

Web Application Security Testing of National eVidhan Application (NeVA - CMS)

Test URL

<https://164.100.140.203>

Level-3

6th Feb 2024



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

info@aaatechnologies.co

www.aaatechnologies.co.in

Web Application Security Test
Report for National eVidhan Application
(NeVA - CMS)



Document Version Control			
Data Classification		CLASSIFIED	
Client Name		NICSI	
Document Title		Web Application Security Test Report	
Author		Parmeet Chaudhary	
Version	Date of Issue	Issued by	Change Description
1.0	22-12-2023	AAA Technologies Ltd.	Initial Issue

Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



Table of Contents

1. Session Hijacking Attack possible in the Application	7
2. Dangerous Http Method Enabled	10
3. Multiple Browser Login	12
4. Outdated version of jQuery	13
5. Vulnerable version of Bootstrap	14
6. SSL Certificate Date Expired	15
7. Weak Ciphers Enabled	17
8. HTTP Security Headers not implemented	18
9. Session Timeout Is Not Implemented	19
10. Out-of-Date version of data tables is used in the application	20
11. Out-of-Date version of jQuery UI is used in the application	21
12. Path Not Set in Cookie Attribute	23
13. Web Server Information Disclosure	24
14. HSTS (HTTP Strict Transport Security) Misconfiguration	25
15. Cross-Origin resource sharing Misconfiguration	26
16. X-Frame Options Misconfiguration	27
17. Audit Trail is not maintained	28
18. Forbidden Resource	30
19. Insecure Transportation Security Protocol Supported (TLS 1.0)	31
20. User Enumeration	32
21. E-tag	34
22. Improper Input Validation	35
23. Password Replay attack is possible	37
24. CAPTCHA is not validating at server side	39

Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



The following key findings support our assessment of the weaknesses associated with the application:

S. No.	Vulnerability Description	Level-1	Level-2	Level-3
1.	Session Hijacking Attack		Complied	Complied
2.	Dangerous Method Enabled		Not Complied	Not Complied
3.	Multiple Browser Login		Complied	Complied
4.	Outdated version of jQuery		Complied	Complied
5.	Vulnerable version of Bootstrap		Complied	Complied
6.	SSL Certificate Date Expired		Complied	Complied
7.	Weak Ciphers Enabled		Not Complied	Not Complied
8.	HTTP Security Headers not implemented		Complied	Complied
9.	Session Timeout Is Not Implemented		Exception	Complied
10.	Out-of-Date version of data tables is used in the application		Not complied	Not Complied
11.	Out-of-Date version of data tables is used in the application		Not Complied	Not Complied
12.	Out-of-Date version of jQuery UI is used in the application		Not Complied	Not Complied
13.	Web Server Information Disclosure		Complied	Complied
14.	HSTS (HTTP Strict Transport Security) Misconfiguration		Complied	Complied
15.	Cross-Origin resource sharing Misconfiguration		Complied	Complied
16.	X-Frame Options Misconfiguration		Complied	Complied
17.	Audit Trail is not maintained		Complied	Complied
18.	Forbidden Resource		Complied	Complied

Web Application Security Test
Report for National eVidhan Application
(NeVA - CMS)



S. No.	Vulnerability Description	Level-1	Level-2	Level-3
19	Insecure Transportation Security Protocol Supported (TLS 1.0)		Not Complied	Not Complied
20.	User Enumeration		Complied	Complied
21.	E-Tag		Complied	Complied
22	Improper Input Validation		Complied	Complied
23.	Password Replay attack is possible.		Complied	Complied
24.	CAPTCHA not validate in server side		New	Not Complied

High

Web Application Security Test
Report for National eVidhan Application
(NeVA - CMS)



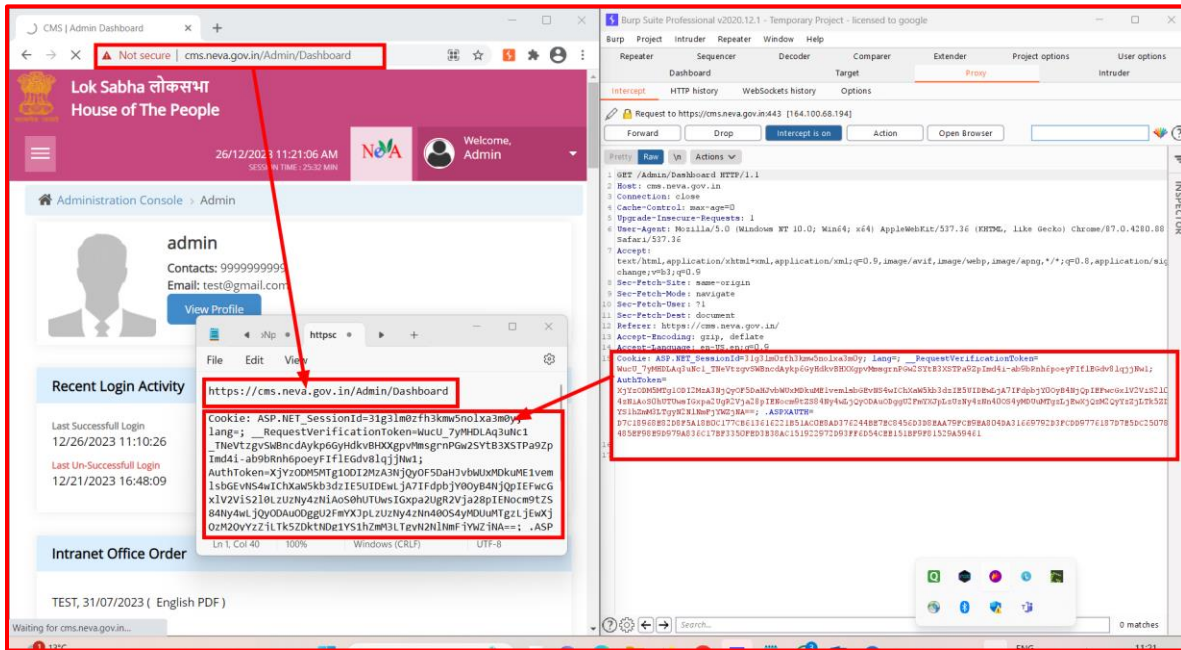
1. Session Hijacking Attack possible in the Application

