/latestactivecorrigendumsnew.js?v=8.6.13>
<https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/to-top.js?v=8.6.13>
<https://164.100.129.63/cppp8/sites/all/modules/appmodules/testmodules/latestactivetendersnew/js/latestactivetendersnew.js?v=8.6.13>

Parameters 54

TOC

Name	Value	URL	Type
v	1.12.1	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/version-min.js?v=1.12.1	Simple Link
op	Search	https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata	Submit
v	8.6.13	https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/c3chartslider.js?v=8.6.13	Simple Link
v	1.12.1	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/focusable-min.js?v=1.12.1	Simple Link
s_pro d_type	Electrical+and+Maintenance +Works	https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata	Select
v	8.6.13	https://164.100.129.63/cppp8/core/modules/locale/locale.datepicker.js?v=8.6.13	Simple Link
v	1.12.1	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/safe-active-element-min.js?v=1.12.1	Simple Link
v	1.12.1	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/ie-min.js?v=1.12.1	Simple Link
s_key word	tyt	https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata	Text

form_id	latestactivetendersnew_form	https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata	Hidden
v	1.12.1	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/scroll-parent-min.js?v=1.12.1	Simple Link
v	1.12.1	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/widgets/datepicker-min.js?v=1.12.1	Simple Link
v	8.6.13	https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/toggle.js?v=8.6.13	Simple Link
s_state	Ministry+of+Railways	https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata	Select
v	8.6.13	https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/to-top.js?v=8.6.13	Simple Link
v	8.6.13	https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/customcommon.js?v=8.6.13	Simple Link
form_id	latestactivecorrigendumsnew_form	https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata	Hidden
v	1.12.1	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/keycode-min.js?v=1.12.1	Simple Link
v	8.6.13	https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/functions.js?v=8.6.13	Simple Link
v	8.6.13	https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/dncalendar.min.js?v=8.6.13	Simple Link
s_short	bid_submission_enddate	https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata	Select
v	1.12.1	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/jquery-1-7-min.js?v=1.12.1	Simple Link
v	8.6.13	https://164.100.129.63/cppp8/sites/all/themes/cppp/bootstrap/js/bootstrap.min.js?v=8.6.13	Simple Link
v	1.12.1	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/safe-bur-min.js?v=1.12.1	Simple Link
v	1.12.1	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/labels-min.js?v=1.12.1	Simple Link
s_key word	tedt	https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata	Text
v	8.6.13	https://164.100.129.63/cppp8/core/misc/drupal.js?v=8.6.13	Simple Link
v	8.6.13	https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/d3.min.js?v=8.6.13	Simple Link
v	8.6.13	https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/pako.min.js?v=8.6.13	Simple Link
op	Search	https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata	Submit
v	8.6.13	https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/gener-al.js?v=8.6.13	Simple Link
v	1.0.8	https://164.100.129.63/cppp8/core/assets/vendor/domready/ready.min.js?v=1.0.8	Simple Link
v	1.12.1	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/plugin-min.js?v=1.12.1	Simple Link
form_build_id	form-a-m6tuAMfWM6EGrFGNRPVn0pBZI7bslwNeGF8QFzhtc	https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata	Hidden
captcha_tok	f4c93648d719bce43cbbb6038dbd9e8d	https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata	Hidden

en			
s_pro d_typ e	Civil+Works	https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppda ta	Select
capth a_sid	407132	https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata	Hidden
v	8.6.13	https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/jquery. base64.min.js?v=8.6.13	Simple Link
v	1.12.1	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/disabl e-selection-min.js?v=1.12.1	Simple Link
capth a_tok en	bcea58a47b78f83b2e52dbaf 45a2fa7c	https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata	Hidden
v	3.2.1	https://164.100.129.63/cppp8/core/assets/vendor/jquery/jquery.min. js?v=3.2.1	Simple Link
s_sho rt	bid_submission_enddate	https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppda ta	Select
v	1.12.1	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/tabb le-min.js?v=1.12.1	Simple Link
capth a_sid	407134	https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppda ta	Hidden
v	8.6.13	https://164.100.129.63/cppp8/sites/all/modules/appmodules/testmo dules/latestactivecorrigendumsnew/js/latestactivecorrigendumsnew .js?v=8.6.13	Simple Link
v	8.6.13	https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/c3.mi n.js?v=8.6.13	Simple Link
v	1.12.1	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/uniqu e-id-min.js?v=1.12.1	Simple Link
v	1.12.1	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/form- min.js?v=1.12.1	Simple Link
s_stat e	Central+Public+Works+Depa rtment+(CPWD)	https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppda ta	Select
v	1.12.1	https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/data- min.js?v=1.12.1	Simple Link
form_ build_ id	form-1UmuarvT81MUIHHUo 4reW2XEhGjA6Qoc8gNVGo HNmRk	https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata	Hidden
v	8.6.13	https://164.100.129.63/cppp8/core/misc/drupalSettingsLoader.js?v= 8.6.13	Simple Link
v	8.6.13	https://164.100.129.63/cppp8/core/misc/drupal.init.js?v=8.6.13	Simple Link
v	8.6.13	https://164.100.129.63/cppp8/sites/all/modules/appmodules/testmo dules/latestactivetendersnew/js/latestactivetendersnew.js?v=8.6.13	Simple Link

Failed Requests 1

TOC

URL	Reason
https://164.100.129.63/cppp8/latestactivetendernew	Response Status '404' - Not Found

Filtered URLs 90

TOC

URL	Reason
https://164.100.129.63/cppp8/sites/default/files/favicon.ico	File Extension
https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata	Likely Similar DOM
https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata/byVFdsdWFYTjBjbmtnYjJZZ1VtRnBiSGRoZVhNPUEXm2gxUld4bFkzUnlhV05oYkNCaGJtUWdUV0ZwYm5SbGJtRnVZMIVnVjl5eWEzTT1BMTNoMVIbGtYM04xWW0xcGMzTnBiMjVmWlc1a1pHRjBaUT09QTEzaDFkR1ZrZEE9PQ==	Similar Body
https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata/byUTJWdWRISmhiQ0JRZFdKc2FXTWdWMjl5YTNNZ1JHVndZWEowYldWdWRDQW9RMUJYUkNrPUExM2gxUTJsMmFXd2dWMjl5YTNPUExM2gxWW1sa1gzTjFZbTFwYzNOcGlyNWZaVzVrWkdGMFpRPT1BMTNoMWRibDA=	Similar Body
https://164.100.129.63/cppp8/sites/default/files/logo/logo.png	File Extension
https://164.100.129.63/cppp8/sites/default/files/images/rightarrow6.png	File Extension
https://164.100.129.63/cppp8/sites/default/files/images/new1.gif	File Extension
https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata/byUTJWdWRISmhiQ0JRZFdKc2FXTWdWMjl5YTNNZ1JHVndZWEowYldWdWRDQW9RMUJYUkNrPUExM2gxUTJsMmFXd2dWMjl5YTNPUExM2gxWW1sa1gzTjFZbTFwYzNOcGlyNWZaVzVrWkdGMFpRPT1BMTNoMWRibDA=	Likely Similar DOM
https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata	Likely Similar DOM
https://164.100.129.63/cppp8/sites/default/files/images/newwindow_external.gif	File Extension
https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata/byVFdsdWFYTjBjbmtnYjJZZ1VtRnBiSGRoZVhNPUEXm2gxUld4bFkzUnlhV05oYkNCaGJtUWdUV0ZwYm5SbGJtRnVZMIVnVjl5eWEzTT1BMTNoMVIbGtYM04xWW0xcGMzTnBiMjVmWlc1a1pHRjBaUT09QTEzaDFkR1ZrZEE9PQ==	Likely Similar DOM
https://164.100.129.63/cppp8/sites/default/files/images/pdf_icon.gif	File Extension
https://164.100.129.63/cppp8/sites/default/files/images/newwindow_icon.gif	File Extension
https://164.100.129.63/cppp8/sites/default/files/eproc/OrgnUsing-eProcurement.pdf	File Extension
https://164.100.129.63/cppp8/sites/default/files/eproc/CPPP_Overview.pdf	File Extension
https://164.100.129.63/cppp8/sites/default/files/images/newgifImage.gif	File Extension
https://164.100.129.63/cppp8/sites/default/files/eproc/XMLStepbyStepDocument.pdf	File Extension
https://164.100.129.63/cppp8/sites/default/files/eproc/CPPP-FAQs.pdf	File Extension
https://164.100.129.63/cppp8/sites/all/libraries/homepage/nic-logo.png	File Extension
https://164.100.129.63/cppp8/sites/default/images/cppp_qr.png	File

	Extension
https://164.100.129.63/cppp8/sites/all/libraries/homepage/footerlogo/digital-india-logo.png	File Extension
https://164.100.129.63/cppp8/sites/all/libraries/homepage/footerlogo/gemgov-footer-logo.png	File Extension
https://164.100.129.63/cppp8/sites/all/libraries/homepage/footerlogo/india-gov-logo.png	File Extension
https://164.100.129.63/cppp8/sites/all/libraries/homepage/footerlogo/data-gov-logo.png	File Extension
https://164.100.129.63/cppp8/sites/all/libraries/homepage/footerlogo/Meity_logo.png	File Extension
https://164.100.129.63/cppp8/sites/all/libraries/homepage/footerlogo/cpgrams_logo.png	File Extension
https://164.100.129.63/cppp8/sites/all/libraries/homepage/footerlogo/gandhi_logo.png	File Extension
https://164.100.129.63/cppp8/core/assets/vendor/normalize-css/normalize.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/misc/normalize-fixes.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/stable/css/system/components/ajax-progress.module.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/stable/css/system/components/align.module.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/stable/css/system/components/autocomplete-loading.module.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/stable/css/system/components/fieldgroup.module.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/stable/css/system/components/container-inline.module.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/stable/css/system/components/clearfix.module.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/stable/css/system/components/details.module.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/stable/css/system/components/hidden.module.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/stable/css/system/components/item-list.module.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/stable/css/system/components/js.module.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/stable/css/system/components/nowrap.module.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/stable/css/system/components/position-container.module.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/stable/css/system/components/progress.module.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/stable/css/system/components/reset-appearance.module.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/stable/css/system/components/resize.module.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/stable/css/system/components/sticky-header.module.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/stable/css/system/components/system-status-counter.css?ppn28w	File

pn28w	Extension
https://164.100.129.63/cppp8/core/themes/stable/css/system/components/system-status-report-counter.s.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/stable/css/system/components/system-status-report-general-info.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/stable/css/system/components/abledrag.module.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/stable/css/system/components/ablesort.module.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/stable/css/system/components/tree-child.module.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/themes/base/core.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/themes/base/datepicker.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/themes/base/theme.css?ppn28w	File Extension
https://164.100.129.63/cppp8/sites/all/modules/appmodules/testmodules/latestactivecorrigendumsnew/css/latestactivecorrigendumsnew.css?ppn28w	File Extension
https://164.100.129.63/cppp8/sites/all/themes/cppp/bootstrap/css/bootstrap.min.css?ppn28w	File Extension
https://164.100.129.63/cppp8/sites/all/modules/appmodules/testmodules/latestactivetendersnew/css/latestactivetendersnew.css?ppn28w	File Extension
https://164.100.129.63/cppp8/sites/all/themes/cppp/css/base/customstyle.css?ppn28w	File Extension
https://164.100.129.63/cppp8/sites/all/themes/cppp/css/base/responsive.css?ppn28w	File Extension
https://164.100.129.63/cppp8/sites/all/themes/cppp/css/base/print.css?ppn28w	File Extension
https://164.100.129.63/cppp8/sites/all/themes/cppp/css/base/style.css?ppn28w	File Extension
https://164.100.129.63/cppp8/sites/all/themes/cppp/css/base/colors.css?ppn28w	File Extension
https://164.100.129.63/cppp8/sites/all/themes/cppp/css/base/local.css?ppn28w	File Extension
https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/css/animate.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/classy/css/components/action-links.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/classy/css/components/breadcrumb.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/classy/css/components/button.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/classy/css/components/collapse-processed.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/classy/css/components/container-inline.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/classy/css/components/details.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/classy/css/components/exposed-filters.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/classy/css/components/field.css?ppn28w	File

	Extension
https://164.100.129.63/cppp8/core/themes/classy/css/components/form.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/classy/css/components/icons.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/classy/css/components/inline-form.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/classy/css/components/item-list.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/classy/css/components/link.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/classy/css/components/links.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/classy/css/components/menu.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/classy/css/components/more-link.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/classy/css/components/pager.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/classy/css/components/abledrag.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/classy/css/components/tableselect.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/classy/css/components/tablesort.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/classy/css/components/tabs.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/classy/css/components/textarea.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/classy/css/components/ui-dialog.css?ppn28w	File Extension
https://164.100.129.63/cppp8/core/themes/classy/css/components/messages.css?ppn28w	File Extension
https://164.100.129.63/cppp8/sites/all/themes/cppp/css/components/primary-menu.css?ppn28w	File Extension
https://164.100.129.63/cppp8/sites/all/themes/cppp/css/components/to-top.css?ppn28w	File Extension

Comments 37

[TOC](#)

