Web Application Security Testing of National e-Vidhan Application

Level - 2

Test Url : https://cms.neva.gov.in/

July,2023

AAA Technologies Ltd
278-280, F Wing, Solaris-1,
Saki Vihar Road, Opp. L & T Gate No. 6,
Powai, Andheri (East),
Mumbai 400 072, INDIA
Tel: + 91 22 28573815 / 16
Fax: + 91 22 40152501
co.in
co.

Document Reference

Item	Description
Document Title	Web Application Security Testing of National e-Vidhan Application
Client	NICSI
Report Number	1
Version No.	2.0
File Name	Web Application Security Testing Level 1 Report of National e-Vidhan Application.pdf
Type	Pdf Document
Status	Final

Document Control Status

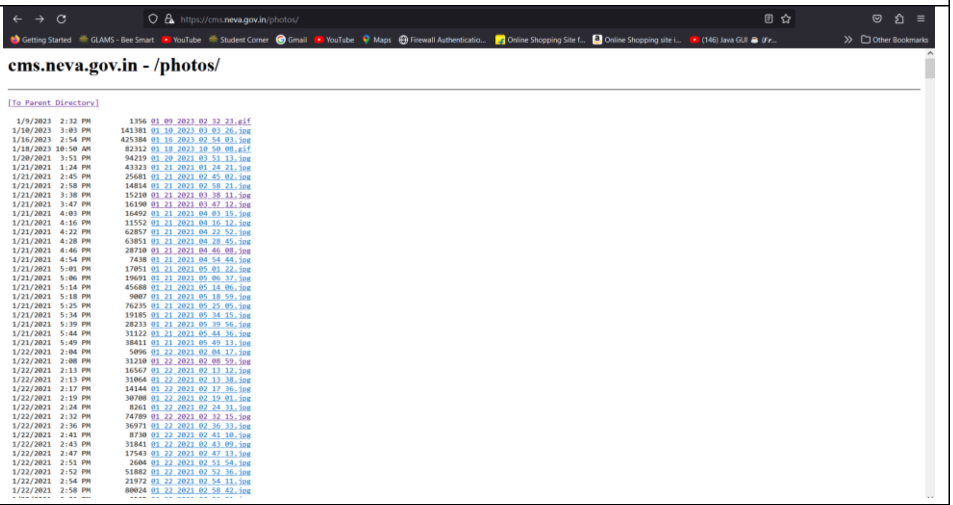
Change No.	Date	Prepared by
1.0	05/06/2023	AAA Technologies Limited
2.0	25/07/2023	AAA Technologies Limited

Table of Contents

S.No	Vulnerabilities Name	Level -1	Level -2
1.	Directory Traversal		**New**
2.	Arbitrary File Upload		**New**
3.	E-tag Information Disclosure	**Open**	**Open**
4.	Referrer – Policy not implemented		**New**
5.	Multiple Browser Login	**Open**	**Open**
6.	http security headers are not implemented in the application	**Open**	**Open**
7.	Dangerous Http Methods Enabled	**Open**	**Open**
8.	Web Server Information Disclosure	**Open**	**Open**
9.	Max. Length of Input Field is not defined		**New**
10.	Password History not maintained		**New**
11.	Outdated version of jQuery	**Open**	**Open**
12.	Vulnerable version of Bootstrap	**Open**	**Open**
13.	Path set to default		**New**

High

1. Directory Traversal

Vulnerability Title: Directory Traversal	
Risk	**High**
Abstract	It was observed that the attackers is able to access restricted directories and execute commands outside of the web server's root directory
CWE	CWE_35
Ease of Exploitation	Medium
Impact	An attacker can step out of the root directory and access files in other directories. As a result, attackers might view restricted files or execute commands, leading to a full compromise of the Web server.
Recommendations	It is recommended to [1] Ensure that the requested file resides in the virtual path of the web server. [2] Make sure that only certain extensions can be opened [3] Remove special characters (Meta-characters) from the user's input. [4] Use 'explicit open' mode for files in Perl CGI Scripts.
Snapshot	
Affected Site	**Throughout the Application.**

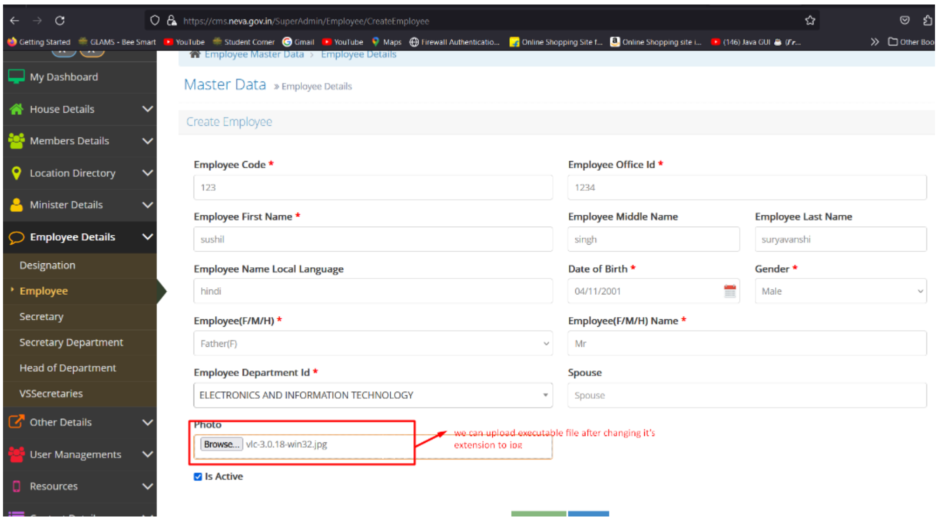
https://cms.neva.gov.in/photos/
Getting Started
GLAMS - Bee Smart
YouTube
Student Corner
Gmail
YouTube
Maps
Firewall Authenticatio...
Online Shopping Site f...
Online Shopping site i...
(146) Java GUI
Other Bookmarks

cms.neva.gov.in - /photos/

[To Parent Directory]