Vulnerability Title: Session Hijacking Attack possible in the Application	
Risk	High
Abstract	It was observed application is vulnerable to session hijacking attack.
Ease of Exploitation	Easy
Impact	An adversary can hijack the victim's session and steal sensitive information
Recommendations	It is recommended to Introduce a token in the body of the request which is random to every request (usually the Anti-CSRF token) and map the token with the Session ID.
Snapshot	Attached Below
Affected Site	Throughout the application
Status	Complied

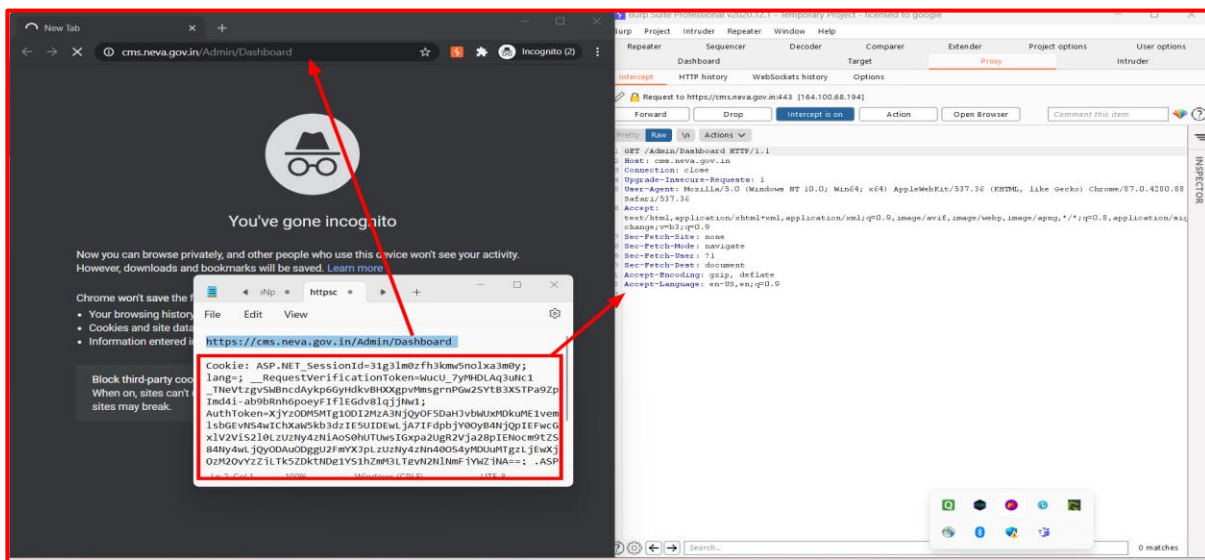
Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



Step#1 -Login into application using valid credentials and now intercept the internal page in burp suite. Now, copy the authenticated cookie and internal URL in notepad as shown below.



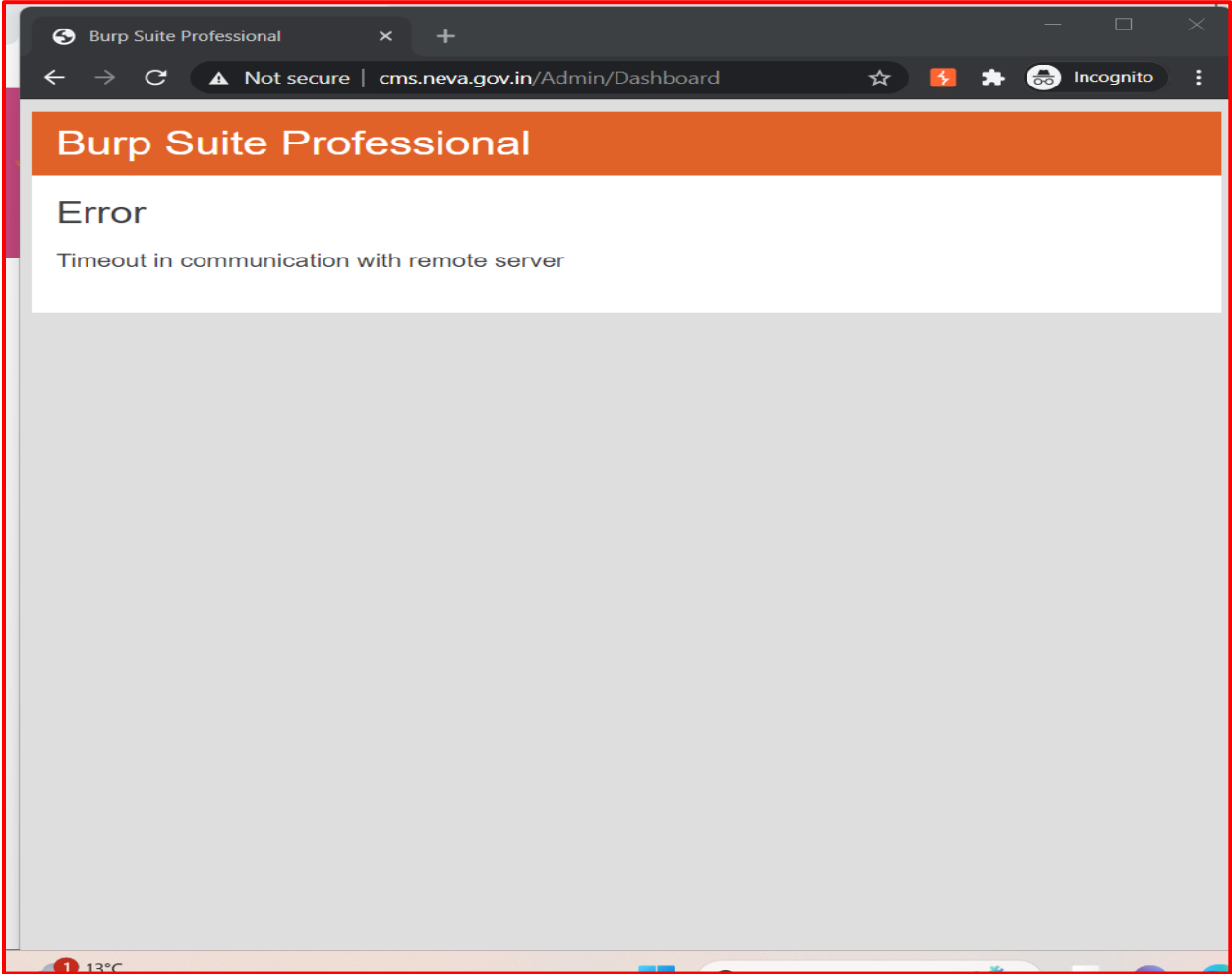
Step#2 –Now, go to another browser and paste the internal URL and intercept the request in burp suite. Now, paste the authenticated cookie as shown below and forward the request in burp suite.



Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



Step#3 -Now, you can clearly see attacker can login with session ID.



Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



2. Dangerous Http Method Enabled

Vulnerability Title: Dangerous HTTP Methods are Enabled	
Risk	High
Abstract	It was observed that Http methods are enabled on this web server.
CVE	CVE-2004-2320
Ease of Exploitation	Easy
Impact	It was observed that using the HTTP methods, it may expose sensitive information that may help an malicious user to prepare more advanced attacks
Recommendations	It is recommended to disable http dangerous methods on the web server
Snapshot	Attached Below
Affected URL	Throughout the application
Status	Not Complied

The screenshot shows the Burp Suite interface with a request and response captured. The request is highlighted in red and contains the following details:

- Request: HTTP /Admin/Notice/NoticeIndex HTTP/1.1
- Host: 164.100.140.203
- Connection: close
- Cache-Control: max-age=0
- Upgrade-Insecure-Requests: 1
- 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
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
- Sec-Fetch-Site: same-origin
- Sec-Fetch-Mode: navigate
- Sec-Fetch-User: ?1
- Sec-Fetch-Dest: document
- Referer: https://164.100.140.203/
- Accept-Encoding: gzip, deflate
- Accept-Language: en-US,en;q=0.9
- Cookie: ASE_SESSIONID=0y3xalug0xyyy0eeclcn2; lang=; _RequestVerificationToken=0Q8H17hbbccF2M9o60d1d8w573ifAmQp_Bw-Revu0M9y4Aa0F0P02W6A1N8mV-Vs-C-0bnyfEJh0e855MMed_pofz2gM0i; Auth0Yf0y0Qy8y8e6407A58j; c0F50a80y0M0H4y0M66ak0xY9I1jAgTF0p0mPod1H9T1CyM7A0M0y021shj071H92W0y0Qy8y0y0ZM0L0X0V0T10h0F0T0y0g01r0B080h0y0g0h0111ng1j; A0W010W04003T0M0m0y0M10j0Cf0y02j; 1w0A40c0M0H0e0c0Q0w0119y0e00A20y0092W0C0F00R0A0h0z00W0; ASEFA0H0F
- 70CAB52F85748c5948e48d1cc073c88f57245280dA174898A328B4478D05DF8FC4858c071170F0D1704F8D0091896ACFA858F8FF8C24A802108881F449568191859801480037F8F527977C7FA4500FC8D878074A49A2850E5CF

The response is shown on the right side of the interface, starting with 'HTTP/1.1 200 OK'.

Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



This screenshot shows a successful HTTP 1.1 200 OK response from the target URL. The response headers include:

- Cache-Control: no-cache, no-store, must-revalidate
- Pragma: no-cache, no-cache
- Content-Type: text/html; charset=utf-8
- Expires: -1
- Vary: Accept-Encoding
- Set-Cookie: LANG; path=/; secure; HttpOnly
- X-XSS-Protection: 1; mode=block
- Content-Security-Policy: default-src 'self'; connect-src *: font-src *: frame-src *: img-src
- Strict-Transport-Security: max-age=1518000; includeSubdomains
- X-Content-Type-Options: nosniff
- X-Frame-Options: SAMEORIGIN
- Referrer-Policy: strict-origin
- Access-Control-Allow-Origin: https://neva.gov.in/
- Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept
- Access-Control-Allow-Methods: GET, POST, PUT, DELETE
- Access-Control-Max-Age: 3000
- Feature-Policy: accelerometer 'none'; camera 'none'; geolocation 'none'; gyroscope 'none';
- Date: Thu, 01 Feb 2024 11:21:58 GMT

This screenshot shows a successful HTTP 1.1 200 OK response from the target URL. The response headers include:

- Cache-Control: no-cache, no-store, must-revalidate
- Pragma: no-cache, no-cache
- Content-Type: text/html; charset=utf-8
- Expires: -1
- Vary: Accept-Encoding
- Set-Cookie: LANG; path=/; secure; HttpOnly
- X-XSS-Protection: 1; mode=block
- Content-Security-Policy: default-src 'self'; connect-src *: font-src *: frame-src *: img-src
- Strict-Transport-Security: max-age=1518000; includeSubdomains
- X-Content-Type-Options: nosniff
- X-Frame-Options: SAMEORIGIN
- Referrer-Policy: strict-origin
- Access-Control-Allow-Origin: https://neva.gov.in/
- Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept
- Access-Control-Allow-Methods: GET, POST, PUT, DELETE
- Access-Control-Max-Age: 3000
- Feature-Policy: accelerometer 'none'; camera 'none'; geolocation 'none'; gyroscope 'none';
- Date: Mon, 05 Feb 2024 11:22:11 GMT

Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



3. Multiple Browser Login

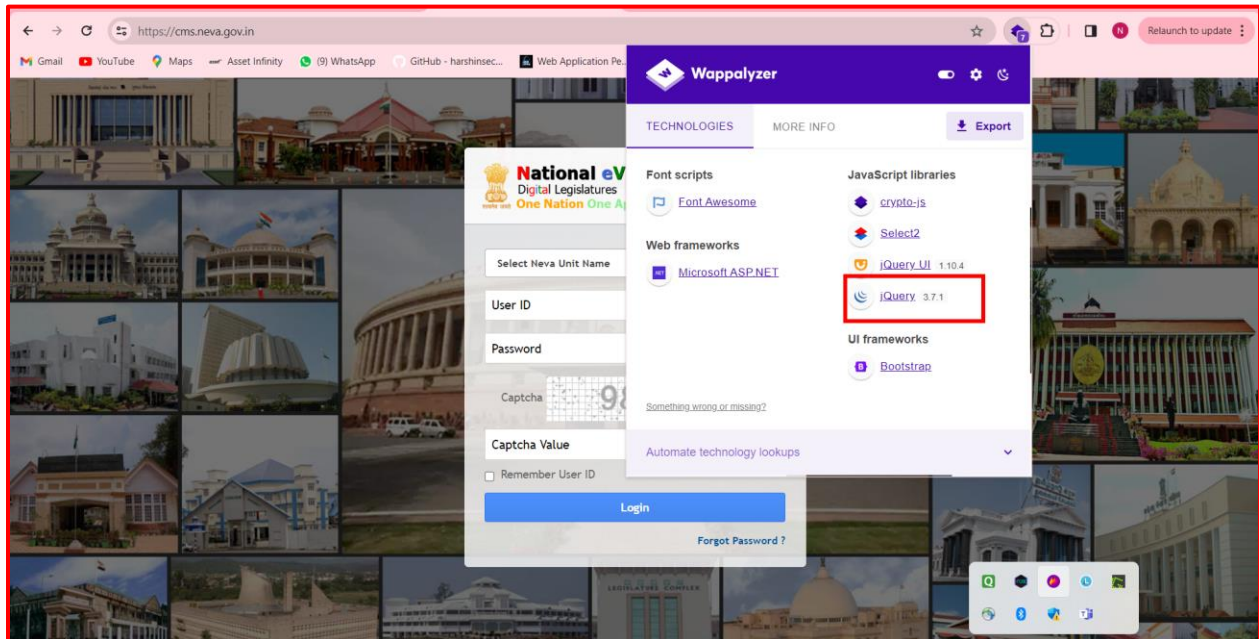
Vulnerability Title: Multiple Browser Login of Admin at the same	
Risk	High
Abstract	It is observed that the same user can login into via multiple browsers.
CWE	CWE_362
Ease of Exploitation	Medium
Impact	The attacker can use the same login ID for exploitation even if the ID is active.
Recommendations	It is recommended to restrict multiple browser login for admin at the same time.
Snapshot	
Affected Site	https://164.100.140.203
Status	Complied

Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



4. Outdated version of jQuery

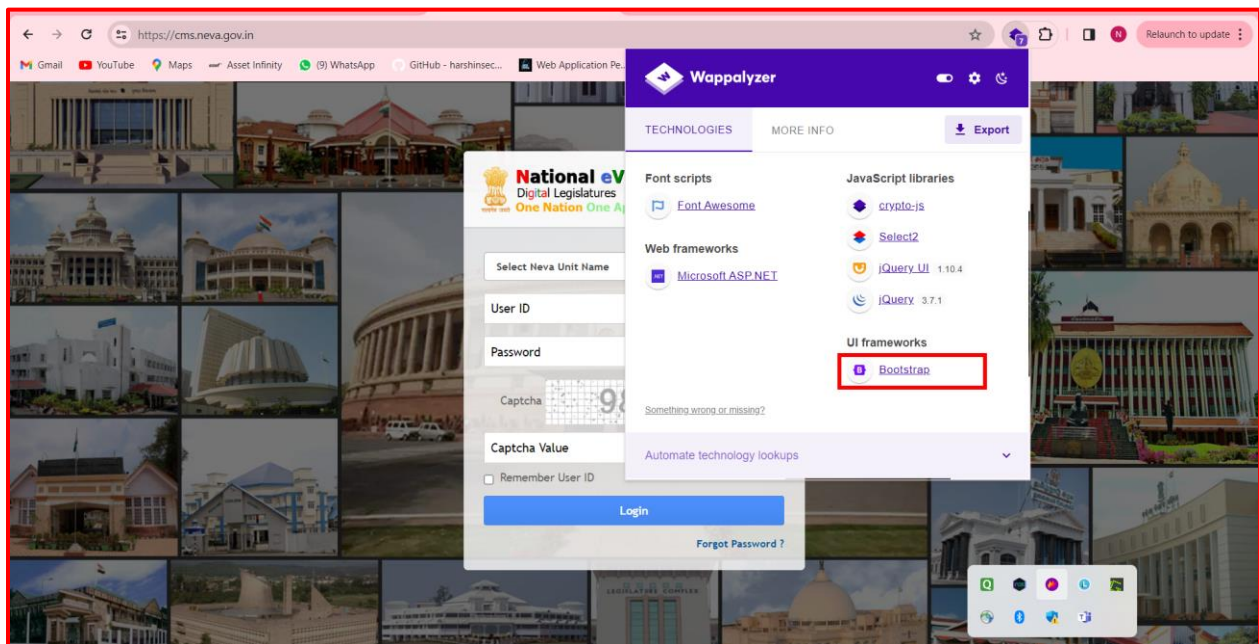
Vulnerability Title: Outdated/Vulnerable version of jQuery	
Risk	High
Abstract	It was observed that an outdated version of jQuery (3.5.0) is used.
Ease of Exploitation	Medium
Impact	An attacker can launch various attacks on application through outdated/vulnerable Version.
Recommendations	It is recommended to use latest and stable version of jQuery.
Snapshots	Attached Below
Affected URLs	Throughout the Application
Status	Complied



Web Application Security Test Report for National eVidhan Application (NeVA - CMS)

5. Vulnerable version of Bootstrap

Vulnerability Title: Vulnerable version of Bootstrap	
Risk	High
Abstract	It was observed that a vulnerable version of Bootstrap (3.1.1) is used.
Ease of Exploitation	Medium
Impact	An attacker can launch various attacks on application through vulnerable/outdated Version.
Recommendations	It is recommended to use latest and stable version of Bootstrap.
Snapshots	Attached Below
Affected URLs	Throughout the Application
Status	Complied