URL	Comment
https://164.100.129.63/cppp8/latestactivetender snew/cpppdata	[if lte IE 8]> <script src="/cppp8/core/assets/vendor/html5shiv/html5shiv.min.js? v=3.7.3"></script> <![endif]
https://164.100.129.63/cppp8/latestactivetender snew/cpppdata	#header-top

https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	#header-top-inside
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	#header-top-right
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	EOF:#header-top-right
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	EOF: #header-top-inside
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	EOF: #header-top
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	header
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	#header-inside
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	EOF: #header-inside
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	EOF: #header
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	#main-navigation
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	#main-navigation-inside
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	EOF: #main-navigation-inside
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	EOF: #main-navigation
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	#page
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	#top-content
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	#top-content-inside
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	EOF:#top-content-inside
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	EOF: #top-content
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	#main-content
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	#main
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	#breadcrumb
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	#breadcrumb-inside
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	EOF: #breadcrumb-inside
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	EOF: #breadcrumb
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	EOF:#content-wrapper
https://164.100.129.63/cppp8/latestactivetender snow/cpppdata	EOF:#main

https://164.100.129.63/cppp8/latestactivetender snew/cpppdata	EOF:#main-content
https://164.100.129.63/cppp8/latestactivetender snew/cpppdata	EOF:#page
https://164.100.129.63/cppp8/latestactivetender snew/cpppdata	#subfooter-inside
https://164.100.129.63/cppp8/latestactivetender snew/cpppdata	#subfooter-left
https://164.100.129.63/cppp8/latestactivetender snew/cpppdata	.widget-area
https://164.100.129.63/cppp8/latestactivetender snew/cpppdata	.sidebar-inner
https://164.100.129.63/cppp8/latestactivetender snew/cpppdata	EOF: #subfooter-left
https://164.100.129.63/cppp8/latestactivetender snew/cpppdata	EOF: #subfooter-inside
https://164.100.129.63/cppp8/latestactivetender snew/cpppdata	EOF:#subfooter

JavaScripts 44

TOC

URL / Code

https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata

```
{ "path":
{ "baseUrl": "\\cppp8\\", "scriptPath": null, "pathPrefix": "", "currentPath": "latestactivetendersnew\\cpppdata", "currentPathIsAdmin": false, "isFront": false, "currentLanguage": "en", "pluralDelimiter": "\u0003", "text_resize":
{ "text_resize_scope": "body", "text_resize_minimum": "10", "text_resize_maximum": "18", "text_resize_line_height_alow": "1", "text_resize_line_height_min": "16", "text_resize_line_height_max": "36", "jquery": { "ui": { "datepicker":
{ "isRTL": false, "firstDay": 0 } } }, "ajaxTrustedUrl":
{ "https://164.100.129.63form_action_p_pvdeGsVG5zNF_XLGPTvYSKCF43t8qZYSwcfZl2uzM": true }, "user":
{ "uid": 0, "permissionsHash": "4f7f379468396a4dddfa34f2750860619d85ec0d770edbec699ebc94e29929c5" } }
```

https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata

```
inputToHreffMani()
```

https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata

```
this.stop();
```

https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata

```
this.start();
```

<https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata>

```
btnSearch_Click()
```

<https://164.100.129.63/cppp8/core/assets/vendor/domready/ready.min.js>

```
/*!
 * domready (c) Dustin Diaz 2014 - License MIT
 */
!function(e,t){typeof module!="undefined"?module.exports=t():typeof define=="function"&&typeof define.amd=="object"?define(t):this[e]=t()}("domready",function(){var e=
[],t,n=document,r=n.documentElement,i="DOMContentLoaded",s=
(r?/^loaded|^c:/^loaded|^i|^c/).test(n.readyState);return s||n.addEventListener(i,t=function(){
n.removeEventListener(i,t),s=1;while(t=e.shift())t()},function(t){s?setTimeout(t,0):e.push(t)}))
```

<https://164.100.129.63/cppp8/core/assets/vendor/jquery/jquery.min.js>

```
/*! jQuery v3.2.1 | (c) JS Foundation and other contributors | jquery.org/license */
!function(a,b){"use strict";"object"===typeof module&&"object"===typeof module.exports?
module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a
document");return b(a)}:b(a)}("undefined"!==typeof window?window:this,function(a,b){"use strict";var c=
[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j=
{},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var
c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c);var
q="3.2.1",r=function(a,b){return new r.fn.init(a,b)},s=/^\s\uFFFF\uA0+|[\s\uFFFF\uA0]+$/g,t="/^ms-/,u=-
([a-z])/g,v=function(a,b){return b.toUpperCase()};r.fn=r.prototype=
{jquery:"q",constructor:r,length:0,toArray:function(){return f.call(this)},get:function(a){return null==a?
f.call(this):a<0?this[a+this.length]:this[a]},pushStack:function(a){var
b=r.merge(this.constructor(),a);return b.prevObject=this,b},each:function(a){return
r.each(this,a)},map:function(a){return this.pushStack(r.map(this,function(b,c){return
a.call(b,c,b)})),slice:function(){return this.pushStack(f.apply(this,arguments))},first:function(){return
this.eq(0)},last:function(){return this.eq(-1)},eq:function(a){var b=this.length,c=a+(a<0?b:0);return
this.pushStack(c>0&&c<b?[this[c]]:[])},end:function(){return
this.prevObject||this.constructor()},push:h,sort:c.sort,splice:c.splice,r.extend=r.fn.extend=function(){var
a,b,c,d,e,f,g=arguments[0]||[],h=1,i=arguments.length,j=1;for("boolean"===typeof g&&(j=g,g=arguments[h]||
{}),h++),"object"===typeof g||r.isFunction(g)||g===!0?h==i&&(g=this,h--):h<i;h++)if(null!=
(a=arguments[h]))for(b in a)c=g[b],d=a[b],g!==d&&(j&&d&&(r.isPlainObject(d)||r.isArray(d)))?(e=
(e=!1,f=c&&r.isArray(c)?c:[]):f=c&&r.isPlainObject(c)?c:[]),g[b]=r.extend(j,f,d):void 0!==d&&
(g[b]=d));return g},r.extend({expando:"jQuery"+
(q+Math.random()).replace(/\D/g,""),isReady:!0,error:function(a){throw new Error(a)},noop:function()
{}}),isFunction:function(a){return"function"===r.type(a)},isWindow:function(a){return
null!=a&&a===a.window},isNumeric:function(a){var b=r.type(a);return("number"===b||"string"===b)&&!isNaN(a-
parseFloat(a))},isPlainObject:function(a){var b,c;return!(!a||"[object Object]"!==k.call(a))&&(!b=e(a))||
(c=l.call(b,"constructor")&&b.constructor,"function"===typeof c&&m.call(c)===n)},isEmptyObject:function(a)
{var b;for(b in a)return!1;return!0},type:function(a){return null==a?"":a:"object"===typeof
a||"function"===typeof a?j[k.call(a)]||"object":typeof a},globalEval:function(a){p(a)},camelCase:function(a)
{return a.replace(t,"ms-").replace(u,v)},each:function(a,b){var c,d=0;if(w(a))
for(c=a.length;d<c;d++)if(b.call(a[d],d,a[d])===!1)break}else for(d in
a)if(b.call(a[d],d,a[d])===!1)break;return a},trim:function(a){return null==a?"":
(a+"").replace(s,"")},makeArray:function(a,b){var c=b||[];return null!=a&&(w(Object(a))?
r.merge(c,"string"===typeof a?[a]:a):h.call(c,a)),c},isArray:function(a,b,c){return null==b?-
1:i.call(b,a,c)},merge:function(a,b){for(var c=a.length,d=0,e=a.length;d<c;d++)a[d++]=b[d];return
a.length=e,a},grep:function(a,b,c){for(var d,e=
[],f=0,g=a.length,h=1;c?f++:d!=b(a[f],f),d!=h&&e.push(a[f]);return e},map:function(a,b,c){var d,e,f=0,h=
[];if(w(a))for(d=a.length;f<d;f++)e=b(a[f],f,c),null!=e&&h.push(e);else for(f in
a)e=b(a[f],f,c),null!=e&&h.push(e);return g.apply([],h)},guid:1,proxy:function(a,b){var
c,d,e;if("string"===typeof b&&(c=a[b],b=a,c),r.isFunction(a))return d=f.call(arguments,2),e=function()
{return
a.apply(b||this,d.concat(f.call(arguments)))},e.guid=a.guid||r.guid++,e,now:Date.now,support:o}),"fun
ction"===typeof Symbol&&(r.fn[Symbol.iterator]=c[Symbol.iterator]),r.each("Boolean Number String Function
Array Date RegExp Object Error Symbol".split(" "),function(a,b){j["[object
"+b+""]]=b.toLowerCase();function w(a){var b=!a&&"length"in
a&&a.length,c=r.type(a);return"function"!==c&&!r.isWindow(a)&&("array"===c||0===b||"number"===typeof
```

```

b&b>0&b-1 in a)}var x=function(a){var b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u="sizzle"+1*new
Date,v=a.document,w=0,x=0,y=ha(),z=ha(),A=ha(),B=function(a,b){return a===b&&(l!=0),0},C={}.hasOwnProperty,D=
[],E=D.pop,F=D.push,G=D.push,H=D.slice,I=function(a,b){for(var c=0,d=a.length;c<d;c++)if(a[c]===b)return
c;return-
1},J="checked|selected|async|autofocus|autoplay|controls|defer|disabled|hidden|ismap|loop|multiple|open|reado
nly|required|scoped",K="[\x20\t\r\n\f]",L="(?:\\\\.|[\\w-]|[^\\0-\\xa0])+",M="\\["+K+"*("+L+")(?:"+K+"*
([*^$|!~]?=)"+K+"*(?:'((?:\\\\.|[^\"]')*)'|\"((?:\\\\.|[^\"]'')*)\"|"+L+")|)"+K+"*\\\\)",N=":("+L+")(?:\\
((?:\\\\.|[^\"]')*)'|\"((?:\\\\.|[^\"]'')*)\"|)((?:\\\\.|[^\"]'')*)|"+K+"*\\\\)",O=new
RegExp(K+"+", "g"),P=new RegExp("^"+K+"+|((?:^|^[^\\\\\\\\])?(?:\\\\\\\\.)*"+K+"+$", "g"),Q=new
RegExp("^"+K+"+", "g"),R=new RegExp("^"+K+"*([>~]|"+K+"")"+K+"*"),S=new RegEx...

```

<https://164.100.129.63/cpp8/core/misc/drupalSettingsLoader.js>

```

/**
 * DO NOT EDIT THIS FILE.
 * See the following change record for more information,
 * https://www.drupal.org/node/2815083
 * @preserve
 */

(function () {
  var settingsElement = document.querySelector('head > script[type="application/json"][data-drupal-
selector="drupal-settings-json"], body > script[type="application/json"][data-drupal-selector="drupal-
settings-json"]');

  window.drupalSettings = {};

  if (settingsElement !== null) {
    window.drupalSettings = JSON.parse(settingsElement.textContent);
  }
})();

```

<https://164.100.129.63/cpp8/core/misc/drupal.js>

```

/**
 * DO NOT EDIT THIS FILE.
 * See the following change record for more information,
 * https://www.drupal.org/node/2815083
 * @preserve
 */

window.Drupal = { behaviors: {}, locale: {} };

(function (Drupal, drupalSettings, drupalTranslations) {
  Drupal.throwError = function (error) {
    setTimeout(function () {
      throw error;
    }, 0);
  };

  Drupal.attachBehaviors = function (context, settings) {
    context = context || document;
    settings = settings || drupalSettings;
    var behaviors = Drupal.behaviors;

    Object.keys(behaviors || {}).forEach(function (i) {
      if (typeof behaviors[i].attach === 'function') {
        try {
          behaviors[i].attach(context, settings);
        } catch (e) {
          Drupal.throwError(e);
        }
      }
    });
  };

  Drupal.detachBehaviors = function (context, settings, trigger) {
    context = context || document;
  };
})();

```

```

settings = settings || drupalSettings;
trigger = trigger || 'unload';
var behaviors = Drupal.behaviors;

Object.keys(behaviors || {}).forEach(function (i) {
  if (typeof behaviors[i].detach === 'function') {
    try {
      behaviors[i].detach(context, settings, trigger);
    } catch (e) {
      Drupal.throwError(e);
    }
  }
});
};

Drupal.checkPlain = function (str) {
  str = str.toString().replace(/&/g, '&amp;').replace(/</g, '&lt;').replace(/>/g, '&gt;').replace(/"/g,
  '&quot;').replace(/'/g, '&#39;');
  return str;
};

Drupal.formatString = function (str, args) {
  var processedArgs = {};

  Object.keys(args || {}).forEach(function (key) {
    switch (key.charAt(0)) {
      case '@':
        processedArgs[key] = Drupal.checkPlain(args[key]);
        break;

      case '!':
        processedArgs[key] = args[key];
        break;

      default:
        processedArgs[key] = Drupal.theme('placeholder', args[key]);
        break;
    }
  });

  return Drupal.stringReplace(str, processedArgs, null);
};

Drupal.stringReplace = function (str, args, keys) {
  if (str.length === 0) {
    return str;
  }

  if (!Array.isArray(keys)) {
    keys = Object.keys(args || {});
  }

  keys.sort(function (a, b) {
    return a.length - b.length;
  });

  if (keys.length === 0) {
    return str;
  }

  var key = keys.pop();
  var fragments = str.split(key);

  if (keys.length) {
    for (var i = 0; i < fragments.length; i++) {
      fragments[i] = Drupal.stringReplace(fragments[i], args, keys.slice(0));
    }
  }

  return fragments.join(args[key]);
};

Drupal.t = function (str, args, options) {
  options = options || {};
  options.context = options.context || '';

  if (typeof drupalTranslations !== 'undefined' && drupalTranslations.strings &&
  drupalTranslations.strings[options.context] && drupalTranslations.strings[options.context][str]) {