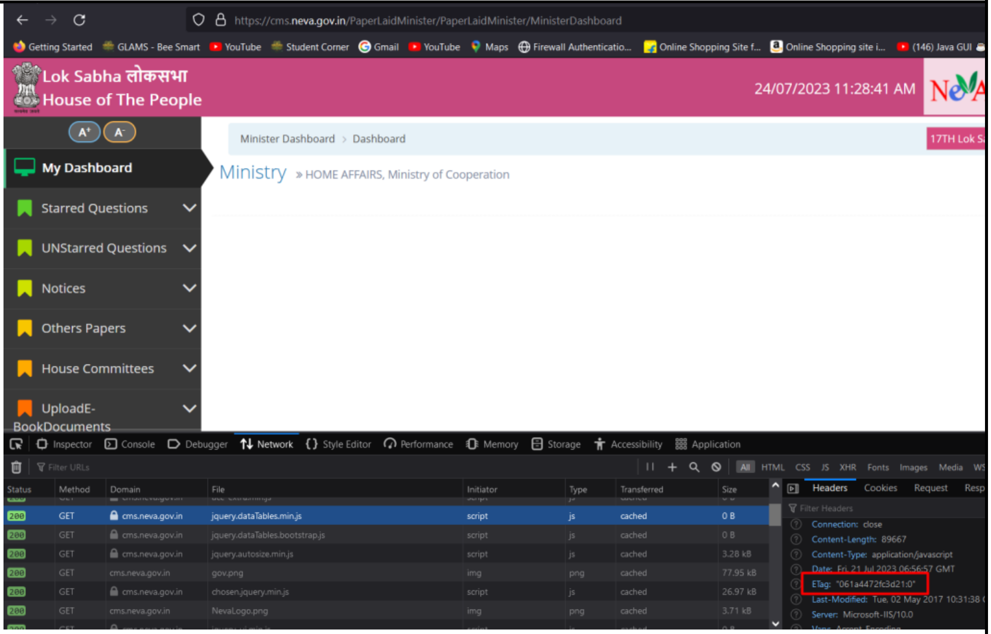
```
 1/9/2023  2:32 PM         1356 01_09_2023_02_32_23.gif
1/10/2023  3:03 PM       141381 01_10_2023_03_03_26.jpg
1/16/2023  2:54 PM       425384 01_16_2023_02_54_03.jpg
1/18/2023 10:50 AM        82312 01_18_2023_10_50_08.gif
1/20/2021  3:51 PM        94219 01_20_2021_03_51_13.jpg
1/21/2021  1:24 PM        43323 01_21_2021_01_24_21.jpg
1/21/2021  2:45 PM        25681 01_21_2021_02_45_02.jpg
1/21/2021  2:58 PM        14814 01_21_2021_02_58_21.jpg
1/21/2021  3:38 PM        15210 01_21_2021_03_38_11.jpg
1/21/2021  3:47 PM        16190 01_21_2021_03_47_12.jpg
1/21/2021  4:03 PM        16492 01_21_2021_04_03_15.jpg
1/21/2021  4:16 PM        11552 01_21_2021_04_16_12.jpg
1/21/2021  4:22 PM        62857 01_21_2021_04_22_52.jpg
1/21/2021  4:28 PM        63851 01_21_2021_04_28_45.jpg
1/21/2021  4:46 PM        28710 01_21_2021_04_46_08.jpg
1/21/2021  4:54 PM         7438 01_21_2021_04_54_44.jpg
1/21/2021  5:01 PM        17051 01_21_2021_05_01_22.jpg
1/21/2021  5:06 PM        19691 01_21_2021_05_06_37.jpg
1/21/2021  5:14 PM        45688 01_21_2021_05_14_06.jpg
1/21/2021  5:18 PM         9007 01_21_2021_05_18_59.jpg
1/21/2021  5:25 PM        76235 01_21_2021_05_25_05.jpg
1/21/2021  5:34 PM        19185 01_21_2021_05_34_15.jpg
1/21/2021  5:39 PM        28233 01_21_2021_05_39_56.jpg
1/21/2021  5:44 PM        31122 01_21_2021_05_44_36.jpg
1/21/2021  5:49 PM        38411 01_21_2021_05_49_13.jpg
1/22/2021  2:04 PM         5096 01_22_2021_02_04_17.jpg
1/22/2021  2:08 PM        31210 01_22_2021_02_08_59.jpg
1/22/2021  2:13 PM        16567 01_22_2021_02_13_12.jpg
1/22/2021  2:13 PM        31064 01_22_2021_02_13_38.jpg
1/22/2021  2:17 PM        14144 01_22_2021_02_17_36.jpg
1/22/2021  2:19 PM        30708 01_22_2021_02_19_01.jpg
1/22/2021  2:24 PM         8261 01_22_2021_02_24_31.jpg
1/22/2021  2:32 PM        74789 01_22_2021_02_32_15.jpg
1/22/2021  2:36 PM        36971 01_22_2021_02_36_33.jpg
1/22/2021  2:41 PM         8730 01_22_2021_02_41_10.jpg
1/22/2021  2:43 PM        31841 01_22_2021_02_43_09.jpg
1/22/2021  2:47 PM        17543 01_22_2021_02_47_13.jpg
1/22/2021  2:51 PM         2604 01_22_2021_02_51_54.jpg
1/22/2021  2:52 PM        51882 01_22_2021_02_52_36.jpg
1/22/2021  2:54 PM        21972 01_22_2021_02_54_11.jpg
1/22/2021  2:58 PM        80024 01_22_2021_02_58_42.jpg
```

2. Arbitrary File Upload

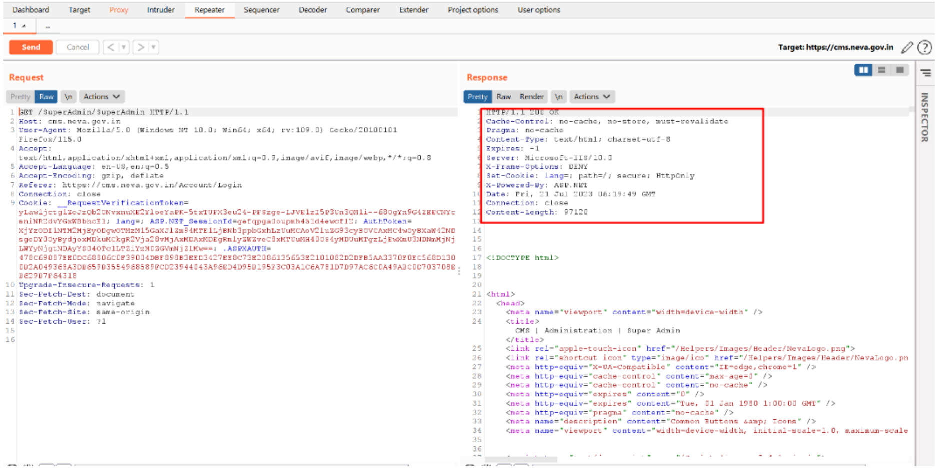
Vulnerability Title: Arbitrary File Upload	
Risk	**High**
Abstract	It was observed that the page contains functionality to handle file uploads and file management.
CWE	CWE_434
Ease of Exploitation	Easy
Impact	An attacker could use this functionality to upload malicious executable files on the system. To test file upload capabilities.
Recommendations	It is recommended to allow specific file format to upload the file
Snapshot	 https://cms.neva.gov.in/SuperAdmin/Employee/CreateEmployee Employee Master Data > Employee Details Master Data » Employee Details Create Employee Employee Code * 123 Employee Office Id * 1234 Employee First Name * sushil Employee Middle Name singh Employee Last Name suryavanshi Employee Name Local Language hindi Date of Birth * 04/11/2001 Gender * Male Employee(F/M/H) * Father(F) Employee(F/M/H) Name * Mr Employee Department Id * ELECTRONICS AND INFORMATION TECHNOLOGY Spouse Spouse Photo Browse... vlc-3.0.18-win32.jpg we can upload executable file after changing it's extension to jpg ☑ Is Active
Affected Site	**Throughout the Application.**

Medium

3. E-tag Information Disclosure

Vulnerability Title: E-tag Information Disclosure	
Risk	**Medium**
Abstract	It was observed that the Server Responds with E-tag Information Disclosure Vulnerability
CVE	-----
Ease of Exploitation	Medium
Impact	An attacker can make use of the Sensitive Information Provided and could proceed with advanced attacks.
Recommendations	It is recommended to Modify the HTTP ETag header of the web server to not include file Inodes in the ETag header calculation
Snapshot	 https://cms.neva.gov.in/PaperLaidMinister/PaperLaidMinister/MinisterDashboard Lok Sabha लोकसभा House of The People 24/07/2023 11:28:41 AM Minister Dashboard › Dashboard Ministry » HOME AFFAIRS, Ministry of Cooperation Status | Method | Domain | File | Initiator | Type | Transferred | Size 200 | GET | cms.neva.gov.in | jquery.dataTables.min.js | script | js | cached | 0 B 200 | GET | cms.neva.gov.in | jquery.dataTables.bootstrap.js | script | js | cached | 0 B 200 | GET | cms.neva.gov.in | jquery.autosize.min.js | script | js | cached | 3.28 kB 200 | GET | cms.neva.gov.in | gov.png | img | png | cached | 77.95 kB 200 | GET | cms.neva.gov.in | chosen.jquery.min.js | script | js | cached | 26.97 kB 200 | GET | cms.neva.gov.in | NevaLogo.png | img | png | cached | 3.71 kB Connection: close Content-Length: 89667 Content-Type: application/javascript Date: Fri, 21 Jul 2023 06:56:57 GMT ETag: "061a4472fc3d21:0" Last-Modified: Tue, 02 May 2017 10:31:38 Server: Microsoft-IIS/10.0 Getting Started GLAMS - Bee Smart YouTube Student Corner Gmail YouTube Maps Firewall Authenticatio... Online Shopping Site f... Online Shopping site i... (146) Java GUI A+ A- 17TH Lok S My Dashboard Starred Questions UNStarred Questions Notices Others Papers House Committees UploadE-BookDocuments Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application Filter URLs All HTML CSS JS XHR Fonts Images Media Headers Cookies Request Filter Headers
Compliance Status	**Throughout the Application.**
Compliance Status	**Open**

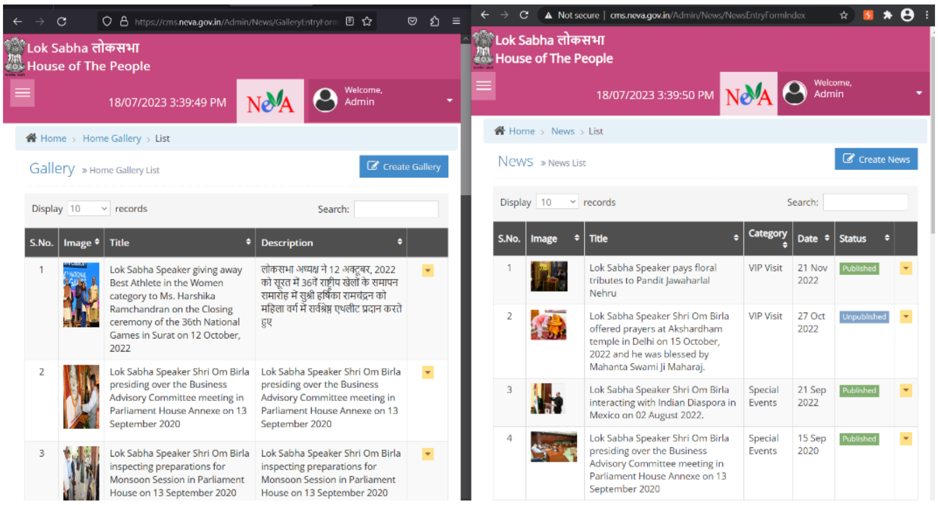
4. Referrer - Policy Not Implemented In The Application

Vulnerability Title: Referrer - Policy Not Implemented	
Risk	**Medium**
Abstract	It was observed that no Referrer-Policy header implemented .
CWE	CWE - 200
Ease of Exploitation	Medium
Impact	Referer header is a request header that indicates the site which the traffic originated from . If there is no adequated prevention in place, the URL itself , and even sensitive information contained in the URL will be leaked to the cross – site .
Recommendations	It is recommended to implement a Refferer-Policy by using Referrer-Policy response header or by declaring it in meta tags.
Snapshot	
Affected Site	**Throughout the application**

```
GET /SuperAdmin/SuperAdmin HTTP/1.1
Host: cms.neva.gov.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://cms.neva.gov.in/Account/Login
Connection: close
Cookie: __RequestVerificationToken=
yLaw1jctglZoJzQb2UNvxnuXE2YloeYaPK-5txTUFX3eu24-PFSzge-LJVE1zI5P3Un3QMli--68OgYn9G4ZEECNYc
aniNRZdvYGxWBbhcZ1; lang=; ASP.NET_SessionId=gefqpga0oupmh451d4ewcf1Z; AuthToken=
XjYzODI1NTM2MjEyODgwOTMzM15GaXJ1Zm94MTE1LjBNb3ppbGxhLzUuMCAoV2luZG93cyBOVCAxMC4wOyBXaW42ND
sgeDY0OyBydjoxMDkuMCkgR2Vja28vMjAxMDAxMDEgRmlyZWZveC8xMTUuMH40OS4yMDUuMTgzLjEwXnU3NDNmMjNj
LWYyNjgtNDAyYS04OTc1LTZiYzM0ZGVmNjZ1Mw==; .ASPXAUTH=
478C69087EE0DC68806C0F39084DBF898B3EED3427EE8C73E2086135653E2101082D2DFB5AA3370F0EC568D130
0BZA04936EA3DB659B3554968585FCD2394443A96ED4D95B195F3C03A1C6A781D7D97AC8C0A49ABC0D703708E
B629B7F84318
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-IIS/10.0
X-Frame-Options: DENY
Set-Cookie: lang=; path=/; secure; HttpOnly
X-Powered-By: ASP.NET
Date: Fri, 21 Jul 2023 06:19:49 GMT
Connection: close
Content-Length: 97120



<!DOCTYPE html>



<html>
  <head>
    <meta name="viewport" content="width=device-width" />
    <title>
      CMS | Administration | Super Admin
    </title>
    <link rel="apple-touch-icon" href="/Helpers/Images/Header/NevaLogo.png">
    <link rel="shortcut icon" type="image/ico" href="/Helpers/Images/Header/NevaLogo.pn
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
    <meta http-equiv="cache-control" content="max-age=0" />
    <meta http-equiv="cache-control" content="no-cache" />
    <meta http-equiv="expires" content="0" />
    <meta http-equiv="expires" content="Tue, 01 Jan 1980 1:00:00 GMT" />
    <meta http-equiv="pragma" content="no-cache" />
    <meta name="description" content="Common Buttons &amp; Icons" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale
```