```



```

    str = drupalTranslations.strings[options.context][str];
  }

  if (args) {
    str = Drupal.formatString(str, args);
  }
  return str;
};

Drupal.url = function (path) {
  return drupalSettings.path.baseUrl + drupalSettings.path.pathPrefix + path;
};

Drupal.url.toAbsolute = function (url) {
  var urlParsingNode = document.createElement('a');

  try {
    url = decodeURIComponent(url);
  } catch (e) {}

  urlParsingNode.setAttribute('href', url);

  return urlParsingNode.cloneNode(false).href;
};

Drupal.url.isLocal = function (url) {
  var absoluteUrl = Drupal.url.toAbsolute(url);
  var protocol = window.location.protocol;

  if (protocol === 'http:' && absoluteUrl.indexOf('https:') === 0) {
    protocol = 'https:';
  }
  var baseUrl = protocol + '//' + window.location.host + drupalSettings.path.baseUrl.slice(0, -1);

  try {
    absoluteUrl = decodeURIComponent(absoluteUrl);
  } catch (e) {}
  try {
    baseUrl = decodeURIComponent(baseUrl);
  } catch (e) {}

  return absoluteUrl === baseUrl || absoluteUrl.indexOf(baseUrl + '/') === 0;
};

Drupal.formatPlural = function (count, singular, plural, args, options) {
  args = args || {};
  args['@count'] = count;

  var pluralDelimiter = drupalSettings.pluralDelimiter;
  var translations = Drupal.t(singular + pluralDelimiter + plural, args, options).split(pluralDelimiter);
  var index = 0;

  if (typeof drupalTranslations !== 'undefined' && drupalTranslations.pluralFormula) {
    index = count in drupalTranslations.pluralFormula ? drupalTranslations.pluralFormula[count] :
drupalTranslations.pluralFormula.default;
  } else if (args['@count'] !== 1) {
    index = 1;
  }

  return translations[index];
};

Drupal.encodePath = function (item) {
  return window.encodeURIComponent(item).replace(/%2F/g, '/');
};

Drupal.theme = function (func) {
  if (func in Drupal.theme) {
    var _Drupal$theme;

    for (var _len = arguments.length, args = Array(_len > 1 ? _len - 1 : 0), _key = 1; _key < _len; _key++)
    {
      args[_key] = arguments[_key];
    }
  }

```

<https://164.100.129.63/cppp8/core/misc/drupal.init.js>

```
/**
 * DO NOT EDIT THIS FILE.
 * See the following change record for more information,
 * https://www.drupal.org/node/2815083
 * @preserve
 **/

if (window.jQuery) {
  jQuery.noConflict();
}

document.documentElement.className += ' js';

(function (domready, Drupal, drupalSettings) {
  domready(function () {
    Drupal.attachBehaviors(document, drupalSettings);
  });
})(domready, Drupal, window.drupalSettings);
```

<https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/data-min.js>

```
/*! jQuery UI - v1.12.1 - 2017-03-31
 * http://jqueryui.com
 * Copyright jQuery Foundation and other contributors; Licensed */
!function(a){function b(c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z){return a.extend(a.expr[":"],{data:a.expr.createPseudo?a.expr.createPseudo(function(b){return function(c){return!!a.data(c,b)}}):function(b,c,d){return!!a.data(b,d[3])}})}(a)
```

<https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/disable-selection-min.js>

```
/*! jQuery UI - v1.12.1 - 2017-03-31
 * http://jqueryui.com
 * Copyright jQuery Foundation and other contributors; Licensed */
!function(a){function b(c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z){return a.fn.extend({disableSelection:function(){var a="onselectstart"in document.createElement("div")?"selectstart":"mousedown";return function(){return this.on(a+".ui-disableSelection",function(a){a.preventDefault()})}})}(),enableSelection:function(){return this.off(".ui-disableSelection")}})}(a)
```

<https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/form-min.js>

```
/*! jQuery UI - v1.12.1 - 2017-03-31
 * http://jqueryui.com
 * Copyright jQuery Foundation and other contributors; Licensed */
!function(a){function b(c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z){return a.fn.form=function(){return"string"==typeof this[0].form?this.closest("form"):a(this[0].form)}}(a)
```

<https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/labels-min.js>

```
/*! jQuery UI - v1.12.1 - 2017-03-31
 * http://jqueryui.com
 * Copyright jQuery Foundation and other contributors; Licensed */
!function(a){function b(c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z){return a.fn.labels=function(){var b,c,d,e,f;return this[0].labels&&this[0].labels.length?this.pushStack(this[0].labels):
```

<https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/jquery-1-7-min.js>

<https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/scroll-parent-min.js>

<https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/tabbable-min.js>

<https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/unique-id-min.js>

<https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/version-min.js>

<https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/focusable-min.js>

https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/ie-min.js

https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/keycode-min.js

<https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/plugin-min.js>

https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/safe-active-element-min.js

```

* http://jqueryui.com
* Copyright jQuery Foundation and other contributors; Licensed */
!function(a){"function"==typeof define&&define.amd?define(["jquery","../version"],a):a(jQuery)}(function(a){
{return a.ui.safeActiveElement=function(a){var b;try{b=a.activeElement}catch(c){b=a.body}return b||
(b=a.body),b.nodeName|| (b=a.body),b)}});

```

<https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/safe-blur-min.js>

```

/! jQuery UI - v1.12.1 - 2017-03-31
* http://jqueryui.com
* Copyright jQuery Foundation and other contributors; Licensed */
!function(a){"function"==typeof define&&define.amd?define(["jquery","../version"],a):a(jQuery)}(function(a){
{return a.ui.safeBlur=function(b){b&&"body"!==b.nodeName.toLowerCase()&&a(b).trigger("blur")}});

```

<https://164.100.129.63/cppp8/core/modules/locale/locale.datepicker.js>

```

/**
 * DO NOT EDIT THIS FILE.
 * See the following change record for more information,
 * https://www.drupal.org/node/2815083
 * @preserve
 */

(function ($, Drupal, drupalSettings) {
  Drupal.behaviors.localeDatepicker = {
    attach: function attach(context, settings) {
      $.datepicker.regional['drupal-locale'] = $.extend({
        closeText: Drupal.t('Done'),
        prevText: Drupal.t('Prev'),
        nextText: Drupal.t('Next'),
        currentText: Drupal.t('Today'),
        monthNames: [Drupal.t('January', {}, { context: 'Long month name' }), Drupal.t('February', {}, {
          context: 'Long month name' }), Drupal.t('March', {}, { context: 'Long month name' }), Drupal.t('April', {}, {
            context: 'Long month name' }), Drupal.t('May', {}, { context: 'Long month name' }), Drupal.t('June', {}, {
              context: 'Long month name' }), Drupal.t('July', {}, { context: 'Long month name' }), Drupal.t('August', {}, {
                context: 'Long month name' }), Drupal.t('September', {}, { context: 'Long month name' }), Drupal.t('October',
                {}, { context: 'Long month name' }), Drupal.t('November', {}, { context: 'Long month name' }),
                Drupal.t('December', {}, { context: 'Long month name' })],
        monthNamesShort: [Drupal.t('Jan'), Drupal.t('Feb'), Drupal.t('Mar'), Drupal.t('Apr'),
          Drupal.t('May'), Drupal.t('Jun'), Drupal.t('Jul'), Drupal.t('Aug'), Drupal.t('Sep'), Drupal.t('Oct'),
          Drupal.t('Nov'), Drupal.t('Dec')],
        dayNames: [Drupal.t('Sunday'), Drupal.t('Monday'), Drupal.t('Tuesday'), Drupal.t('Wednesday'),
          Drupal.t('Thursday'), Drupal.t('Friday'), Drupal.t('Saturday')],
        dayNamesShort: [Drupal.t('Sun'), Drupal.t('Mon'), Drupal.t('Tue'), Drupal.t('Wed'), Drupal.t('Thu'),
          Drupal.t('Fri'), Drupal.t('Sat')],
        dayNamesMin: [Drupal.t('Su'), Drupal.t('Mo'), Drupal.t('Tu'), Drupal.t('We'), Drupal.t('Th'),
          Drupal.t('Fr'), Drupal.t('Sa')],
        dateFormat: Drupal.t('mm/dd/yy'),
        firstDay: 0,
        isRTL: 0
      }, drupalSettings.jquery.ui.datepicker);
      $.datepicker.setDefaults($.datepicker.regional['drupal-locale']);
    }
  };
})(jQuery, Drupal, drupalSettings);

```

<https://164.100.129.63/cppp8/core/assets/vendor/jquery.ui/ui/widgets/datepicker-min.js>

```

/! jQuery UI - v1.12.1 - 2017-03-31
* http://jqueryui.com
* Copyright jQuery Foundation and other contributors; Licensed */
!function(a){"function"==typeof define&&define.amd?define(["jquery","../version","../ keycode"],a):a(jQuery)}
(function(a){function b(a){for(var b,c;a.length&&a[0]!==document;){if(b=a.css("position"),

```

```

("absolute"===b||"relative"===b||"fixed"===b)&&(c=parseInt(a.css("zIndex"),10),!isNaN(c)&&0!==c)return
c;a=a.parent())return 0}function c(){this._curInst=null,this._keyEvent=!1,this._disabledInputs=
[],this._datepickerShowing=!1,this._inDialog=!1,this._mainDivId="ui-datepicker-div",this._inlineClass="ui-
datepicker-inline",this._appendClass="ui-datepicker-append",this._triggerClass="ui-datepicker-
trigger",this._dialogClass="ui-datepicker-dialog",this._disableClass="ui-datepicker-
disabled",this._unselectableClass="ui-datepicker-unselectable",this._currentClass="ui-datepicker-current-
day",this._dayOverClass="ui-datepicker-days-cell-over",this.regional=[],this.regional[""]=
{closeText:"Done",prevText:"Prev",nextText:"Next",currentText:"Today",monthNames:
["January","February","March","April","May","June","July","August","September","October","November","December
"],monthNamesShort:["Jan","Feb","Mar","Apr","May","Jun","Jul","Aug","Sep","Oct","Nov","Dec"],dayNames:
["Sunday","Monday","Tuesday","Wednesday","Thursday","Friday","Saturday"],dayNamesShort:
["Sun","Mon","Tue","Wed","Thu","Fri","Sat"],dayNamesMin:
["Su","Mo","Tu","We","Th","Fr","Sa"],weekHeader:"Wk",dateFormat:"mm/dd/yy",firstDay:0,isRTL:!1,showMonthAfter
Year:!1,yearSuffix:""},this._defaults={showOn:"focus",showAnim:"fadeIn",showOptions:
{},{defaultDate:null,appendText:"",buttonText:"",buttonImage:"",buttonImageOnly:!1,hideIfNoPrevNext:!1,navi
gationAsDateFormat:!1,gotoCurrent:!1,changeMonth:!1,changeYear:!1,yearRange:"c-
10:c+10",showOtherMonths:!1,selectOtherMonths:!1,showWeek:!1,calculateWeek:this.iso8601Week,shortYearCutoff:"
+10",minDate:null,maxDate:null,duration:"fast",beforeShowDay:null,beforeShow:null,onSelect:null,onChangeMonth
Year:null,onClose:null,numberMonths:1,showCurrentAtPos:0,stepMonths:1,stepBigMonths:12,altField:"",altForma
t:"",constrainInput:!0,showButtonPanel:!1,autoSize:!1,disabled:!1},a.extend(this._defaults,this.regional[""])
,this.regional.en=a.extend(!0,{},this.regional[""]),this.regional["en-US"]=a.extend(!0,
{},this.regional.en),this.dpDiv=d(a("<div id='"+this._mainDivId+"' class='ui-datepicker ui-widget ui-widget-
content ui-helper-clearfix ui-corner-all'></div>"))}function d(b){var c="button, .ui-datepicker-prev, .ui-
datepicker-next, .ui-datepicker-calendar td a";return b.on("mouseout",c,function(){a(this).removeClass("ui-
state-hover"),this.className.indexOf("ui-datepicker-prev")!==-1&&a(this).removeClass("ui-datepicker-prev-
hover"),this.className.indexOf("ui-datepicker-next")!==-1&&a(this).removeClass("ui-datepicker-next-
hover")}).on("mouseover",c,e)}function e(){a.datepicker._isDisabledDatepicker(g.inline?g.dpDiv.parent()
[0]:g.input[0])||a(this).parents(".ui-datepicker-calendar").find("a").removeClass("ui-state-
hover"),a(this).addClass("ui-state-hover"),this.className.indexOf("ui-datepicker-prev")!==-
1&&a(this).addClass("ui-datepicker-prev-hover"),this.className.indexOf("ui-datepicker-next")!==-
1&&a(this).addClass("ui-datepicker-next-hover")})function f(b,c){a.extend(b,c);for(var d in c)null==c[d]&&
(b[d]=c[d]);return b;a.extend(a.ui,{datepicker:{version:"1.12.1"}});var g;return a.extend(c.prototype,
{markerClassName:"hasDatepicker",maxRows:4,_widgetDatepicker:function(){return
this.dpDiv},setDefaults:function(a){return f(this._defaults,a||{}),this},_attachDatepicker:function(b,c){var
d,e,f;d=b.nodeName.toLowerCase(),e="div"===d||"span"===d,b.id||
(this.uuid+=1,b.id="dp"+this.uuid),f=this._newInst(a(b),e),f.settings=a.extend({},c||{}),"input"===d?
this._connectDatepicker(b,f):e&&this._inlineDatepicker(b,f),_newInst:function(b,c){var
e=b[0].id.replace(/([A-Za-z0-9_\-
])/g,"\\$1");return{id:e,input:b,selectedDay:0,selectedMonth:0,selectedYear:0,drawMonth:0,drawYear:0,inline
:c,dpDiv:c.d(a("<div class='"+this._inlineClass+"' ui-datepicker ui-widget ui-widget-content ui-helper-
clearfix ui-corner-all'></div>")):this.dpDiv}},_connectDatepicker:function(b,c){var
d=a(b);c.append=a([]),c.trigger=a([]),d.hasClass(this.markerClassName)||
(this._attachments(d,c),d.addClass(this.markerClassName).on("keydown",this._doKeyDown).on("keypress",this._do
KeyPress).on("keyup",this._doKeyUp),this._autoSize(c),a.data(b,"datepicker",c),c.settings.disabled&&this._dis
ableDatepicker(b)),_attachments:function(b,c){var
d,e,f,g=this._get(c,"appendText"),h=this._get(c,"isRTL");c.append&&c.append.remove(),g&&(c.append=a("<span
class='"+this._appendClass+"'>"+g+"</span>"),b[h?"before":"after"]
(c.append)),b.off("focus",this._showDatepicker),c.trigger&&c.trigger.remove(),d=this._get(c,"showOn"),"focus"
!==(d&&"both")!==(d||b.on("focus",this._showDatepicker),"button"!=d&&"both")!==(d||
(e=this._get(c,"buttonText"),f=this._get(c,"buttonImage"),c.trigger=a(th...