5. Multiple Browser Login

Vulnerability Title: Multiple Browser Login of Admin at the same	
Risk	**Medium**
Abstract	It is observed that the same user can login into via multiple browsers.
CVE	-----
Ease of Exploitation	Medium
Impact	The attacker can use the same login ID for exploitation even if the ID is active.
Recommendations	It is recommended to restrict multiple browser login for admin at the same time.
Snapshot	
Affected Site	**Throughout the application**
Compliance Status	**Open**

https://cms.neva.gov.in/Admin/News/GalleryEntryForm

Lok Sabha लोकसभा
House of The People

18/07/2023 3:39:49 PM

Welcome,
Admin

Home › Home Gallery › List

Gallery » Home Gallery List

Create Gallery

Display 10 records

Search:

S.No.	Image	Title	Description	
1		Lok Sabha Speaker giving away Best Athlete in the Women category to Ms. Harshika Ramchandran on the Closing ceremony of the 36th National Games in Surat on 12 October, 2022	लोकसभा अध्यक्ष ने 12 अक्टूबर, 2022 को सूरत में 36वें राष्ट्रीय खेलों के समापन समारोह में सुश्री हर्षिका रामचंद्रन को महिला वर्ग में सर्वश्रेष्ठ एथलीट प्रदान करते हुए	▾
2		Lok Sabha Speaker Shri Om Birla presiding over the Business Advisory Committee meeting in Parliament House Annexe on 13 September 2020	Lok Sabha Speaker Shri Om Birla presiding over the Business Advisory Committee meeting in Parliament House Annexe on 13 September 2020	▾
3		Lok Sabha Speaker Shri Om Birla inspecting preparations for Monsoon Session in Parliament House on 13 September 2020	Lok Sabha Speaker Shri Om Birla inspecting preparations for Monsoon Session in Parliament House on 13 September 2020	▾

Not secure | cms.neva.gov.in/Admin/News/NewsEntryFormIndex

Lok Sabha लोकसभा
House of The People

18/07/2023 3:39:50 PM

Welcome,
Admin

Home › News › List

News » News List

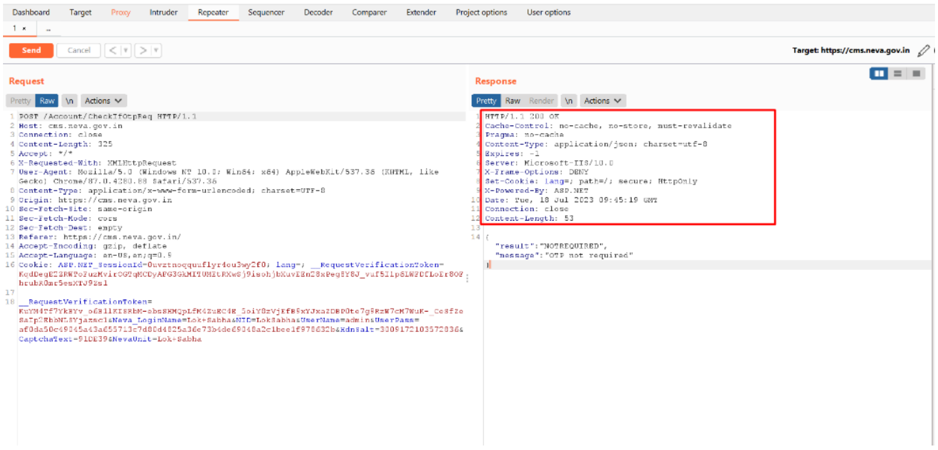
Create News

Display 10 records

Search:

S.No.	Image	Title	Category	Date	Status	
1		Lok Sabha Speaker pays floral tributes to Pandit Jawaharlal Nehru	VIP Visit	21 Nov 2022	Published	▾
2		Lok Sabha Speaker Shri Om Birla offered prayers at Akshardham temple in Delhi on 15 October, 2022 and he was blessed by Mahanta Swami Ji Maharaj.	VIP Visit	27 Oct 2022	Unpublished	▾
3		Lok Sabha Speaker Shri Om Birla interacting with Indian Diaspora in Mexico on 02 August 2022.	Special Events	21 Sep 2022	Published	▾
4		Lok Sabha Speaker Shri Om Birla presiding over the Business Advisory Committee meeting in Parliament House Annexe on 13 September 2020	Special Events	15 Sep 2020	Published	▾

6. HTTP Security Headers Are Not Implemented In The Application

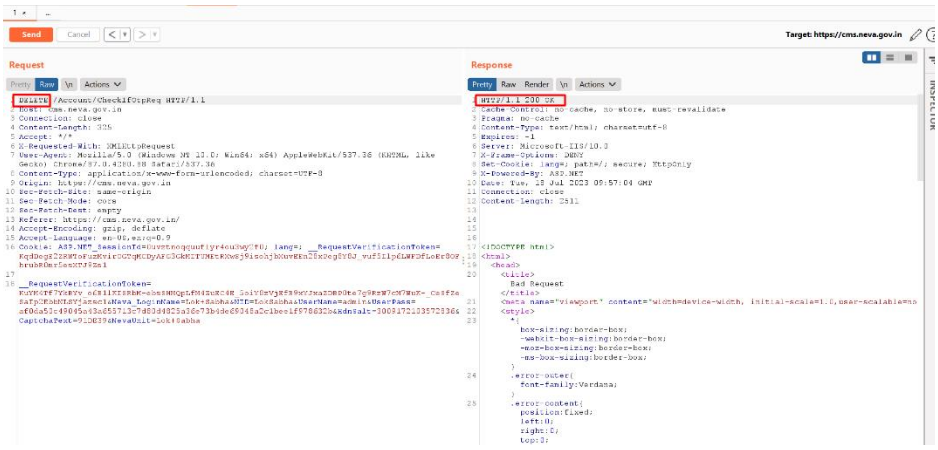
Vulnerability Title: http security headers are not implemented	
Risk	**Low**
Abstract	It was observed that the http security headers security such as X-XSS protection, Content Security Policy, Strict Transport security policy are not implemented.
Ease of Exploitation	Easy
Impact	If security headers are not implemented in the application then it may help an attacker to exploit existing vulnerabilities in application logic and result in lack of defense in depth approach to prevent security attacks.
Recommendations	• It is recommended to implement the following HTTP headers: • • X-Frame-Options: DENY/SAMEORIGIN • X-XSS-Protection: 1; mode=block [2] • X-Content-Type-Options: nosniff • Content-Type: text/html; charset=utf-8 • Strict-Transport-Security: max-age=31536000; includeSubDomains; preload • Content-security-policy:script-src'self'
Snapshot	
Affected URL's	**throughout the application**
Compliance Status	**Open**

```
POST /Account/CheckIfOtpReq HTTP/1.1
Host: cms.neva.gov.in
Connection: close
Content-Length: 325
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/87.0.4280.88 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://cms.neva.gov.in
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://cms.neva.gov.in/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: ASP.NET_SessionId=0uvztnoqquuflyr4ou3wy2f0; lang=; __RequestVerificationToken=
KqdDegEZ2RWPoFuzMvirOGTqMCDyAPG3GkMITUMZtRXwSj9isohjbXuvEEnZ8xPeg8Y8J_vuf5I1p6LWFDfLoEr8OF
hrubR0mr5esXTJ9Zs1

__RequestVerificationToken=
KuYM4Tf7YkEYv_o6B1lKISRbM-ebsSHMQpLfM4ZuEC4E_5oiY8zVjEfB9xYJxaZDBP0te7g9RzW7cM7WuK-_Ce8fZe
SaIp2RbbNLSYjazsc1&Neva_LoginName=Lok+Sabha&NID=LokSabha&UserName=admin&UserPass=
af0da50c49045a43a655713c7d80d4825a36e73b4de69048a2c1bee1f978632b&HdnSalt=330917210357283G&
CaptchaText=91DE39&NevaUnit=Lok+Sabha
```