```

<https://164.100.129.63/cppp8/sites/all/themes/cppp/bootstrap/js/bootstrap.min.js>

```

/*!
 * Bootstrap v3.3.7 (http://getbootstrap.com)
 * Copyright 2011-2016 Twitter, Inc.
 * Licensed under the MIT license
 */
if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery");+function(a){
"use strict";var b=a.fn.jquery.split(" ")[0].split(".");if(b[0]<2&&b[1]<9||1==b[0]&&9==b[1]&&b[2]<1||b[0]>3)throw
new Error("Bootstrap's JavaScript requires jQuery version 1.9.1 or higher, but lower than version 4")
}(jQuery),+function(a){
"use strict";function b(){var a=document.createElement("bootstrap"),b=
{WebkitTransition:"webkitTransitionEnd",MozTransition:"transitionend",OTransition:"oTransitionEnd
ransitionend",transition:"transitionend"};for(var c in b)if(void
0!==a.style[c])return{end:b[c]};return!1}a.fn.emulateTransitionEnd=function(b){var
c=!1,d=this;a(this).one("bsTransitionEnd",function(){c=!0});var e=function(){
c||a(d).trigger(a.support.transition.end)};return setTimeout(e,b),this,a(function(){
a.support.transition=b(),a.support.transition&&(a.event.special.bsTransitionEnd=
{bindType:a.support.transition.end,delegateType:a.support.transition.end,handle:function(b)
{if(a(b.target).is(this))return b.handleObj.handler.apply(this,arguments)}})})(jQuery),+function(a){
"use strict";function b(b){return this.each(function(){var
c=a(this),e=c.data("bs.alert");e||c.data("bs.alert",e=new d(this)),e.string=="typeof b&&e[b].call(c)}
var c='[data-dismiss="alert"]',d=function(b)

```

```
{a(b).on("click",c,this.close));d.VERSION="3.3.7",d.TRANSITION_DURATION=150,d.prototype.close=function(b){function c(){g.detach().trigger("closed.bs.alert").remove()}var e=a(this),f=e.attr("data-target");f||(f=e.attr("href"),f=f&&f.replace(/.*(?=#[^\s]*$)/,""));var g=a("#"===f?[]:f);b&&b.preventDefault(),g.length||(g=e.closest(".alert")),g.trigger(b=a.Event("close.bs.alert")),b.isDefaultPrevented()||(g.removeClass("in"),a.support.transition&&g.hasClass("fade")?g.one("bsTransitionEnd",c).emulateTransitionEnd(d.TRANSITION_DURATION):c());var e=a.fn.alert;a.fn.alert=b,a.fn.alert.Constructor=d,a.fn.alert.noConflict=function(){return a.fn.alert=e,this},a(document).on("click.bs.alert.data-api",c,d.prototype.close)}(jQuery),+function(a){function b(b){return this.each(function(){var d=a(this),e=d.data("bs.button"),f="object"===typeof b&&b;e||d.data("bs.button",e=new c(this,f)),toggle=b?e.toggle():b&&e.setState(b)});var c=function(b,d){this.$element=a(b),this.options=a.extend({},c.DEFAULTS,d),this.isLoading=!1;c.VERSION="3.3.7",c.DEFAULTS={loadingText:"loading..."},c.prototype.setState=function(b){var c="disabled",d=this.$element,e=d.is("input")?"val":"html",f=d.data();b+="Text",null==f.resetText&&d.data("resetText",d[e]()),setTimeout(a.proxy(function(){d[e](null==f[b]?this.options[b]:f[b]),"loadingText"==b?(this.isLoading=!0,d.addClass(c).attr(c,c).prop(c,!0)):this.isLoading&&(this.isLoading=!1,d.removeClass(c).removeAttr(c).prop(c,!1))},this),0)},c.prototype.toggle=function(){var a=!0,b=this.$element.closest("[data-toggle='buttons']");if(b.length){var c=this.$element.find("input");"radio"==c.prop("type")?(c.prop("checked")&&(a=!1),b.find(".active").removeClass("active"),this.$element.addClass("active")):"checkbox"==c.prop("type")&&(c.prop("checked")!=this.$element.hasClass("active")&&(a=!1),this.$element.toggleClass("active")),c.prop("checked",this.$element.hasClass("active")),a&&c.trigger("change")}else this.$element.attr("aria-pressed",!this.$element.hasClass("active")),this.$element.toggleClass("active"));var d=a.fn.button;a.fn.button=b,a.fn.button.Constructor=c,a.fn.button.noConflict=function(){return a.fn.button=d,this},a(document).on("click.bs.button.data-api",'[data-toggle="button"]',function(c){var d=a(c.target).closest(".btn");b.call(d,"toggle"),a(c.target).is("input[type='radio'],input[type='checkbox']")||(c.preventDefault(),d.is("input,button")?d.trigger("focus"):d.find("input:visible,button:visible").first().trigger("focus"))}).on("focus.bs.button.data-api blur.bs.button.data-api",'[data-toggle="button"]',function(b){a(b.target).closest(".btn").toggleClass("focus",/^focus(in)?$/i.test(b.type))})}(jQuery),+function(a){function b(b){return this.each(function(){var d=a(this),e=d.data("bs.carousel"),f=a.extend({},c.DEFAULTS,d.data(),"object"===typeof b&&b),g="string"===typeof b?b:f.slide;e||d.data("bs.carousel",e=new c(this,f)),number="number"===typeof b?e.to(b):g?e[g]():f.interval&&e.pause().cycle();var c=function(b,c){this.$element=a(b),this.$indicators=this.$element.find(".carousel-indicators"),this.options=c,this.paused=null,this.sliding=null,this.interval=null,this.$active=null,this.$items=null,this.options.keyboard&&this.$element.on("keydown.bs.carousel",a.proxy(this.keydown,this)),this.options.pause&&("ontouchstart"in document.documentElement)&&this.$element.on("mouseenter.bs.carousel",a.proxy(this.pause,this)).on("mouseleave.bs.carousel",a.proxy(this.cycle,this));c.VERSION="3.3.7",c.TRANSITION_DURATION=600,c.DEFAULTS={interval:5e3,pause:"hover",wrap:!0,keyboard:!0},c.pro...}
```

<https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/toggle.js>

```
function hidePreHeader(){
  jQuery(".toggle-control").html("<a href='\"javascript:showPreHeader()\"'><span class='\"glyphicon glyphicon-plus\"'></span></a>");
  jQuery("#pre-header-inside").slideUp("fast");
}

function showPreHeader(){
  jQuery(".toggle-control").html("<a href='\"javascript:hidePreHeader()\"'><span class='\"glyphicon glyphicon-minus\"'></span></a>");
  jQuery("#pre-header-inside").slideDown("fast");
}
```

<https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/functions.js>

```
var $ = jQuery;

/*=====
Plugins: jQuery Easing, jQuery Cookie, jQuery Marquee, Access Script, Equal Heights, Dropdown Menu, Custom
Selectbox, OWL Slider, Responsive Tabs, GMAP3, Detect Element Resize Plugin, Images Loaded, LiteBox, jQuery
UI, Multiple Ticker, Photo Gallery
=====*/

// jQuery Easing
jQuery.easing["jswing"]=jQuery.easing["swing"];jQuery.extend(jQuery.easing,
```

```

{def:"easeOutQuad",swing:function(x,t,b,c,d){return jQuery.easing[jQuery.easing.def]
(x,t,b,c,d)},easeInQuad:function(x,t,b,c,d){return c*(t/=d)*t+b},easeOutQuad:function(x,t,b,c,d){return-c*
(t/=d)*(t-2)+b},easeInOutQuad:function(x,t,b,c,d){if((t/=d/2)<1)return c/2*t*t+b;return-c/2*(-t*(t-2)-
1)+b},easeInCubic:function(x,t,b,c,d){return c*(t/=d)*t*t+b},easeOutCubic:function(x,t,b,c,d){return c*
((t=t/d-1)*t*t+1)+b},easeInOutCubic:function(x,t,b,c,d){if((t/=d/2)<1)return c/2*t*t*t+b;return c/2*((t-
2)*t*t+2)+b},easeInQuart:function(x,t,b,c,d){return c*(t/=d)*t*t*t+b},easeOutQuart:function(x,t,b,c,d)
{return-c*((t=t/d-1)*t*t*t-1)+b},easeInOutQuart:function(x,t,b,c,d){if((t/=d/2)<1)return
c/2*t*t*t*t+b;return-c/2*((t-2)*t*t*t-2)+b},easeInQuint:function(x,t,b,c,d){return c*
(t/=d)*t*t*t*t+b},easeOutQuint:function(x,t,b,c,d){return c*((t=t/d-
1)*t*t*t*t+1)+b},easeInOutQuint:function(x,t,b,c,d){if((t/=d/2)<1)return c/2*t*t*t*t*t+b;return c/2*((t-
2)*t*t*t*t+2)+b},easeInSine:function(x,t,b,c,d){return-c*Math.cos(t/d*
(Math.PI/2))+c+b},easeOutSine:function(x,t,b,c,d){return c*Math.sin(t/d*
(Math.PI/2))+b},easeInOutSine:function(x,t,b,c,d){return-c/2*(Math.cos(Math.PI*t/d)-
1)+b},easeInExpo:function(x,t,b,c,d){return t==0?b:c*Math.pow(2,10*(t/d-
1))+b},easeOutExpo:function(x,t,b,c,d){return t==d?b+c:c*(-Math.pow(2,-
10*(t/d)+1))+b},easeInOutExpo:function(x,t,b,c,d){if(t==0)return b;if(t==d)return b+c;if((t/=d/2)<1)return
c/2*Math.pow(2,10*(t-1))+b;return c/2*(-Math.pow(2,-10*(-t)+2))+b},easeInCirc:function(x,t,b,c,d){return-c*
(Math.sqrt(1-(t/=d)*t)-1)+b},easeOutCirc:function(x,t,b,c,d){return c*Math.sqrt(1-(t=t/d-
1)*t)+b},easeInOutCirc:function(x,t,b,c,d){if((t/=d/2)<1)return-c/2*(Math.sqrt(1-t*t)-1)+b;return c/2*
(Math.sqrt(1-(t=t-2)*t)+1)+b},easeInElastic:function(x,t,b,c,d){var s=1.70158;var p=0;var a=c;if(t==0)return
b;if((t/=d)==1)return b+c;if(!p)p=d*0.3;if(a<Math.abs(c)){a=c;var s=p/4}else var
s=p/(2*Math.PI)*Math.asin(c/a);return-(a*Math.pow(2,10*(t-1))*Math.sin((t*d-s)*(2*
Math.PI)/p))+b},easeOutElastic:function(x,t,b,c,d){var s=1.70158;var p=0;var a=c;if(t==0)return
b;if((t/=d)==1)return b+c;if(!p)p=d*0.3;if(a<Math.abs(c)){a=c;var s=p/4}else var
s=p/(2*Math.PI)*Math.asin(c/a);return a*Math.pow(2,-10*t)*Math.sin((t*d-s)*
(2*Math.PI)/p)+c+b},easeInOutElastic:function(x,t,b,c,d){var s=1.70158;var p=0;var a=c;if(t==0)return
b;if((t/=d/2)==1)return b+c;if(!p)p=d*(0.3*1.5);if(a<Math.abs(c)){a=c;var s=p/4}else var
s=p/(2*Math.PI)*Math.asin(c/a);if(t<1)return-0.5*(a*Math.pow(2,10*(t-1))*Math.sin((t*d-s)*
(2*Math.PI)/p))+b;return a*Math.pow(2,-10*(t-1))*Math.sin((t*d-s)*
(2*Math.PI)/p)*0.5+c+b},easeInBack:function(x,t,b,c,d,s){if(s==undefined)s=1.70158;return c*(t/=d)*t*
((s+1)*t-s)+b},easeOutBack:function(x,t,b,c,d,s){if(s==undefined)s=1.70158;return c*((t=t/d-1)*t*
((s+1)*t+s)+1)+b},easeInOutBack:function(x,t,b,c,d,s){if(s==undefined)s=1.70158;if((t/=d/2)<1)return c/2*
(t*t*((s*=1.525)+1)*t-s))+b;return c/2*((t-2)*t*((s*=1.525)+1)*t+s)+2)+b},easeInBounce:function(x,t,b,c,d)
{return c-JQuery.easing.easeOutBounce(x,d-t,0,c,d)+b},easeOutBounce:function(x,t,b,c,d){if((t/=d)
<1/2.75)return c*(7.5625*t*t)+b;else if(t<2/2.75)return c*(7.5625*(t-=1.5/2.75)*t+0.75)+b;else
if(t<2.5/2.75)return c*(7.5625*(t-=2.25/2.75)*t+0.9375)+b;else return c*(7.5625*(t-
=2.625/2.75)*t+0.984375)+b},easeInOutBounce:function(x,t,b,c,d){if(t<d/2)return
jQuery.easing.easeInBounce(x,t*2,0,c,d)*0.5+b;return jQuery.easing.easeOutBounce(x,t*2-
d,0,c,d)*0.5+c*0.5+b}});

/*! jquery.cookie v1.4.1 | MIT */
jQuery.cookie=function(name,value,options){if(typeof value!='undefined'){options=options||{};if(value===null)
{value='';options=$.extend({},options);options.expires=-1;}var expires='';if(options.expires&&(typeof
options.expires=='number'||options.expires.toUTCString)){var date;if(typeof options.expires=='number')
{date=new Date();date.setTime(date.getTime()+
(options.expires*24*60*60*1000));}else{date=options.expires;}expires=''; expires='+date.toUTCString();}var
path=options.path?'; path='+options.path: '';var domain=options.domain?'; domain='+options.domain: '';var
secure=options.secure?'; secure='';document.cookie=
[name,'',encodeURIComponent(value),expires,path,domain,secure].join(';');}else{var
cookieValue=null;if(document.cookie&&document.cookie!=''){var cookies=document.cookie.split(';');for(var
i=0;i<cookies.length;i++){var cookie=jQuery.trim(cookies[i]);if(cookie.substring(0,name.length+1)==
(name+'='))}{cookieValue=decodeURIComponent(cookie.substring(n...

```

<https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/general.js>

```

/*-----*/
;(function($){

/*===== Global Variable Start =====*/
var isMobile = /Android|webOS|iPhone|iPod|BlackBerry|IEMobile|Opera Mini/i.test(navigator.userAgent);
var IEbellow9 = !$.support.leadingWhitespace;
var iPhoneAndiPad = /iPhone|iPod/i.test(navigator.userAgent);
var isIE = navigator.userAgent.indexOf('MSIE') != -1 || navigator.appVersion.indexOf('Trident/') > 0;
function isIEEver () {
    var myNav = navigator.userAgent.toLowerCase();
    return (myNav.indexOf('msie') != -1) ? parseInt(myNav.split('msie')[1]) : false;
}
//if (isIEEver () == 8) {}

//var jsFolder = "js/";
//var cssFolder = "css/";
// var basePath = $('input[id=basepath]').val();

```



```

var http_protocol = window.location.protocol;
var ip = window.location.protocol + "://" + window.location.host;
var protocol = window.location.protocol;
var host = window.location.host;
var pathname = window.location.pathname;
var path = (pathname.split("/", 2));
var contextPath = protocol + "://" + host + path;
contextPath = contextPath.replace("/", "/");
var project_name;
project_name = new String(path);
project_name = project_name.replace("/", "/");
var baseurllink=contextPath;
var jsFolder = baseurllink + "/sites/all/themes/cppp/js/custom/js/";
var cssFolder = baseurllink + "/sites/all/themes/cppp/js/custom/css/";

var ww = document.body.clientWidth, wh = document.body.clientHeight;
var mobilePort = 1023, iPadView = 1024, wideScreen = 1600;

/*===== Global Variable End =====*/

//css3 style calling
document.write('<link rel="stylesheet" type="text/css" href="' + cssFolder + 'animate.css">');

/*===== On Document Load Start =====*/
$(document).ready( function(){
    $('body').removeClass('noJS').addClass("hasJS");
    $(this).scrollTop(0);
    getWidth();

    //Custome Select Dropdown
    if( $(".customSelect").length){
        $('.customSelect').customSelect();
    }

    //Set Element to vertical center using padding
    $.fn.verticalAlign = function () {return this.css("padding-top", ($(this).parent().height() -
    $(this).height()) / 2 + 'px');};

    setTimeout(function(){
        $('.vCenter').each(function () {$(this).verticalAlign();});
    }, 800);

    // Index Banner Slider
    if( $(".sliderBanner").length) {
        var owl = $(".sliderBanner");
        var autoplay;
        if (owl.children().length == 1) {autoplay = false}
        else {autoplay = true}

        owl.owlCarousel({
            loop:true
            ,autoplay:true
            ,mouseDrag:false
            ,autoplayTimeout:4000
            ,autoplaySpeed:800
            ,smartSpeed:1200
            ,nav:false
            ,animateOut: 'owlFadeOut'
            ,animateIn: 'owlFadeIn'
            ,items : 1
            ,autoplayHoverPause: false
            ,navText: ["Prev","Next"]
            ,dots : false
        });

        var homeSlider = $(".sliderBanner");
        $(".indexBanner .playSlider").click(function(){
            homeSlider.trigger('play.owl.autoplay',[5000]);
            $(this).css("display", "none");
            $(".indexBanner .stopSlider").css("display", "block");

            return false;
        })
        $(".indexBanner .stopSlider").click(function(){

```

```

        homeSlider.trigger('stop.owl.autoplay');
        $(this).css("display", "none");
        $(".indexBanner .playSlider").css("display", "block");
        return false;
    });

    $(".indexBanner .next").click(function(){
        homeSlider.trigger('next.owl.carousel');
        return false;
    })
    $(".indexBanner .prev").click(function(){
        homeSlider.trigger('prev.owl.carousel');
        return false;
    })
}

};

// Inner Banner Slider
if( $(".slider").length ) {
    var owl2 = $(".slider");
    var autoplay;
    if (owl2.children().length == 1) {autoplay = false}
    else {autoplay = true}

    owl2.owlCarousel({
        loop:autoplay
        ,autoplay:autoplay
        ,mouseDrag:autoplay
        ,autoplayTimeout:3000
        ,autoplaySpeed:800
        ,smartSpeed:1200
        ,nav:autoplay
        ,dots:autoplay
        ,items : 1
        ,autoplayHoverPause: true
        //dots : false
        ,onInitialized: function(event) {
            if (owl2.children().length > 1) {

            }
        }
    });
};

if( $(".carouselBlock").length ) {
    $('.carouselBlock').owlCarousel({
        loop:true
        ,autoplay:false
        ,autoplayTimeout:3000
        ,smartSpeed:1200
        ,margin:0
        ,dots : false
        ,nav:true
        ,responsive:{
            0:{
                items:1
            }
            ,
            600:{
                items:3
            }
            ,
            1000:{
                items:5
            }
        }
    })
};

if( $(".marqueeScrolling li").length > 1){
    var $mq = $('.marquee').marquee({
        speed: 25000
        ,gap: 0
        ,duplicated: true
        ,pauseOnHover: true
        ,direction:'Up'
    })
    $(".btnMPPause").toggle(function(){
        $(this).addClass('play');
    });
}

```

```

                $(this).text('Play');
                $mq.marquee('pause');
            },function(){
                $(this).removeClass('play');
                $(this).text('Pause');
                $mq.marquee('resume');
                return false;
            });
    });

    // whats new
    if( $(".ticker").len...

```

<https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/customcommon.js>

```

var $ = jQuery.noConflict();

var protocol = window.location.protocol;
var host = window.location.host;
var pathname = window.location.pathname;
var path = (pathname.split("/", 2));
var contextPath = protocol + "/" + host + path;
contextPath = contextPath.replace(" ", "/");

// Active Today Start

function executeQuery(){
$.post(contextPath+"/sites/default/files/dashboard_json/active_json_data.json",
function(data, status){

var arr = JSON.parse(JSON.stringify(data));

var i;
for(i = 0; i < arr.length; i++) {

var timer;
var t=arr[i].active;
document.getElementById('active_1').innerHTML = t;

var val = document.getElementById('active_1');
var cn = parseFloat(val.innerHTML);
var t=cn/25;
var ad=cn-Math.round(t);

document.getElementById('active3').innerHTML = ad;

function startCount()
{
var speed = 0.01;
speed = speed / 6 * 5; // or whatever

timer = setInterval(count, 100);
}

function count()
{
var rand_no = 20;

var el = document.getElementById('active_1');
var currentNumber = parseFloat(el.innerHTML);

var el1 = document.getElementById('active3');
var currentNumber1 = parseFloat(el1.innerHTML);

var newNumber = currentNumber1 + rand_no;

if (newNumber <= currentNumber) {
document.getElementById('active4').innerHTML = newNumber;
document.getElementById('active3').innerHTML = newNumber;
}
}
}

```

```

else{
document.getElementById('active4').innerHTML = currentNumber;

}

}

startCount();
}

setTimeout(executeQuery, 30000);

});
}

$(document).ready(function() {
$.post(contextPath+"/sites/default/files/dashboard_json/active_json_data.json",
function(data, status){

var arr = JSON.parse(JSON.stringify(data));
var i;
for(i = 0; i < arr.length; i++) {

var timer;

var t=arr[i].active;
document.getElementById('active_1').innerHTML = t;

var val = document.getElementById('active_1');
var cn = parseFloat(val.innerHTML);
var t=cn/25;
var ad=cn-Math.round(t);

document.getElementById('active3').innerHTML = ad;

function startCount()
{

var speed = 0.1;
speed = speed / 6 * 5; // or whatever

timer = setInterval(count, 0.1);
}

function count()
{
var rand_no = 20;

var el = document.getElementById('active_1');
var currentNumber = parseFloat(el.innerHTML);

var el1 = document.getElementById('active3');
var currentNumber1 = parseFloat(el1.innerHTML);

var newNumber = currentNumber1 + rand_no;

if (newNumber <= currentNumber) {
document.getElementById('active4').innerHTML = newNumber;
document.getElementById('active3').innerHTML = newNumber;
}

else{
document.getElementById('active4').innerHTML = currentNumber;
}

}

startCount();
}

});

setTimeout(executeQuery, 30000);
});

// Active Today End

```

```

// Opening Today Start

function executeQuery1(){
$.post(contextPath+"/sites/default/files/dashboard_json/open_json_data.json",
function(data, status){
var arr = JSON.parse(JSON.stringify(data));
var i;
for(i = 0; i < arr.length; i++) {

var timer;

var t=arr[i].open;
document.getElementById('open_1').innerHTML = t;

var val = document.getElementById('open_1');
var cn = parseFloat(val.innerHTML);
var t=cn/25;
var ad=cn-Math.round(t);

document.getElementById('open3').innerHTML = ad;

function startCount1()
{
var speed = 0.01;
speed = speed / 6 * 5; // or whatever

timer = setInterval(count1, 100);
}
function count1()
{
var rand_no = 1;

var el = document.getElementById('open_1');
var currentNumber = parseFloat(el.innerHTML);

var el1 = document.getElementById('open3');
var currentNumber1 = parseFloat(el1.innerHTML);

var newNumber = currentNumber1 + rand_no;

if (newNumber <= currentNumber) {
document.getElementById('open4').innerHTML = newNumber;
document.getElementById('open3').innerHTML = newNumber;
}
else{
document.getElementById('open4').innerHTML = currentNumber;
}

}

startCount1();
}
setTimeout(executeQuery1, 30000);
});
}

$(document).ready(function() {
$.post(contextPath+"/sites/default/files/dashboard_json/open_json_data.json",
function(data, status){

var arr = JSON.parse(JSON.stringify(data));
var i;
for(i = 0; i < arr.length; i++) {

var timer;

var t=arr[i].open;
document.getElementById('open_1').innerHTML = t;

```

```

var val = document.getElementById('open_1');
var cn = parseFloat(val.innerHTML);
var t=cn/25;
var ad=cn-Math.round(t);

document.getElementById('open3').innerHTML = ad;

function startCount1()
{
    var speed = 0.1;
    speed = speed / 6 * 5; // or whatever

    timer = setInterval(count1, 0.1);
}
function count1()
{
    var rand_no = 1;

    var el = document.getElementById('open_1');
    var currentNumber = parseFloat(el.innerHTML);

var ell = document.getElementById('open3');
    var currentNumber1 = parseFloat(ell.innerHTML);

    var newNumber = currentNumber1 + rand_no;

    if (newNumber <= currentNumber) {
        document.getElementById('open4').inner...
    }
}

```

<https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/dncalendar.min.js>

```

(function(a){a.fn.dnCalendar=function(n){var l=a(this);var b={};var d=new Date();var i=null;var f=new Date();var e=function(q,s){var r=new Date(q,s-1,1);var o=new Date(q,s,0);var p=r.getDay()+o.getDate();return Math.ceil(p/7)};var h=function(){var Z=d.getMonth();var ag=d.getDate();var T=d.getFullYear();var J=b.monthNames[Z];if(b.monthUseShortName==true){J=b.monthNamesShort[Z]}var X=a("<div id='dncalendar-header' class='dncalendar-header'></div>");X.append("<h2>"+J+" "+T+"</h2>");var v=false;var r=null;if(typeof b.minDate!="undefined"){var aj=b.minDate.split("-");r=new Date(aj[0],aj[1]-1,aj[2]);if(r.getFullYear()==T){if(r.getMonth()==Z){v=true}}var M=false;var A=null;if(typeof b.maxDate!="undefined"){var F=b.maxDate.split("-");A=new Date(F[0],F[1]-1,F[2]);if(A.getFullYear()==T){if(A.getMonth()==Z){M=true}}var Q=a("<div id='dncalendar-links' class='dncalendar-links'></div>");var W=a("<div id='dncalendar-prev-month' class='dncalendar-prev-month'><i class='fa fa fa-chevron-left'></i></div>");var B=a("<div id='dncalendar-next-month' class='dncalendar-next-month'><i class='fa fa fa-chevron-right'></i></div>");if(v){W.addClass("dncalendar-inactive");W.removeAttr("id")}if(M){B.addClass("dncalendar-inactive");B.removeAttr("id")}Q.append(W);Q.append(B);X.append(Q);var C=a("<div id='dncalendar-body' class='dncalendar-body'></div>");var P=a("<table></table>");var N=b.dayNames;if(b.dayUseShortName==true){N=b.dayNamesShort}var q=a("<thead></thead>");var p=a("<tr></tr>");var af=N.length;for(var ad=0;ad<af;ad++){p.append("<td "+(ad==0||ad==af-1)?'class="holiday"'></td>");q.append(p);var u=a("<tbody></tbody>");var x=e(T,Z+1);var E=7;var t=1;var o=new Date(T,Z,1);var ah=new Date(T,Z+1,0);var O=new Date(T,Z,0);var R=O.getDate()-o.getDay()+1;var s=new Date(T,Z+1,1);var Y=s.getDate();var K=0;if(r!=null){K=r.getDate();var S=0;if(A!=null){S=A.getDate();var z="today";var ac="default date";if(typeof b.dataTitles!="undefined"){if(typeof b.dataTitles.defaultDate!="undefined"){ac=b.dataTitles.defaultDate}if(typeof b.dataTitles.today!="undefined"){z=b.dataTitles.today}}for(var ad=0;ad<x;ad++){var V=a("<tr></tr>");for(var ab=0;ab<E;ab++){if((ad!=0&&ad!=x-1)||ad==0&&ab==o.getDay())||ad==x-1&&ab<ah.getDay()){var w="";var H="";if(f.getFullYear()==T&&f.getMonth()==Z&&f.getDate()==t){w="today-date ";H="data-title="+z+""}if(i!=null&&i.getFullYear()==T&&i.getMonth()==Z&&i.getDate()==t){w="default-date ";H="data-title="+ac+""}if(ab==0||ab==E-1){w+=" holiday "}if(typeof b.notes!="undefined"){if(k(new Date(T,Z,t))){w+=" note "}}var U="<td id='calendarClick' class='"+w+" calendarClick' data-date='"+t+"' data-month='"+(Z+1)+"' data-year='"+T+"'><div class='entry' "+H+">"+t+"</div></td>";if(r!=null){if(r.getFullYear()==T){if(r.getMonth()==Z&&t<K){U="<td class='"+w+"' data-date='"+t+"' data-month='"+(Z+1)+"' data-year='"+T+"'><div class='entry' "+H+">"+t+"</div></td>";if(A!=null){if(A.getFullYear()==T){if(A.getMonth()==Z&&t>S){U="<td class='"+w+"' data-date='"+t+"' data-month='"+(Z+1)+"' data-year='"+T+"'><div class='entry' "+H+">"+t+"</div></td>";if(r!=null){if(r.getFullYear()==O.getFullYear()){if(r.getMonth()==O.getMonth()){if(r.getDate()==R){w=" today-date ";H="data-title="+z+""}if(i!=null&&i.getFullYear()==O.getFullYear()){if(i.getMonth()==O.getMonth()){if(i.getDate()==R){w=" default-date ";H="data-title="+ac+""}if(ab==0||ab==E-1){w+=" holiday "}if(typeof b.notes!="undefined"){if(k(new Date(O.getFullYear(),O.getMonth(),R))){w+=" note "}}var U="<td id='calendarClick' class='"+w+"' data-date='"+R+"' data-month='"+(O.getMonth()+1)+"' data-year='"+O.getFullYear()+"'><div class='entry' "+H+">"+R+"</div></td>";if(r!=null){if(r.getFullYear()==O.getFullYear()){if(r.getMonth()==O.getMonth()){if(r.getDate()==R){U="<td