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Content-Type: application/json; charset=utf-8
Expires: -1
Server: Microsoft-IIS/10.0
X-Frame-Options: DENY
Set-Cookie: lang=; path=/; secure; HttpOnly
X-Powered-By: ASP.NET
Date: Tue, 18 Jul 2023 09:45:19 GMT
Connection: close
Content-Length: 53

{
  "result":"NOTREQUIRED",
  "message":"OTP not required"
}
```

Low

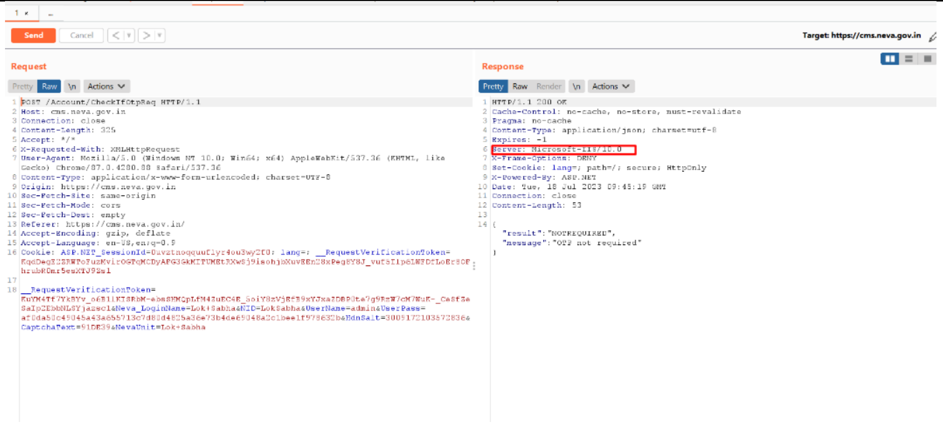
7. Dangerous Http Methods Enabled

Vulnerability Title: Dangerous HTTP Methods Enabled	
Risk	**Low**
Abstract	It was observed that Http (DELETE) method is enabled on this web server.
Ease of Exploitation	Easy
Impact	It was observed that using the DELETE method may expose sensitive information that may help a malicious user to prepare more advanced attacks
Recommendations	It is recommended to disable http dangerous methods on the web server
Snapshot	
Affected Site	**Throughout the application**
Compliance Status	**Open**

```
DELETE /Account/CheckIfOtpReq HTTP/1.1
Host: cms.neva.gov.in
Connection: close
Content-Length: 325
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/87.0.4280.88 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://cms.neva.gov.in
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://cms.neva.gov.in/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: ASP.NET_SessionId=0uvztnoqquuflyr4ou3wy2f0; lang=; __RequestVerificationToken=
KqdDogZ22RWToFuzKvirDGTqMCDyAFC3GkMITUMEtRXwSj9isohjbXuvEEn28xPeg6Y8J_vuf5Ilp6LWFDfLoEr8OF
hrubR0mr5esXTJ9Zs1

__RequestVerificationToken=
KuYM4Tf7YkBYv_o6E1lKISRbM-ebsSHMQpLfM4ZuEC4E_5oiY8zVjEfB9xYJxaZDBP0te7g9RzW7cM7WuK-_Ce8fZe
SaIp2EbbNLSYjazsc1&Neva_LoginName=Lok+Sabha&NID=LokSabha&UserName=admin&UserPass=
af0da53c49045a43a655713c7d80d4825a36e73b4de69048a2c1bee1f978632b&HdnSalt=30091721035728365&
CaptchaText=91DB39&NevaUnit=Lok+Sabha
```

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-IIS/10.0
X-Frame-Options: DENY
Set-Cookie: lang=; path=/; secure; HttpOnly
X-Powered-By: ASP.NET
Date: Tue, 18 Jul 2023 09:57:04 GMT
Connection: close
Content-Length: 2511




<!DOCTYPE html>
<html>
  <head>
    <title>
      Bad Request
    </title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0,user-scalable=no
    <style>
      *{
        box-sizing:border-box;
        -webkit-box-sizing:border-box;
        -moz-box-sizing:border-box;
        -ms-box-sizing:border-box;
      }
      .error-outer{
        font-family:Verdana;
      }
      .error-content{
        position:fixed;
        left:0;
        right:0;
        top:0;
```

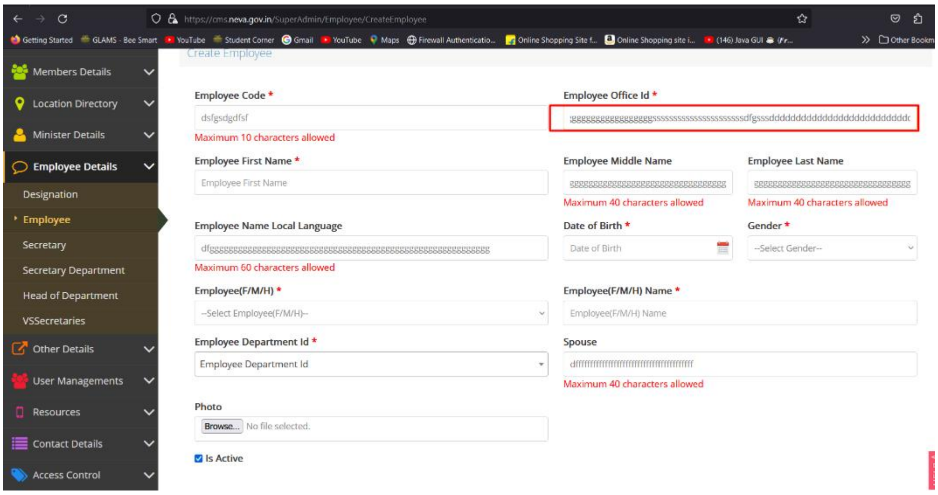
8. Web Server Information Disclosure

Vulnerability Title: Web Server Information Disclosure	
Risk	**Low**
Abstract	Banner grabbing (application is displaying Server version version which may help attacker to learn more about his target) is possible in the application.
Ease of Exploitation	Easy
Impact	Application is displaying Server version which may help attacker to learn more about his target.
Recommendations	Server version should not be displayed to the end user.
Snapshot	
Affected Site	**Throughout the application**
Compliance Status	**Open**