```

```

class="w+" data-date="+R+" data-month="+O.getMonth()+1+" data-year="+O.getFullYear()+"><div
class='entry' "+H+">"</div></td>"} }V.append(U);R++}if(ad==x-1){var w="";var
H="";if(f.getFullYear()==s.getFullYear())&&f.getMonth()==s.getMonth()&&f.getDate()==Y){w=" today-date
";H="data-
title="+z+""}if(i!=null&&i.getFullYear()==s.getFullYear()&&i.getMonth()==s.getMonth()&&i.getDate()==Y){w="
default-date ";H="data-title="+ac+""}if(ab==0||ab==E-1){w=" holiday "}if(typeof b.notes!="undefined")
{if(k(new Date(s.getFullYear(),s.getMonth(),Y))){w=" note "}}var U="<td id='calendarClick' class='"+w+"'
data-date='"+Y+"' data-month='"+(s.getMonth()+1)+"' data-year='"+s.getFullYear()+"'><div class='entry'
"+H+">"</div></td>";if(A!=null){if(A.getFullYear()<s.getFullYear()){if(A.getMonth()<s.getMonth())
{if(A.getMonth()<s.getMonth()){U="<td class='"+w+"' data-date='"+Y+"' data-month='"+(s.getMonth()+1)+"' data-
year='"+s.getFullYear()+"'><div class='entry' "+H+">"</div></td>"}else{if(S<Y){U="<td class='"+w+"' data-
date='"+Y+"' data-month='"+(s.getMonth()+1)+"' data-year='"+s.getFullYear()+"'><div class='entry' "+H+">"</div></td>"}}}}V.append(U);Y++}}u.append(V)}var ai="";if(b.show...

```

<https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/c3.min.js>

```

!function(a){"use strict";function b(a){this.owner=a}function c(a,b)
{if(Object.create)b.prototype=Object.create(a.prototype);else{var c=function()
{};c.prototype=a.prototype,b.prototype=new c;return b.prototype.constructor=b,b}function d(a){var
b=this.internal=new e(this);b.loadConfig(a),b.init(),function c(a,b,d){Object.keys(a).forEach(function(e)
{b[e]=a[e].bind(d),Object.keys(a[e]).length>0&&c(a[e],b[e],d)})}(h,this,this)}function e(b){var
c=this;c.d3=a.d3?a.d3:"undefined"!=typeof require?require("d3"):void
0,c.api=b,c.config=c.getDefaultConfig(),c.data={},c.cache={},c.axes={}}function f(a){b.call(this,a)}function
g(a,b){function c(a,b){a.attr("transform",function(a){return"translate("+Math.ceil(b(a)+u)+", 0)"})}function
d(a,b){a.attr("transform",function(a){return"translate(0,"+Math.ceil(b(a))+")"})}function e(a){var
b=a[0],c=a[a.length-1];return c>b?[b,c]:[c,b]}function f(a){var b,c,d=[];if(a.ticks)return
a.ticks.apply(a,n);for(c=a.domain(),b=Math.ceil(c[0]);b<c[1];b++)d.push(b);return
d.length>0&&d[0]>0&&d.unshift(d[0]-(d[1]-d[0])),d}function g(){var a,c=p.copy();return b.isCategory&&
(a=p.domain(),c.d.domain([a[0],a[1]-1])),c}function h(a){var b=m?m(a):a;return"undefined"!=typeof b?
b:""}function i(a){if(z)return z;var b={h:11.5,w:5.5};return a.select("text").text(h).each(function(a){var
c=this.getBoundingClientRect(),d=h(a),e=c.height,f=d?c.width/d.length:void 0;e&&f&&
(b.h=e,b.w=f)).text(""),z=b,b}function j(c){return b.withoutTransition?c.a.transition(c)}function k(m)
{m.each(function(){function m(a,c){function d(a,b){f=void 0;for(var h=1;h<b.length;h++)if(" "===b.charAt(h)&&
(f=h),e=b.substr(0,h+1),g=U.w*e.length,g>c)return d(a.concat(b.substr(0,f?f:h)),b.slice(f?f+1:h));return
a.concat(b)}var e,f,g,i=h(a),j=[];return[object Array]===Object.prototype.toString.call(i)?i:((c||0>c)&&
(c=X?95:b.isCategory?Math.ceil(F(G[1])-F(G[0]))-12:110),d(j,i+""))}function n(a,b){var c=U.h;return 0===b&&
(c="left"===q||"right"===q?-((V[a.index]-1)*(U.h/2)-3):".71em"),c}function v(a){var b=p(a)+(o?0:u);return
L[0]<b&&b<L[1]?r:0}function w(a){return a?>0?"start":"end":"middle"}function x(a){return
a?"rotate("+a+""):""}function y(a){return a?8*Math.PI*(a/180):0}function z(a){return a?11.5-2.5*
(a/15)*(a>0?1:-1):W}var A,B,C,D=k.g=a.select(this),E=this.__chart__|p,F=this.__chart__&g(),G=t?
t(F),H=D.selectAll(".tick").data(G,F),I=H.enter().insert("g",".domain").attr("class","tick").style("opacity",
"1e-6"),J=H.exit().remove(),K=j(H).style("opacity",1),L=p.rangeExtent?
p.rangeExtent():e(p.range()),M=D.selectAll(".domain").data([0]),N=
(M.enter().append("path").attr("class","domain"),j(M));I.append("line"),I.append("text");var
O=I.select("line"),P=K.select("line"),Q=I.select("text"),R=K.select("text");b.isCategory?(u=Math.ceil((F(1)-
F(0))/2),B=o?0:u,C=o?u:0):u=B=0;var S,T,U=i(D.select(".tick")),V=
[],W=Math.max(r,0)+s,X="left"===q||"right"===q;S=H.select("text"),T=S.selectAll("tspan").data(function(a,c)
{var d=b.tickMultiline?m(a,b.tickWidth):[];return V[c]=d.length,d.map(function(a)
{return(index:c,splitted:a)})),T.enter().append("tspan"),T.exit().remove(),T.text(function(a){return
a.splitted});var Y=b.tickTextRotate;switch(q)
{case"bottom":A=c,O.attr("y2",r),Q.attr("y",W),P.attr("x1",B).attr("x2",B).attr("y2",v),R.attr("x",0).attr("y",
z(Y)).style("text-
anchor",w(Y)).attr("transform",x(Y)),T.attr("x",0).attr("dy",n).attr("dx",y(Y)),N.attr("d","M"+L[0]+","+1+"V0
H"+L[1]+V+1);break;case"top":A=c,O.attr("y2",-r),Q.attr("y",-W),P.attr("x2",0).attr("y2",-
r),R.attr("x",0).attr("y",-W),S.style("text-
anchor","middle"),T.attr("x",0).attr("dy",n).attr("dx",0),N.attr("d","M"+L[0]+","+1+"V0H"+L[1]+V+1);break;case"left":A=d,O.attr("x2",-r),Q.attr("x",-W),P.attr("x2",-r).attr("y1",C).attr("y2",C),R.attr("x",-
W).attr("y",u),S.style("text-anchor","end"),T.attr("x",-W).attr("dy",n),N.attr("d","M"+1+
"+L[0]+H0V"+L[1]+H+1);break;case"right":A=d,O.attr("x2",r),Q.attr("x",W),P.attr("x2",r).attr("y2",0),R.attr("x",W).attr("y",0),S
.style("text-
anchor","start"),T.attr("x",W).attr("dy",n),N.attr("d","M"+1+
"+L[0]+H0V"+L[1]+H+1)}if(F.rangeBand){var
Z=F,$=Z.rangeBand()/2;E=F=function(a){return Z(a)+$}}else E.rangeBand?
E=F:J.call(A,F);I.call(A,E),K.call(A,F)}var
l,m,n,o,p=a.scale.linear(),r=6,s=3,t=null,u=0,v=!0;return b=b||{,l=b.withOuterTick?
6:0,k.scale=function(a){return arguments.length?(p=a,k):p,k.orient=function(a){return arguments.length?(q=a
in{top:1,right:1,bottom:1,left:1}?a:"bottom"):k},k.tickFormat=function(a){return arguments.length?
(m=a,k):m},k.tickCentered=function(a){return arguments.length?(o=a,k):o},k.tickOffset=function(){return
u},k.tickInterval=function(){var a,c;return b.isCategory?a=2*u:
(c=k.g.select("path.domain").node().getTotalLength()-2*l,a=c/k.g.selectAll("line").size()),1/0===a?
0:a},k.ticks=function(){return arguments.length?(n=arguments,k):n},k.tickCulling=function(a){return
arguments.length?(v=a,k):v},k.tickValues=function(a){if("function"===typeof a)t=function(){return
a(p.domain())...

```

<https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/d3.min.js>

```
!function(){function n(n){return n&&(n.ownerDocument||n.document||n).documentElement}function t(n){return n&&(n.ownerDocument&&n.ownerDocument.defaultView||n.document&&n.defaultView)}function e(n,t){return t>n?-1:n>t?1:n>=t?0:NaN}function r(n){return null===n?NaN:n}function u(n){return!isNaN(n)}function i(n){return{left:function(t,e,r,u){for(arguments.length<3&&(r=0),arguments.length<4&&(u=t.length);u>r;){var i=r+u>>1;n(t[i],e)<0?r=i+1:u=i}return r},right:function(t,e,r,u){for(arguments.length<3&&(r=0),arguments.length<4&&(u=t.length);u>r;){var i=r+u>>1;n(t[i],e)>0?u=i-1:r=i+1}return r}}function a(n){return n.length}function o(n){for(var t=1;n*t%1;t*=10;return t)}function l(n,t){for(var e in t)Object.defineProperty(n.prototype,e,{value:t[e],enumerable:!1})}function c(){this._=Object.create(null)}function s(n){return(n+""===x||n[0]===b?b+n:n)}function f(n){return(n+""[0]===b?n.slice(1):n)}function h(n){return s(n)}function g(n){return(n=s(n))in this._&&delete this._[n]}function p(){var n=[];for(var t in this._)n.push(f(t));return n}function v(){var n=0;for(var t in this._)++n;return n}function d(){for(var n in this._)return!1;return!0}function m(){this._=Object.create(null)}function y(n){return n}function M(n,t,e){return function(){var r=e.apply(t,arguments);return r==t?n:r}}function x(n,t){if(t in n)return t;t=t.charAt(0).toUpperCase()+t.slice(1);for(var e=0,r=_a.length;r>e;e++){var u=_a[e]+t;if(u in n)return u}}function b(){function _(){function w(n){function t(){for(var t,r=e,u=-1,i=r.length;u<i;){t=r[u].on}&&t.apply(this,arguments);return n}var e=[],r=new c;return t.on=function(t,u){var i,a=r.get(t);return arguments.length<2?a&&a.on:(a&&(a.on=null,e=e.slice(0,i=e.indexOf(a)).concat(e.slice(i+1)),r.remove(t)),u&&e.push(r.set(t,{on:u})),n),t)}function S(){oa.event.preventDefault()}function k(){for(var n,t=oa.event;n=t.sourceEvent;t=n;return t)}function N(n){for(var t=new _e=0,r=arguments.length;e<r;e++)t[arguments[e]]=(t)?w(t):return t.of=function(e,r){return function(u){try{var i=u.sourceEvent=oa.event;u.target=n,oa.event=u,t[u.type].apply(e,r)}finally{oa.event=i}}},t)}function E(n){return Sa(n,Aa,n)}function A(n){return"function"===typeof n?n:function(){return ka(n,this)}}function C(n){return"function"===typeof n?n:function(){return Na(n,this)}}function z(n,t){function e(){this.removeAttribute(n)}function r(){this.removeAttributeNS(n.space,n.local)}function u(){this.setAttribute(n,t)}function i(){this.setAttributeNS(n.space,n.local,t)}function a(){var e=t.apply(this,arguments);null==e?this.removeAttribute(n):this.setAttribute(n,e)}function o(){var e=t.apply(this,arguments);null==e?this.removeAttributeNS(n.space,n.local):this.setAttributeNS(n.space,n.local,e)}return n=oa.ns.qualify(n),null==t?n.local?r:e:"function"===typeof t?n.local?o:a:n.local?i:u}function L(n){return n.trim().replace(/s/g," ")}function q(n){return new RegExp("(?:^|\\s+)" + oa.regquote(n) + "(?:\\s+|$)", "g")}}function T(n){return(n+"" ).trim().split(/s+/)}function R(n,t){function e(){for(var e=-1;e<u;e++)n[e](this,t)}function r(){for(var e=-1,r=t.apply(this,arguments);e<u;e++)n[e](this,r)}n=T(n).map(D);var u=n.length;return"function"===typeof t?r:e}function D(n){var t=q(n);return function(e,r){if(u=e.classList)return r?u.add(n):u.remove(n);var u=e.getAttribute("class")||"";r?(t.lastIndexOf,t.test(u)||e.setAttribute("class",L(u+" "+n))):e.setAttribute("class",L(u.replace(t," ")))}}function P(n,t,e){function r(){this.style.removeProperty(n)}function u(){this.style.setProperty(n,t,e)}function i(){var r=t.apply(this,arguments);null==r?this.style.removeProperty(n):this.style.setProperty(n,r,e)}return null==t?r:"function"===typeof t?i:u}function U(n,t){function e(){delete this[n]}function r(){this[n]=t}function u(){var e=t.apply(this,arguments);null==e?delete this[n]:this[n]=e}return null==t?e:"function"===typeof t?u:r}function j(n){function t(){var t=this.ownerDocument,e=this.namespaceURI;return e===Ca&&t.documentElement.namespaceURI===Ca?t.createElement(n):t.createElementNS(e,n)}function e(){return this.ownerDocument.createElementNS(n.space,n.local)}return"function"===typeof n?n:(n=oa.ns.qualify(n)).local?e:t}function F(){var n=this.parentNode;n&&n.removeChild(this)}function H(n){return{__data__:n}}function O(n){return function(){return Ea(this,n)}}function I(n){return arguments.length||n?e,function(t,e){return t&&e?n(t.__data__,e.__data__):!t!e}function Y(n,t){for(var e=0,r=n.length;r>e;e++)for(var u,i=n[e],a=0,o=i.length;o>a;a++)u=i[a]&&t(u,a,e);return n}function Z(n){return Sa(n,La,n)}function V(n){var t,e;return function(r,u,i){var a,o=n[i].update,l=o.length;for(i!=e&&(e=i,t=0),u>t&&(t=u+1);!(a=o[t])&&t<l;return a)}function X(n,t,e){function r(){var t=this[a];t&&(this.removeEventListener(n,t,t.$),delete this[a])}function u(){var u=l(t,ca(arguments));r.call(this),this.addEventListener(n,this[a]=u,u.$=e),u._t}function i(){var t,e=new RegExp("^_on([^.]+)" + oa.regquote(n) + "$");for(var r in this)if(t=r.match(e)){var u=this...
```