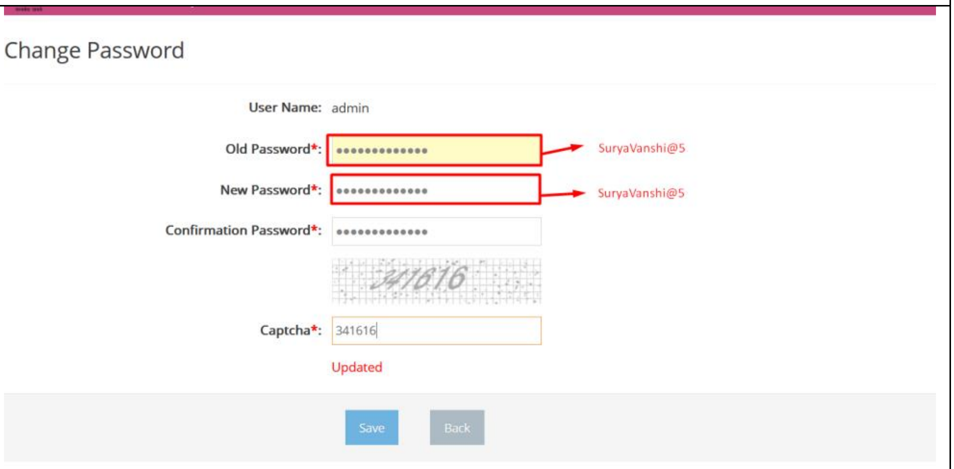
```
POST /Account/CheckIfOtpReq HTTP/1.1
Host: cms.neva.gov.in
Connection: close
Content-Length: 325
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/87.0.4280.88 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://cms.neva.gov.in
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://cms.neva.gov.in/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: ASP.NET_SessionId=0uvztnoqquuflyr4ou3wy2f0; lang=; __RequestVerificationToken=
KqdDegZZZRWToFuzMvirOGTqMCDyAFG3GkMITUMBtRXwSj9isohjbXuvEEnZ8xPegBY8J_vuf5I1p6LWFDfLoBr8OF
hrubR0mr5esXTJ92s1

__RequestVerificationToken=
KuYM4Tf7YkBYv_o6B11KISRbM-ebsSHMQpLfM4ZuEC4E_5oiY8zVjEfB9xYJxaZDBP0te7g9RzW7cM7WuK-_CeSfZe
SaIpZEbbNLSYjazscl&Neva_LoginName=Lok+Sabha&NID=LokSabha&UserName=admin&UserPass=
af0da50c45045a43a655713c7d80d4825a36e73b4de65048a2c1bee1f978632b&HdnSalt=300917210357283б&
CaptchaText=91DE39&NevaUnit=Lok+Sabha
```

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Content-Type: application/json; charset=utf-8
Expires: -1
Server: Microsoft-IIS/10.0
X-Frame-Options: DENY
Set-Cookie: lang=; path=/; secure; HttpOnly
X-Powered-By: ASP.NET
Date: Tue, 18 Jul 2023 09:45:19 GMT
Connection: close
Content-Length: 53