<https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/jquery.base64.min.js>

```
"use strict";jQuery.base64=(function($){var _PADCHAR="", ALPHA="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/", _VERSION="1.0";function _getbyte64(s,i){var idx=_ALPHA.indexOf(s.charAt(i));if(idx===-1){throw"Cannot decode base64"}}return idx}function _decode(s){var pads=0,i,b10,imax=s.length,x=[];s=String(s);if(imax===0){return s;if(imax%4!==0){throw"Cannot decode base64"}}if(s.charAt(imax-1)=== _PADCHAR){pads=1;if(s.charAt(imax-2)=== _PADCHAR){pads=2}imax-=4}for(i=0;i<imax;i+=4){b10=(_getbyte64(s,i)<<18)|(_getbyte64(s,i+1)<<12)|(_getbyte64(s,i+2)<<6)|_getbyte64(s,i+3);x.push(String.fromCharCode(b10>>16,(b10>>8)&255,(b10&255)))}switch(pads){case 1:b10=(_getbyte64(s,i)<<18)|(_getbyte64(s,i+1)<<12)|(_getbyte64(s,i+2)<<6);x.push(String.fromCharCode(b10>>16,(b10>>8)&255));break;case 2:b10=(_getbyte64(s,i)<<18)|(_getbyte64(s,i+1)<<12)|(_getbyte64(s,i+2)<<6)|_getbyte64(s,i+3);x.push(String.fromCharCode(b10>>16,(b10>>8)&255,(b10&255)))}
```



```
<<12);x.push(String.fromCharCode(b10>>16));break}return x.join("")}function _getbyte(s,i){var
x=s.charCodeAt(i);if(x>255){throw"INVALID_CHARACTER_ERR: DOM Exception 5"}return x}function _encode(s)
{if(arguments.length!==1){throw"SyntaxError: exactly one argument required"}s=String(s);var i,b10,x=
[],imax=s.length-s.length%3;if(s.length===0){return s}for(i=0;i<imax;i+=3){b10=(_getbyte(s,i)<<16)|
(_getbyte(s,i+1)
<<8)|_getbyte(s,i+2);x.push(_ALPHA.charAt(b10>>18));x.push(_ALPHA.charAt((b10>>12)&63));x.push(_ALPHA.charAt(
(b10>>6)&63));x.push(_ALPHA.charAt(b10&63))}switch(s.length-imax){case 1:b10=_getbyte(s,i)
<<16;x.push(_ALPHA.charAt(b10>>18)+_ALPHA.charAt((b10>>12)&63)+_PADCHAR+_PADCHAR);break;case 2:b10=
(_getbyte(s,i)<<16)|(_getbyte(s,i+1)
<<8);x.push(_ALPHA.charAt(b10>>18)+_ALPHA.charAt((b10>>12)&63)+_ALPHA.charAt((b10>>6)&63)+_PADCHAR);break}ret
urn x.join("")}return{decode:_decode,encode:_encode,VERSION:_VERSION}}(jQuery);
```

<https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/pako.min.js>

```
!function(t){if("object"===typeof exports&&"undefined"!==typeof module)module.exports=t();else
if("function"===typeof define&&define.amd)define([],t);else{"undefined"!==typeof window?
window:"undefined"!==typeof global?global:"undefined"!==typeof self?self:this).pako=t()}(function(){return
function t(e,a,i){function n(s,o){if(!a[s]){if(!e[s]){var l="function"===typeof
require&&require;if(!o&&l)return l(s,!0);if(r)return r(s,!0);var h=new Error("Cannot find module
"+s+"");throw h.code="MODULE_NOT_FOUND",h}var d=a[s]={exports:{}};e[s][0].call(d.exports,function(t){var
a=e[s][1][t];return n(a||t)},d,d.exports,t,e,a,i)}return a[s].exports}for(var r="function"===typeof
require&&require,s=0;s<i.length;s++)n(i[s]);return n}({1:[function(t,e,a){"use strict";function i(t){if(!
(this instanceof i))return new
i(t);this.options=s.assign({level:_,method:c,chunkSize:16384>windowBits:15,memLevel:8,strategy:u,to:""},t||
{});var e=this.options;e.raw&&e.windowBits>0?e.windowBits=-
e.windowBits:e.gzip&&e.windowBits>0&&e.windowBits<16&&
(e.windowBits+=16),this.err=0,this.msg="",this.ended=!1,this.chunks=[],this.strm=new
h,this.strm.avail_out=0;var
a=r.deflateInit2(this.strm,e.level,e.method,e.windowBits,e.memLevel,e.strategy);if(a!==f)throw new
Error(1[a]);if(e.header&&r.deflateSetHeader(this.strm,e.header),e.dictionary){var n;if(n="string"===typeof
e.dictionary?o.string2buf(e.dictionary):"object ArrayBuffer"===d.call(e.dictionary)?new
Uint8Array(e.dictionary):e.dictionary,(a=r.deflateSetDictionary(this.strm,n))!==f)throw new
Error(1[a]);this.dict_set=!0}function n(t,e){var a=new i(e);if(a.push(t,!0),a.err)throw
a.msg||1[a.err];return a.result}var
r=t("./zlib/deflate"),s=t("./utils/common"),o=t("./utils/strings"),l=t("./zlib/messages"),h=t("./zlib/zstream
"),d=Object.prototype.toString,f=0,_=-1,u=0,c=8,i.prototype.push=function(t,e){var
a,i,n=this.strm,l=this.options.chunkSize;if(this.ended)return!1;i=e===~e?e:!0===e?4:0,"string"===typeof t?
n.input=o.string2buf(t):"object ArrayBuffer"===d.call(t)?n.input=new
Uint8Array(t):n.input=t,n.next_in=0,n.avail_in=n.input.length;do{if(0===n.avail_out&&(n.output=new
s.Buf8(1),n.next_out=0,n.avail_out=1),l!==(a=r.deflate(n,i))&&a!==f)return
this.onEnd(a),this.ended=!0,!1;0!==(n.avail_out&&(0!==(n.avail_in||4!==(i&2!==(i)||("string"===this.options.to?
this.onData(o.buf2binstring(s.shrinkBuf(n.output,n.next_out)):this.onData(s.shrinkBuf(n.output,n.next_out)))
}while((n.avail_in>0||0!==(n.avail_out)&&1!==(a))return 4===i?
(a=r.deflateEnd(this.strm),this.onEnd(a),this.ended=!0,a===f):2!==(i||
(this.onEnd(f),n.avail_out=0,!0)),i.prototype.onData=function(t)
{this.chunks.push(t)},i.prototype.onEnd=function(t){t===f&&("string"===this.options.to?
this.result=t.chunks.join(""):this.result=s.flattenChunks(this.chunks)),this.chunks=
[],this.err=t,this.msg=this.strm.msg,a.Deflate=i,a.deflate=n,a.deflateRaw=function(t,e){return e||
{}},e.raw=!0,n(t,e)),a.gzip=function(t,e){return e||{}},e.gzip=!0,n(t,e)},
{"./utils/common":3,"./utils/strings":4,"./zlib/deflate":8,"./zlib/messages":13,"./zlib/zstream":15}],2:
[function(t,e,a){"use strict";function i(t){if(!(this instanceof i))return new
i(t);this.options=s.assign({chunkSize:16384>windowBits:0,to:""},t||{});var
e=this.options;e.raw&&e.windowBits>0&&e.windowBits<16&&(e.windowBits=-e.windowBits,0===e.windowBits&&
(e.windowBits=-15)),!(e.windowBits>0&&e.windowBits<16)||t&&t.windowBits||
(e.windowBits+=32),e.windowBits>15&&e.windowBits<48&&0==(15&e.windowBits)&&
(e.windowBits|=15),this.err=0,this.msg="",this.ended=!1,this.chunks=[],this.strm=new
d,this.strm.avail_out=0;var a=r.inflateInit2(this.strm,e.windowBits);if(a!==1.Z_OK)throw new
Error(h[a]);this.header=new f,r.inflateGetHeader(this.strm,this.header)}function n(t,e){var a=new
i(e);if(a.push(t,!0),a.err)throw a.msg||h[a.err];return a.result}var
r=t("./zlib/inflate"),s=t("./utils/common"),o=t("./utils/strings"),l=t("./zlib/constants"),h=t("./zlib/messag
es"),d=t("./zlib/zstream"),f=t("./zlib/gzheader"),_Object.prototype.toString; i.prototype.push=function(t,e)
{var
a,i,n,h,d,f,u=this.strm,c=this.options.chunkSize,b=this.options.dictionary,g=!1;if(this.ended)return!1;i=e===
~e?e:!0===e?1.Z_FINISH:1.Z_NO_FLUSH,"string"===typeof t?u.input=o.binstring2buf(t):"object
ArrayBuffer"===_call(t)?u.input=new
Uint8Array(t):u.input=t,u.next_in=0,u.avail_in=u.input.length;do{if(0===u.avail_out&&(u.output=new
s.Buf8(c),u.next_out=0,u.avail_out=c),(a=r.inflate(u,1.Z_NO_FLUSH))===1.Z_NEED_DICT&&b&&(f="string"===typeof
b?o.string2buf(b):"object ArrayBuffer"===_call(b)?new
Uint8Array(b):b,a=r.inflateSetDictionary(this.strm,f)),a===1.Z_BUF_ERROR&&!0===g&&
(a=1.Z_OK,g=!1),a!==1.Z_STREAM_END&&a!==1.Z_OK)return this.onEnd(a),this.ended=!0,!1;u.next_out&&
(0!==(u.avail_out&&1.Z_STREAM_END&&(0!==(u.avail_in||i!==(1.Z_FINISH&&i!==(1.Z_SYNC_FLUSH)||
("string"===this.options.to?n(o.utf8border(u.output,u.next_out),h=u.next_out-
n,d=o.buf2string(u.output,n),u.next_out=h,u.avail_out=c-
```

```
h,h&&s.arraySet(u.output,u.output,n,h,0),this.onData(d)):this.o...
```

<https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/c3chartslider.js>

```
$('.slider').each(function() {
  var $this = $(this);
  var $group = $this.find('.slide_group');
  var $slides = $this.find('.slide');
  var bulletArray = [];
  var currentIndex = 0;
  var timeout;

  function move(newIndex) {
    var animateLeft, slideLeft;

    advance();

    if ($group.is(':animated') || currentIndex === newIndex) {
      return;
    }

    bulletArray[currentIndex].removeClass('active');
    bulletArray[newIndex].addClass('active');

    if (newIndex > currentIndex) {
      slideLeft = '100%';
      animateLeft = '-100%';
    } else {
      slideLeft = '-100%';
      animateLeft = '100%';
    }

    $slides.eq(newIndex).css({
      display: 'block',
      left: slideLeft
    });
    $group.animate({
      left: animateLeft
    }, function() {
      $slides.eq(currentIndex).css({
        display: 'none'
      });
      $slides.eq(newIndex).css({
        left: 0
      });
      $group.css({
        left: 0
      });
      currentIndex = newIndex;
    });
  }

  function advance() {
    clearTimeout(timeout);
    timeout = setTimeout(function() {
      if (currentIndex < ($slides.length - 1)) {
        move(currentIndex + 1);
      } else {
        move(0);
      }
    }, 4000);
  }

  $('.next_btn').on('click', function() {
    if (currentIndex < ($slides.length - 1)) {
      move(currentIndex + 1);
    } else {
      move(0);
    }
  });

  $('.previous_btn').on('click', function() {
    if (currentIndex !== 0) {