{
  "result":"NOTREQUIRED",
  "message":"OTP not required"
}
```

9. Max. Length Of Input Fields Is Not Defined In The Application

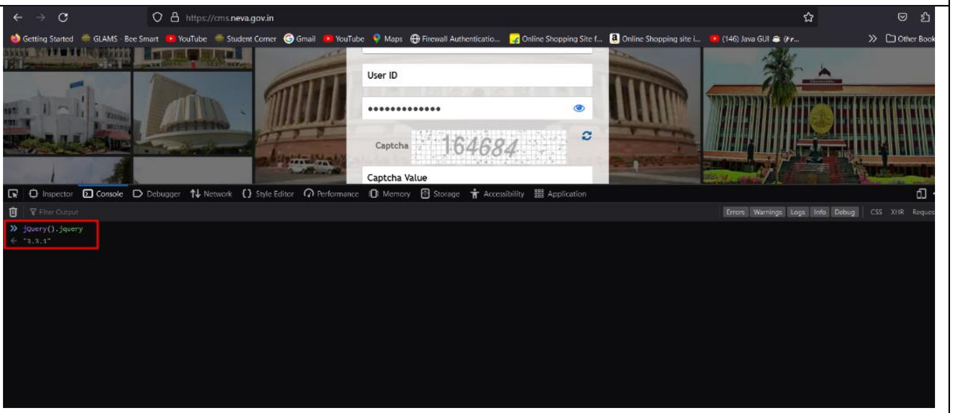
Vulnerability Title: Max. length of input field is not defined in the application	
Risk	**Low**
Abstract	It was observed that max. Length for input fields is not defined.
Ease of Exploitation	Easy
Impact	This may lead to a buffer overflow attack.
Recommendations	Length restriction for every input field should be defined at client as well as at server end.
Snapshot	 https://cms.neva.gov.in/SuperAdmin/Employee/CreateEmployee Getting Started GLAMS - Bee Smart YouTube Student Corner Gmail YouTube Maps Firewall Authenticatio... Online Shopping Site f... Online Shopping site i... (146) Java GUI (Fr... Other Bookm Members Details Location Directory Minister Details Employee Details Designation Employee Secretary Secretary Department Head of Department VSSecretaries Other Details User Managements Resources Contact Details Access Control Browse... Create Employee Employee Code * dsfgsdgdfsf Maximum 10 characters allowed Employee Office Id * ggggggggggggggggggsssssssssssssssssssssssdfgsssddddddddddddddddddddddddddc Employee First Name * Employee First Name Employee Middle Name gggggggggggggggggggggggggggggggggggggg Maximum 40 characters allowed Employee Last Name gggggggggggggggggggggggggggggggggggggg Maximum 40 characters allowed Employee Name Local Language dfgggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg Maximum 60 characters allowed Date of Birth * Date of Birth Gender * --Select Gender-- Employee(F/M/H) * --Select Employee(F/M/H)-- Employee(F/M/H) Name * Employee(F/M/H) Name Employee Department Id * Employee Department Id Spouse dffffffffffffffffffffffffffffffffffffffffffff Maximum 40 characters allowed Photo No file selected. ☑ Is Active
Affected URLs	**throughout the application**

10. Password History Is Not Maintained

Vulnerability Title: Password history is not maintained	
Risk	**Low**
Abstract	It was observed that While changing password, there is no check on password history. This allows the user to change the password to his previous password.
Ease of Exploitation	Easy
Impact	Password reuse can threaten security by giving attackers a greater opportunity in using old passwords.
Recommendations	Users should be prevented from reusing their current or previous 3 passwords. Password history should ideally be 3.
Snapshot	 Change Password User Name: admin Old Password*: ••••••••••••• SuryaVanshi@5 New Password*: ••••••••••••• SuryaVanshi@5 Confirmation Password*: ••••••••••••• Captcha*: 341616 Updated
Affected URLs	**throughout the application**

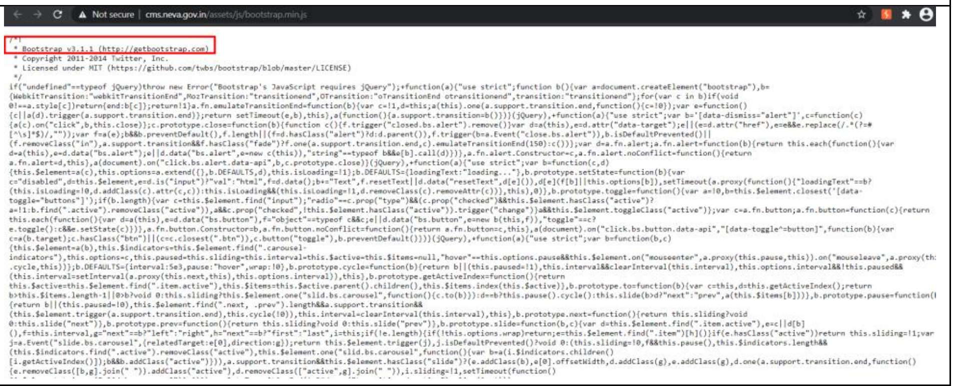
11.Outdated Version Of JQuery

Vulnerability Title: Outdated version of jQuery is used in the application	
Risk	**Low**
Abstract	It was observed that this page is using an older version of jQuery .
Ease of Exploitation	Medium
Impact	An attacker can steal the cookies as well as the user session id
Recommendations	It is recommended to update to latest version of jQuery.

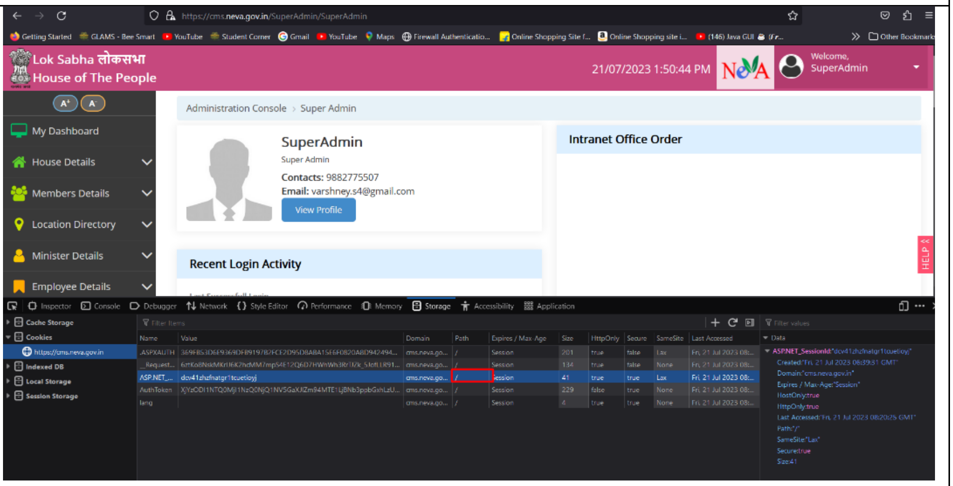
Snapshot	
	https://cms.neva.gov.in
	User ID
	Captcha
	Captcha Value
	`>> jQuery().jquery`
	`← "3.3.1"`

Affected URLs	**throughout the application**
Compliance Status	**Open**

12.Vulnerable Version Of Bootstrap

<table>
<tr><th colspan="2">Vulnerability Title: Vulnerable version of Bootstrap is used in the application</th></tr>
<tr><td>Risk</td><td><b>Low</b></td></tr>
<tr><td>Abstract</td><td>It was observed that the application is using an older version of Bootstrap i.e 3.1.1 .</td></tr>
<tr><td>Ease of Exploitation</td><td>Medium</td></tr>
<tr><td>Impact</td><td>Older version of Bootstrap may not fully support newer web technologies , CSS features, or browser versions . This can lead to inconsistencies in rendering and functionality across different browsers and devices. Compatibility issues may result in a suboptimal user experience and require additional effort to address and fix .</td></tr>
<tr><td>Recommendations</td><td>It is recommended to update to latest version of Bootstrap.</td></tr>
<tr><td>Snapshot</td><td>
Not secure | cms.neva.gov.in/assets/js/bootstrap.min.js
<pre>
/*!
 * Bootstrap v3.1.1 (http://getbootstrap.com)
 * Copyright 2011-2014 Twitter, Inc.
 * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE)
 */
if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery");+function(a){"use strict";function b(){var a=document.createElement("bootstrap"),b=
{WebkitTransition:"webkitTransitionEnd",MozTransition:"transitionend",OTransition:"oTransitionEnd otransitionend",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(a.support.transition.end,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()})}(jQuery),+function(a){"use strict";var b='[data-dismiss="alert"]',c=function(c)
{a(c).on("click",b,this.close)};c.prototype.close=function(b){function c(){f.trigger("closed.bs.alert").remove()}var d=a(this),e=d.attr("data-target");e||(e=d.attr("href"),e=e&&e.replace(/.*(?=#
[^\s]*$)/,""));var f=a(e);b&&b.preventDefault(),f.length||(f=d.hasClass("alert")?d:d.parent()),f.trigger(b=a.Event("close.bs.alert")),b.isDefaultPrevented()||
(f.removeClass("in"),a.support.transition&&f.hasClass("fade")?f.one(a.support.transition.end,c).emulateTransitionEnd(150):c())};var d=a.fn.alert;a.fn.alert=function(b){return this.each(function(){var
d=a(this),e=d.data("bs.alert");e||d.data("bs.alert",e=new c(this)),"string"==typeof b&&e[b].call(d)})},a.fn.alert.Constructor=c,a.fn.alert.noConflict=function(){return
a.fn.alert=d,this},a(document).on("click.bs.alert.data-api",b,c.prototype.close)}(jQuery),+function(a){"use strict";var b=function(c,d)