```

```

        move(currentIndex - 1);
    } else {
        move(3);
    }
});

$.each($slides, function(index) {
    var $button = $('<a class="slide_btn">&bull;</a>');

    if (index === currentIndex) {
        $button.addClass('active');
    }
    $button.on('click', function() {
        move(index);
    }).appendTo('.slide_buttons');
    bulletArray.push($button);
});

advance();
});

var protocol = window.location.protocol;
var host = window.location.host;
var pathname = window.location.pathname;
var path = (pathname.split("/", 2));
var contextPath = protocol + "/" + host + path;
contextPath = contextPath.replace(" ", "/");

//chart

urllink = contextPath+'/sites/default/files/dashboard_json/';

jQuery(document).ready(function($) {

//bar-chart

var colorsbarchart = ['#1f77b4', '#aec7e8', '#ff7f0e', '#ffbb78', '#2ca02c', '#98df8a', '#d62728', '#ff9896',
'#9467bd', '#c5b0d5', '#8c564b', '#c49c94', '#e377c2', '#7b6d2', '#7f7f7f', '#c7c7c7', '#bcbd22', '#dbdb8d',
'#17becf', '#9edae5'];

var barchart = c3.generate({

    bindto: '#barchart',
    data: {
        type: 'bar',

labels: true,

        url: urllink+'fin_yr_chart_data_live.json',

        mimeType: 'json',

        keys: {
            x: 'finyear',
            value: ['num_tender']
        },

        color: function (color, d) {
            return colorsbarchart[d.index];
        }
    },

    axis: {
        x: {
            label: {
                text: '* Fin Year 2018-2019 etender details pertains to data as on date',
                position: 'outer-center'
            },

            type: 'category',
        },

        y: {
            label: {
                text: 'No. of Tenders Published',
                position: 'outer-middle'
            }
        }
    }
});

```

```

    }
  },

  },

  bar: {
    width: {
      ratio: 0.3
    }
  },

  legend: {
    show: false
  },

  tooltip: {
    format: {
      name: function (name, ratio, id, index) {
        if (id === "num_tender") {
          return "No of eTenders";
        } else {
          return "No of eTenders";
        }
      }
    }
  }
}

});

//pie-chart

$.getJSON(urllink+'orgwise_chart_data_live.json', function(jsondata) {

var data = {};
var sites = [];
jsondata.forEach(function(e) {

  var datakey = {

'Ministry of Railways' : 'MoR',
'Central Public Works Department (CPWD)' : 'CPWD',
'Defence PSUs' : 'DefPSUs',
'Bharat Heavy Electricals Limited' : 'BHEL',
'NTPC Ltd' : 'NTPC',
'Indian Oil Corporation Limited' : 'IOCL',
'Electronics Division, BHEL' : 'Elec BHEL',
'Bharat Petroleum Corporation Limited' : 'BPCL',
'Nuclear Power Corporation of India Ltd' : 'NPCIL',
'Coal India Limited' : 'CIL',
'Department of Posts' : 'DoP',
'National Rural Roads Development Agency (NRRDA)' : 'NRRDA',
'Ordnance Factory Board' : 'OFB',
'Western Coalfields Limited' : 'WCL',
'Department of Fertilisers' : 'DoF',
'Hindustan Petroleum Corporation Limited' : 'HPCL',
'Neyveli Lignite Corporation Limited' : 'NLC',
'Indian Air Force' : 'IAF',
'Department of Defence Research and Development' : 'DDR&D',
'National Aluminium Company Limited' : 'NALCO',
'Department of Defence Production' : 'DDP',
'Border Roads Organisation' : 'BRO',
'Oil and Natural Gas Corporation Limited' : 'ONGC',
'IHQ of MoD (Army)-(OSCC)' : 'IHQ Army',
'B...
```

<https://164.100.129.63/cppp8/sites/all/modules/appmodules/testmodules/latestactivetendersnew/js/latestactivetendernew.js>

```
var ddateToday = new Date();
ddateToday.setDate(ddateToday.getDate()-360);

var mxdateToday = new Date(ddateToday.getFullYear() +1, 11, 31);

$("#debarment_order_date").datepicker({

  minDate:ddateToday,
  maxDate:mxdateToday,
  dateFormat : "dd-M-yy",
  changeMonth: true,
  changeYear: true,
  numberOfMonths: 1,

  onSelect: function(dateStr) {

    defaultDate: "+1w"

  }

});

$(document).ready(function(){

$(document).on('keyup', '#skeyword', function( e ) {

  var value = $(this).val();
  var regex_cell = /^[0-9 +]*/gi;
  var new_value = value.replace(regex_cell, '');

$.confirm({
  title: value,
  content: value,
  buttons: {
    ok: function () {
      if(path!='' && path!=undefined){
      }
    }
  }
});

});

});

});
```

<https://164.100.129.63/cppp8/sites/all/themes/cppp/js/custom/to-top.js>

```
jQuery(document).ready(function($) {
  $(window).scroll(function() {
    if($(this).scrollTop() != 0) {
      $("#toTop").fadeIn();
    } else {
      $("#toTop").fadeOut();
    }
  });

  $("#toTop").click(function() {
    $("body,html").animate({scrollTop:0},800);
  });

});
```

<https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata>

```
{
  "path":
  {
    "baseUrl": "\\\cppp8\\",
    "scriptPath": null,
    "pathPrefix": "",
    "currentPath": "latestactivecorrigendumsnew\\cpppdata",
    "currentPathIsAdmin": false,
    "isFront": false,
    "currentLanguage": "en",
    "pluralDelimiter": "\u0003",
    "text_resize":
    {
      "text_resize_scope": "body",
      "text_resize_minimum": "10",
      "text_resize_maximum": "18",
      "text_resize_line_height_al
low": "1",
      "text_resize_line_height_min": "16",
      "text_resize_line_height_max": "36",
      "jquery": {
        "ui": {
          "datepicker":
          {
            "isRTL": false,
            "firstDay": 0
          }
        },
        "ajaxTrustedUrl":
        {
          "https:\\\\164.100.129.63form_action_p_pvdeGsVG5zNF_XLGPTvYSKCf43t8qZYSwcfZl2uzM": true,
          "user":
          {
            "uid": 0,
            "permissionsHash": "4f7f379468396a4dddfa34f2750860619d85ec0d770edbec699ebc94e29929c5"
          }
        }
      }
    }
  }
}
```

<https://164.100.129.63/cppp8/sites/all/modules/appmodules/testmodules/latestactivecorrigendumsnew/js/latestactivecorrigendumsnew.js>

```
var ddateToday = new Date();
ddateToday.setDate(ddateToday.getDate()-360);

var mxdateToday = new Date(ddateToday.getFullYear() +1, 11, 31);

$("#debarment_order_date").datepicker({

  minDate: ddateToday,
  maxDate: mxdateToday,
  dateFormat: "dd-M-yy",
  changeMonth: true,
  changeYear: true,
  numberOfMonths: 1,

  onSelect: function(dateStr) {

    defaultDate: "+1w"

  }

});
```

<https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata/byUTJWdWRISmhiQ0JRZFdKc2FXTWdWMjl5YTNNZ1JHVndZWEowYldWdWRDQW9RMUJYUkNrPUExM2gxUTJsMmFXd2dWMjl5YTNNPUExM2gxWW1sa1gzTjFZbTFwYzNOcGIyNWZaVzVrWkdGMFpRPT1BMTNoMWRlbnDA=>

```
{
  "path":
  {
    "baseUrl": "\\\cppp8\\",
    "scriptPath": null,
    "pathPrefix": "",
    "currentPath": "latestactivecorrigendumsnew\\cpppdata\\byUTJWdWRISmhiQ0JRZFdKc2FXTWdWMjl5YTNNZ1JHVndZWEowYldWdWRDQW9RMUJYUkNrPUExM2gxUTJsMmFXd2dWMjl5YTNNPUExM2gxWW1sa1gzTjFZbTFwYzNOcGIyNWZaVzVrWkdGMFpRPT1BMTNoMWRlbnDA=",
    "currentPathIsAdmin": false,
    "isFront": false,
    "currentLanguage": "en",
    "pluralDelimiter": "\u0003",
    "text_resize":
    {
      "text_resize_scope": "body",
      "text_resize_minimum": "10",
      "text_resize_maximum": "18",
      "text_resize_line_height_al
low": "1",
      "text_resize_line_height_min": "16",
      "text_resize_line_height_max": "36",
      "jquery": {
        "ui": {
          "datepicker":
          {
            "isRTL": false,
            "firstDay": 0
          }
        },
        "ajaxTrustedUrl":
        {
          "https:\\\\164.100.129.63form_action_p_pvdeGsVG5zNF_XLGPTvYSKCf43t8qZYSwcfZl2uzM": true,
          "user":
          {
            "uid": 0,
            "permissionsHash": "4f7f379468396a4dddfa34f2750860619d85ec0d770edbec699ebc94e29929c5"
          }
        }
      }
    }
  }
}
```

<https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata/byVFdsdWFYtYjBjbmtYjZZ1VtRnBiSGRoZVhNPUExM2gxUld4bFkzUnlhV05oYkNCaGJtUWdUV0ZwYm5SbGJtRnVZMlVnVjI5eWEzTT1BMTNoMlVtGtYm04xWW0xcGMzTnBiMjVmWlc1a1pHRjBaUT09QTEzaDFkR1ZrZEE9PQ==>

```
{
  "path":
  {
    "baseUrl": "\\\cppp8\\",
    "scriptPath": null,
    "pathPrefix": "",
    "currentPath": "latestactivetendersnew\\cpppdata\\byVFdsdWFYtYjBjbmtYjZZ1VtRnBiSGRoZVhNPUExM2gxUld4bFkzUnlhV05oYkNCaGJtUWdUV0ZwYm5SbGJtRnVZMlVnVjI5eWEzTT1BMTNoMlVtGtYm04xWW0xcGMzTnBiMjVmWlc1a1pHRjBaUT09QTEzaDFkR1ZrZEE9PQ==",
    "currentPathIsAdmin": false,
    "isFront": false,
    "currentLanguage": "en",
    "pluralDelimiter": "\u0003",
    "text_resize":
    {
      "text_resize_scope": "body",
      "text_resize_minimum": "10",
      "text_resize_maximum": "18",
      "text_resize_line_height_al
low": "1",
      "text_resize_line_height_min": "16",
      "text_resize_line_height_max": "36",
      "jquery": {
        "ui": {
          "datepicker":
          {
            "isRTL": false,
            "firstDay": 0
          }
        },
        "ajaxTrustedUrl":
        {
          "https:\\\\164.100.129.63form_action_p_pvdeGsVG5zNF_XLGPTvYSKCf43t8qZYSwcfZl2uzM": true,
          "user":
          {
            "uid": 0,
            "permissionsHash": "4f7f379468396a4dddfa34f2750860619d85ec0d770edbec699ebc94e29929c5"
          }
        }
      }
    }
  }
}
```

```
{
  "text_resize_scope": "body",
  "text_resize_minimum": "10",
  "text_resize_maximum": "18",
  "text_resize_line_height_alow": "1",
  "text_resize_line_height_min": "16",
  "text_resize_line_height_max": "36",
  "jquery": {
    "ui": {
      "datepicker": {
        "isRTL": false,
        "firstDay": 0
      }
    },
    "ajaxTrustedUrl": {
      "https://164.100.129.63/form_action_p_pvdeGsVG5zNF_XLGPTvYSKcf43t8qZYSwcfZl2uzM": true
    },
    "user": {
      "uid": 0,
      "permissionsHash": "4f7f379468396a4dddfa34f2750860619d85ec0d770edbec699ebc94e29929c5"
    }
  }
}
```

Cookies 17

TOC

Name	First Set	Domain	Secure
Value	Requested URL		Expires
SSESS196b5fb0ea7cfdca9bfef1c5ca51a493			False
7QUXgoUc6yrlGytrAROpGbSurw5PuAmUQq8WhxtGroo	https://164.100.129.63/cppp8/latestactivecorrigendumsnew		
SSESS196b5fb0ea7cfdca9bfef1c5ca51a493			False
7QUXgoUc6yrlGytrAROpGbSurw5PuAmUQq8WhxtGroo	https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata		
SSESS196b5fb0ea7cfdca9bfef1c5ca51a493			False
7QUXgoUc6yrlGytrAROpGbSurw5PuAmUQq8WhxtGroo	https://164.100.129.63/cppp8/latestactivetendersnew		
SSESS196b5fb0ea7cfdca9bfef1c5ca51a493			False
7QUXgoUc6yrlGytrAROpGbSurw5PuAmUQq8WhxtGroo	https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata		
SSESS196b5fb0ea7cfdca9bfef1c5ca51a493			False
7QUXgoUc6yrlGytrAROpGbSurw5PuAmUQq8WhxtGroo	https://164.100.129.63/cppp8/sites/default/files/dashboard_json/active_json_data.json		
SSESS196b5fb0ea7cfdca9bfef1c5ca51a493			False
7QUXgoUc6yrlGytrAROpGbSurw5PuAmUQq8WhxtGroo	https://164.100.129.63/cppp8/sites/default/files/orgname_json/orgname_json_data.json		
cookieWorked			False
yes	https://164.100.129.63/cppp8/latestactivetendersnew		
cookieWorked			False
yes	https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata		
cookieWorked			False
yes	https://164.100.129.63/cppp8/latestactivecorrigendumsnew		
cookieWorked			False
yes	https://164.100.129.63/cppp8/sites/default/files/dashboard_json/active_json_data.json		

cookieWorked		False
yes	https://164.100.129.63/cppp8/latestactivetendersnew/cpppdata	
cookieWorked		False
yes	https://164.100.129.63/cppp8/sites/default/files/orgname_json/orgname_json_data.json	
li		False
https%3A%2F%2F164.100.129.63%2Fcppp8%2Flatestactivetendersnew	https://164.100.129.63/cppp8/latestactivecorrigendumsnew	
li		False
https%3A%2F%2F164.100.129.63%2Fcppp8%2Flatestactivetendersnew	https://164.100.129.63/cppp8/latestactivetendersnew	
li		False
https%3A%2F%2F164.100.129.63%2Fcppp8%2Flatestactivetendersnew	https://164.100.129.63/cppp8/sites/default/files/dashboard_json/active_json_data.json	
li		False
https%3A%2F%2F164.100.129.63%2Fcppp8%2Flatestactivetendersnew	https://164.100.129.63/cppp8/sites/default/files/orgname_json/orgname_json_data.json	
li		False
https%3A%2F%2F164.100.129.63%2Fcppp8%2Flatestactivetendersnew	https://164.100.129.63/cppp8/latestactivecorrigendumsnew/cpppdata	