{this.$element=a(c),this.options=a.extend({},b.DEFAULTS,d),this.isLoading=!1};b.DEFAULTS={loadingText:"loading..."},b.prototype.setState=function(b){var
c="disabled",d=this.$element,e=d.is("input")?"val":"html",f=d.data();b+="Text",f.resetText||d.data("resetText",d[e]()),d[e](f[b]||this.options[b]),setTimeout(a.proxy(function(){"loadingText"==b?
(this.isLoading=!0,d.addClass(c).attr(c,c)):this.isLoading&&(this.isLoading=!1,d.removeClass(c).removeAttr(c))},this),0)},b.prototype.toggle=function(){var a=!0,b=this.$element.closest('[data-
toggle="buttons"]');if(b.length){var c=this.$element.find("input");"radio"==c.prop("type")&&(c.prop("checked")&&this.$element.hasClass("active")?
a=!1:b.find(".active").removeClass("active")),a&&c.prop("checked",!this.$element.hasClass("active")).trigger("change")}a&&this.$element.toggleClass("active")};var c=a.fn.button;a.fn.button=function(c){return
this.each(function(){var d=a(this),e=d.data("bs.button"),f="object"==typeof c&&c;e||d.data("bs.button",e=new b(this,f)),"toggle"==c?
e.toggle():c&&e.setState(c)})},a.fn.button.Constructor=b,a.fn.button.noConflict=function(){return a.fn.button=c,this},a(document).on("click.bs.button.data-api","[data-toggle^=button]",function(b){var
c=a(b.target);c.hasClass("btn")||(c=c.closest(".btn")),c.button("toggle"),b.preventDefault()})}(jQuery),+function(a){"use strict";var b=function(b,c)
{this.$element=a(b),this.$indicators=this.$element.find(".carousel-
indicators"),this.options=c,this.paused=this.sliding=this.interval=this.$active=this.$items=null,"hover"==this.options.pause&&this.$element.on("mouseenter",a.proxy(this.pause,this)).on("mouseleave",a.proxy(th
.cycle,this))};b.DEFAULTS={interval:5e3,pause:"hover",wrap:!0},b.prototype.cycle=function(b){return b||(this.paused=!1),this.interval&&clearInterval(this.interval),this.options.interval&&!this.paused&&
(this.interval=setInterval(a.proxy(this.next,this),this.options.interval)),this},b.prototype.getActiveIndex=function(){return
this.$active=this.$element.find(".item.active"),this.$items=this.$active.parent().children(),this.$items.index(this.$active)},b.prototype.to=function(b){var c=this,d=this.getActiveIndex();return
b>this.$items.length-1||0>b?void 0:this.sliding?this.$element.one("slid.bs.carousel",function(){c.to(b)}):d==b?this.pause().cycle():this.slide(b>d?"next":"prev",a(this.$items[b]))},b.prototype.pause=function(
{return b||(this.paused=!0),this.$element.find(".next, .prev").length&&a.support.transition&&
(this.$element.trigger(a.support.transition.end),this.cycle(!0)),this.interval=clearInterval(this.interval),this},b.prototype.next=function(){return this.sliding?void
0:this.slide("next")},b.prototype.prev=function(){return this.sliding?void 0:this.slide("prev")},b.prototype.slide=function(b,c){var d=this.$element.find(".item.active"),e=c||d[b]
(),f=this.interval,g="next"==b?"left":"right",h="next"==b?"first":"last",i=this;if(!e.length){if(!this.options.wrap)return;e=this.$element.find(".item")[h]()}if(e.hasClass("active"))return this.sliding=!1;var
j=a.Event("slide.bs.carousel",{relatedTarget:e[0],direction:g});return this.$element.trigger(j),j.isDefaultPrevented()?void 0:(this.sliding=!0,f&&this.pause(),this.$indicators.length&&
(this.$indicators.find(".active").removeClass("active"),this.$element.one("slid.bs.carousel",function(){var b=a(i.$indicators.children()
[i.getActiveIndex()]);b&&b.addClass("active")})),a.support.transition&&this.$element.hasClass("slide")?(e.addClass(b),e[0].offsetWidth,d.addClass(g),e.addClass(g),d.one(a.support.transition.end,function()
{e.removeClass([b,g].join(" ")).addClass("active"),d.removeClass(["active",g].join(" ")),i.sliding=!1,setTimeout(function()
</pre></td></tr>
<tr><td>Affected URLs</td><td><b>throughout the application</b></td></tr>
<tr><td>Compliance Status</td><td><b>Open</b></td></tr>
</table>

13.Path Is Set To Default In The Application

Vulnerability Title: Path is set to Default in the application	
Risk	**Low**
Abstract	It was observed that path is set to default i.e. ‘/’ in the application.
Ease of Exploitation	Easy
Impact	It is difficult to keep track of logged in users in case of any incident theft/fraud.
Recommendations	It is recommended to verify that that the path attribute, just as the Domain attribute, has not been set too loosely. Even if the Domain attribute has been configured as tight as possible, if the path is set to the root directory "/" then it can be vulnerable to less secure applications on the same server.
Snapshot	
Affected URLs	**throughout the application**

https://cms.neva.gov.in/SuperAdmin/SuperAdmin

Lok Sabha लोकसभा
House of The People

21/07/2023 1:50:44 PM

Welcome,
SuperAdmin

Administration Console › Super Admin

SuperAdmin
Super Admin
Contacts: 9882775507
Email: varshney.s4@gmail.com

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
.ASPXAUTH	369FB53D6E9369DFB9197B2FCE2D95D8ABA15E6F0820ABD942494...	cms.neva.go...	/	Session	201	true	false	Lax	Fri, 21 Jul 2023 08:...
__Request...	6ztKo8NskMKrU6K2hdMM7mpS4E12Q6D7HWnWh3RrTJZk_5JofLLR91...	cms.neva.go...	/	Session	134	true	false	None	Fri, 21 Jul 2023 08:...
ASP.NET_...	dcv41zhzfnatgr1tcuetioyj	cms.neva.go...	/	Session	41	true	true	Lax	Fri, 21 Jul 2023 08:...
AuthToken	XjYzODI1NTQ0MjI1NzQ0NjQ1NVSGaXJlZm94MTE1LjBNb3pobGxhLzU...	cms.neva.go...	/	Session	229	false	true	None	Fri, 21 Jul 2023 08:...
lang		cms.neva.go...	/	Session	4	true	true	None	Fri, 21 Jul 2023 08:...

```
ASP.NET_SessionId:"dcv41zhzfnatgr1tcuetioyj"
  Created:"Fri, 21 Jul 2023 06:39:31 GMT"
  Domain:"cms.neva.gov.in"
  Expires / Max-Age:"Session"
  HostOnly:true
  HttpOnly:true
  Last Accessed:"Fri, 21 Jul 2023 08:20:25 GMT"
  Path:"/"
  SameSite:"Lax"
  Secure:true
  Size:41
```