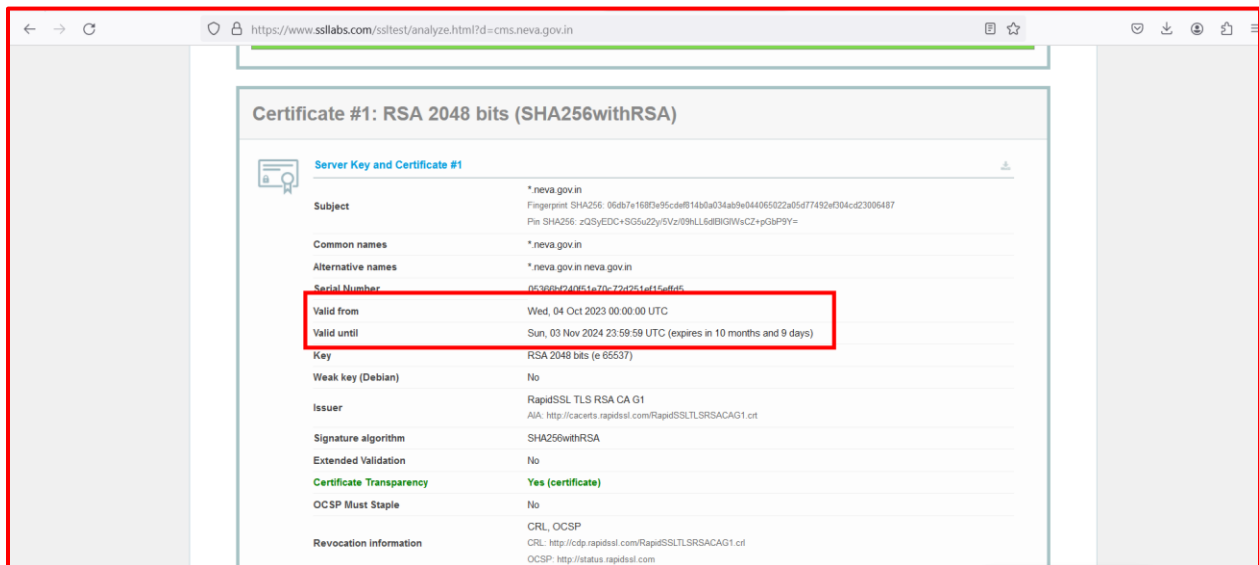


Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



6. SSL Certificate Date Expired

Vulnerability Title: SSL Certificate date expired	
Risk	High
Abstract	It was observed that the SSL certificate is expired and not valid
Ease of Exploitation	Medium
Impact	Some browsers will continue connecting to the site after presenting the user with the warning, while others will prompt the user with a dialog box requesting their approval to proceed. These warnings are extremely confusing for the typical web user, and cause most users to question the authenticity of the site they are attempting to view.
Recommendations	It is recommended to verify the Start Date and End Date of SSL Certificate
Snapshot	Attached Below
Affected Site	Throughout the Application
Status	Complied



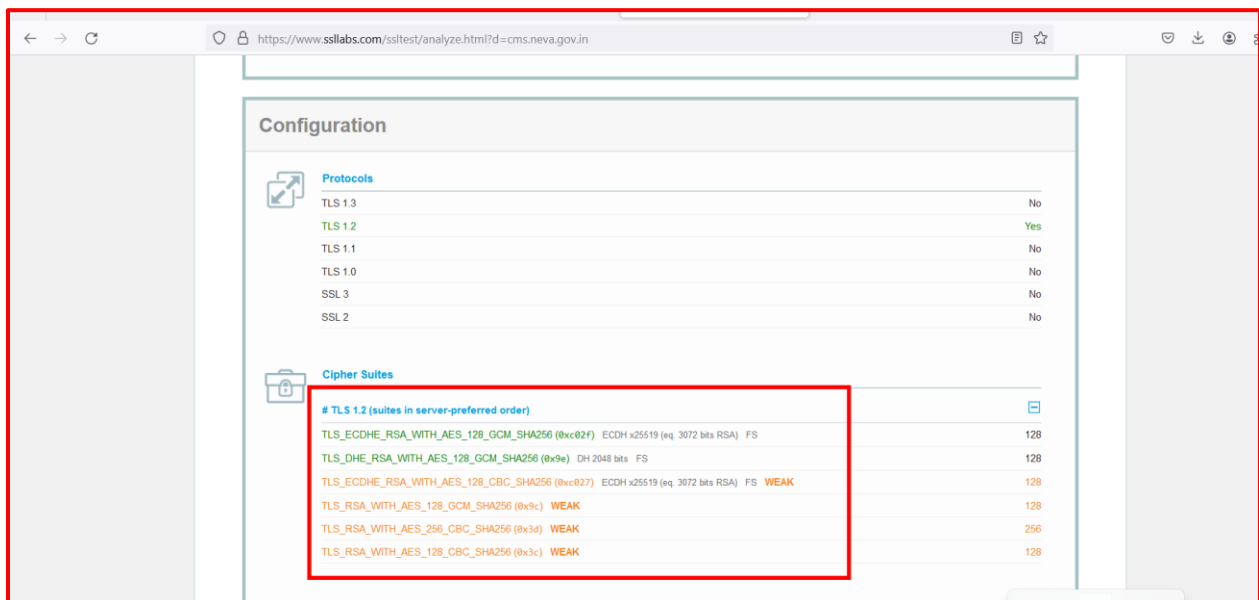
Medium

Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



7. Weak Ciphers Enabled

Vulnerability Title: Weak Ciphers Enabled	
Risk	Medium
Abstract	It was observed that that weak ciphers are enabled during secure communication (SSL).
Impact	Attackers might decrypt SSL traffic between your server and your visitors.
Recommendations	It is recommended to modify the SSL Cipher Suite directive in the httpd. conf. SSL Cipher Suite HIGH:MEDIUM:!MD5:!RC4
Snapshot	Attached Below
Affected Site	Throughout the application
Status	Not Compiled



Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



8. HTTP Security Headers not implemented

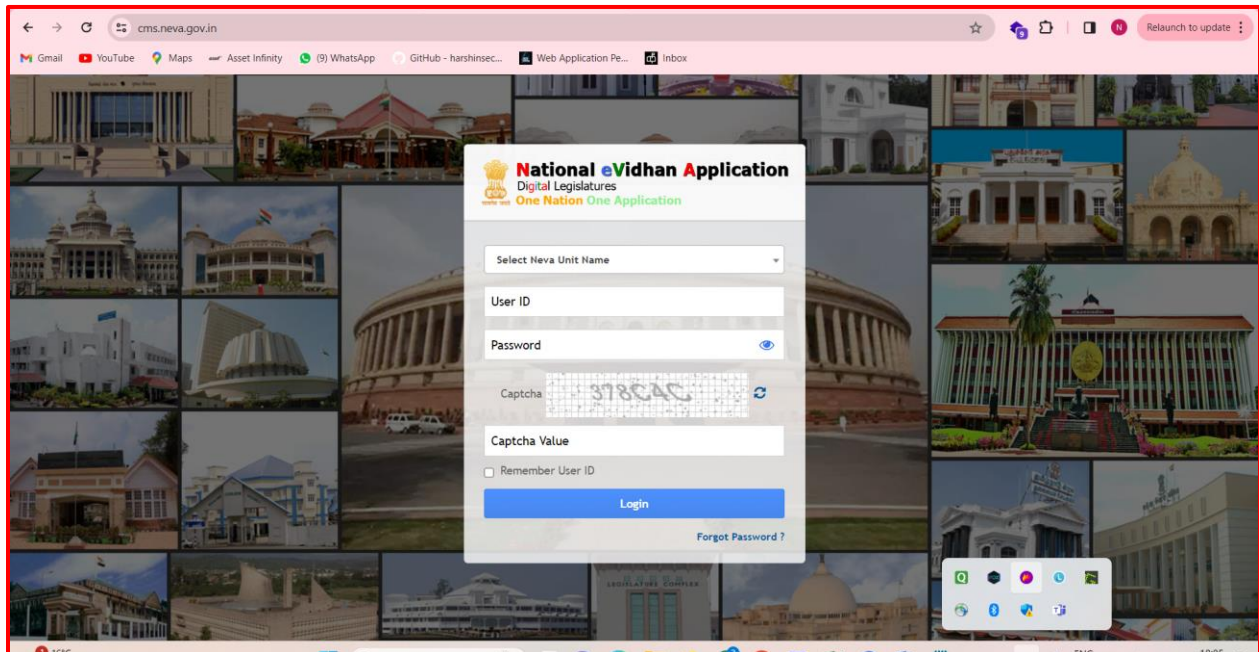
Vulnerability Title: HTTP Security Headers Not Implemented	
Risk	Medium
Abstract	It was observed that security headers such as X-XSS protection, Content Security Policy, Strict Transport security policy, X-Content-Type-Options were not implemented in remote application.
Ease of Exploitation	Medium
Impact	If security headers are not implemented in application then it may help an attacker to exploit existing vulnerabilities in application logic and results in lack of defense in depth approach to prevent security attacks.
Recommendations	It is recommended to implement security headers to provide additional layer of security in application such as X-XSS protection, Content Security Policy, Strict Transport security policy, X-Content-Type-Options
Snapshot	
Affected Site	Throughout the application
Status	Complied

Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



9. Session Timeout Is Not Implemented

Vulnerability Title: Session Timeout not implemented	
Risk	Medium
Abstract	It was observed that even if the Browser is logged in and idle it does not logout the session automatically.
Ease of Exploitation	Easy
Impact	It is possible to access authenticated pages.
Recommendations	Application should terminate a session if there is no activity from the user-side for a fixed period of time, e.g., 15 minutes.
Snapshot	Attached Below
Affected Site	Throughout the application
Status	Complied



Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



10. Out-of-Date version of data tables is used in the application

1) Vulnerability Title: Older version of data tables is used in the application	
Risk	Medium
Abstract	It was observed that application is using an older version of older version of data tables i.e., 1.9.4
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/stable version.
Snapshot	Given below
Affected Site	Throughout the application

The screenshot shows a web application interface with a table of queries and a Wappalizer security scan results panel. The table contains the following data:

#	Diary Number	Subject	Sent Date	Status	Action
1	17/2023/8	Demo	14/06/2023 11:29 AM	Under Consideration	Online
2	17/2023/7	test	02/06/2023 10:39 AM	Accepted on 02/06/2023	Online
3	17/2023/6	test	30/05/2023 12:02 PM	Accepted on 02/06/2023	Online
4	17/2023/5	test	29/05/2023 03:04 PM	Accepted on 29/05/2023	Online
5	17/2023/4	test	29/05/2023 01:02 PM	Under Consideration	Online
6	17/2023/3	TESTING	29/05/2023 12:54 PM	Accepted on 29/05/2023	Online
7	17/2023/1	test	18/05/2023 11:20 AM	Rejected on 18/05/2023	Online

The Wappalizer scan results show the following technologies and libraries:

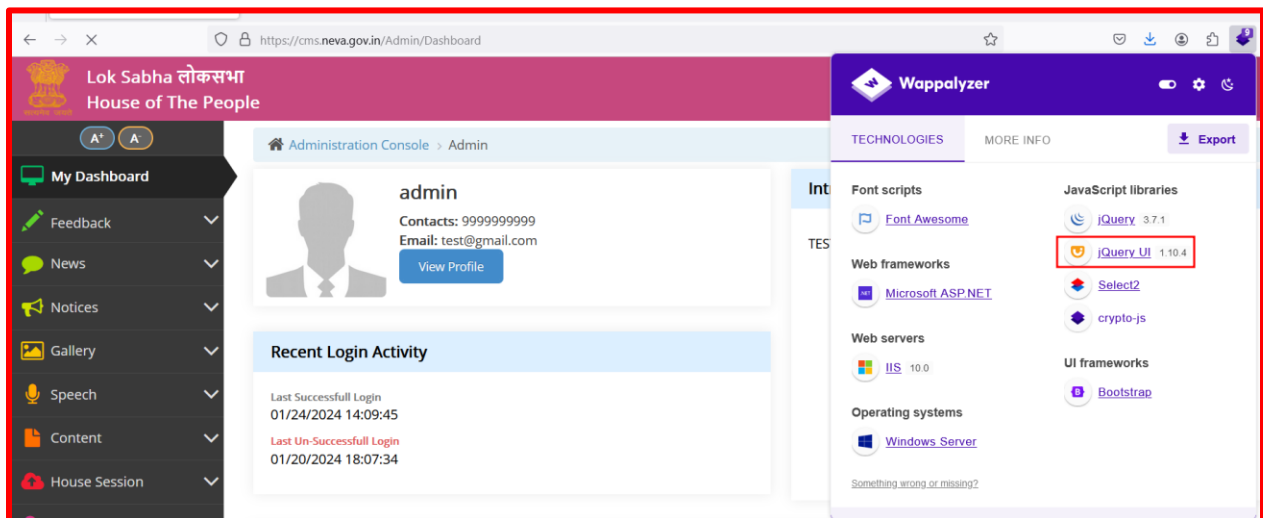
- Security: HSTS
- Font scripts: Font Awesome
- Web frameworks: Microsoft ASP.NET
- CDN: Google Hosted Libraries
- JavaScript libraries: JQuery 3.7.1, JQuery UI 1.10.4, Select2, crypte-is
- UI frameworks: Bootstrap
- DataTables 1.9.4** (highlighted in red)

Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



11. Out-of-Date version of jQuery UI is used in the application

2) Vulnerability Title: Older version of jQuery UI is used in the application	
Risk	Medium
Abstract	It was observed that application is using an older version of older version of jQuery UI i.e., 1.10.4
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/stable version.
Snapshot	Given below
Affected Site	Throughout the application



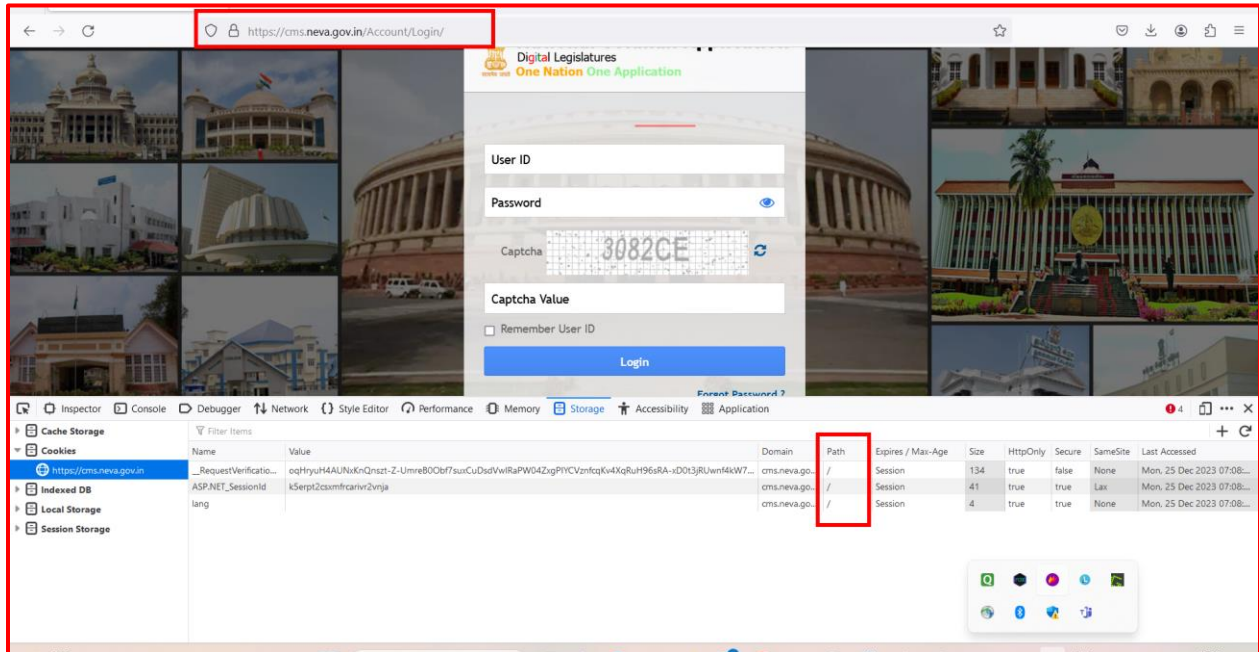
Low

Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



12. Path Not Set in Cookie Attribute

Vulnerability Title: Path Not Set in Cookie Attribute	
Risk	Low
Abstract	Path is not defined.
Ease of Exploitation	Medium
Impact	This may redirect to another application.
Recommendations	It is recommended to define path.
Snapshot	Attached Below
Affected Site	Throughout the application
Status	Compiled



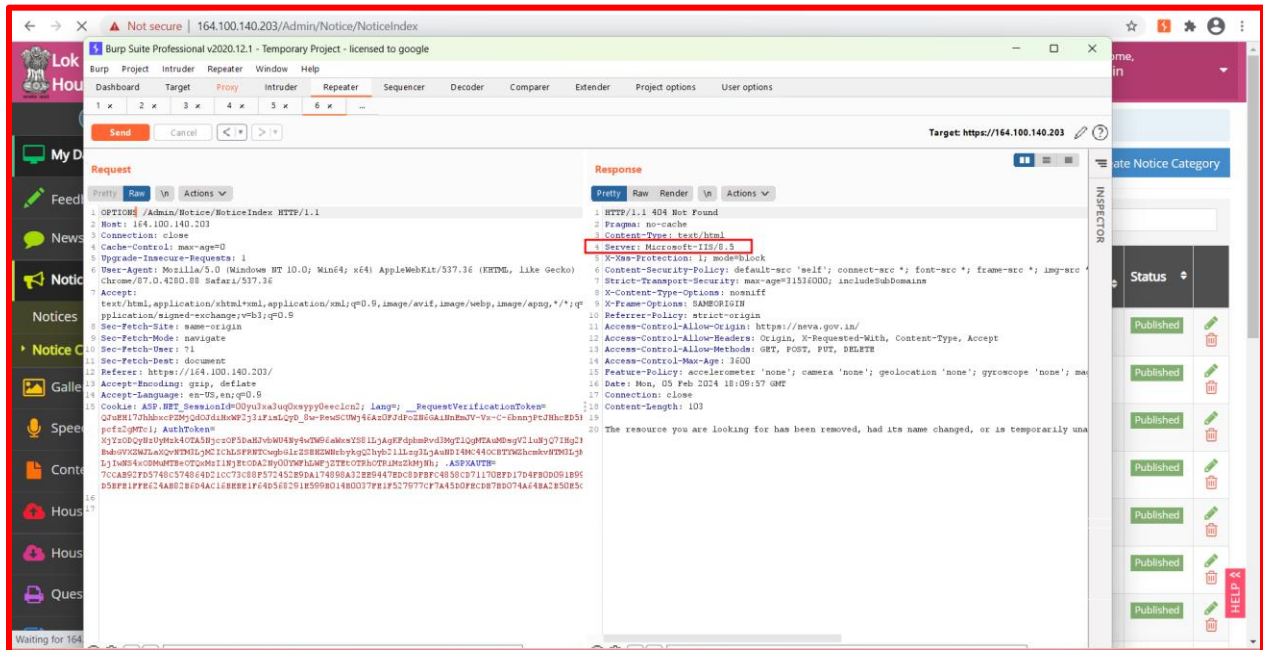
Note:-Point no 8 is needed to be put in the exception case while making cookies attribute path it was creating issues in login.

Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



13. Web Server Information Disclosure

Vulnerability Title: Web Server Information Disclosure	
Risk	Low
Abstract	Banner grabbing (application is displaying Server name and 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 name and version which may help attacker to learn more about his target.
Recommendations	Server version should not be displayed to the end user.
Snapshot	Attached below
Affected Site	Throughout the application
Status	Not Complied

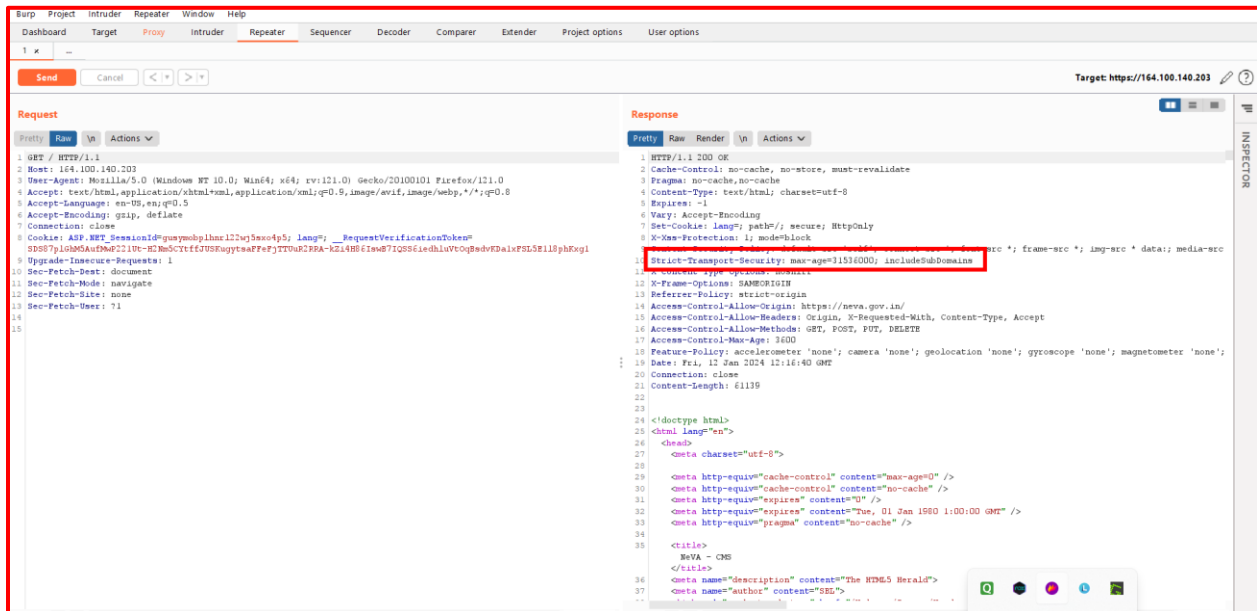


Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



14. HSTS (HTTP Strict Transport Security) Misconfiguration

Vulnerability Title: HSTS (HTTP Strict Transport Security) header is misconfigured.	
Risk	Low
Abstract	HSTS (HTTP Strict Transport Security) security header is misconfigured.
Ease of Exploitation	Easy
Impact	If HSTS is not configured correctly, it may not be effective in enforcing a secure, encrypted connection. This could leave the website vulnerable to man-in-the-middle attacks, where an attacker could intercept and manipulate the communication between the user's browser and the server.
Recommendations	Ensure that the HSTS header is correctly configured in the server's response headers. The key directive is Strict-Transport-Security. Specify the max-age directive to indicate the duration for which the HSTS policy should be enforced.
Snapshot	Attached Below
Affected Site	Throughout application
Status	Complied



Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



15. Cross-Origin resource sharing Misconfiguration

Vulnerability Title: Cross-Origin resource sharing misconfiguration	
Risk	Low
Abstract	It was observed that the CORS (Cross Origin Resource Sharing_Misconfiguration) Lead to sensitive information.
Ease of Exploitation	Hard
Impact	If CORS is not properly configured, a web page from one domain may be able to make requests to a different domain, leading to potential unauthorized access to sensitive data.
Recommendations	Configure CORS Headers Properly: Set the appropriate CORS headers in your web server or application to define which domains are allowed to access your resources. Common headers include Access-Control-Allow-Origin, Access-Control-Allow-Methods, and Access-Control-Allow-Headers.
Snapshot	Attached Below
Affected URLs	Throughout the application
Status	Complied

```

Request
1 GET /Account/Login/ HTTP/1.1
2 Host: cms.neva.gov.in
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/120.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: __RequestVerificationToken=DxP3DOv-gIAJ2Folk7v5y8CMkAmh3-vv-w7N10q4dFh9eSHY908-g_JHa5jgHuham00K7ob5h58Kno8vjk871Cp8K0e0#35n0eI; ASP.NET_SessionId=mkx2y8t4mcrlzljf8q6w; Lang=
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: none
13 Sec-Fetch-User: ?1
14
15

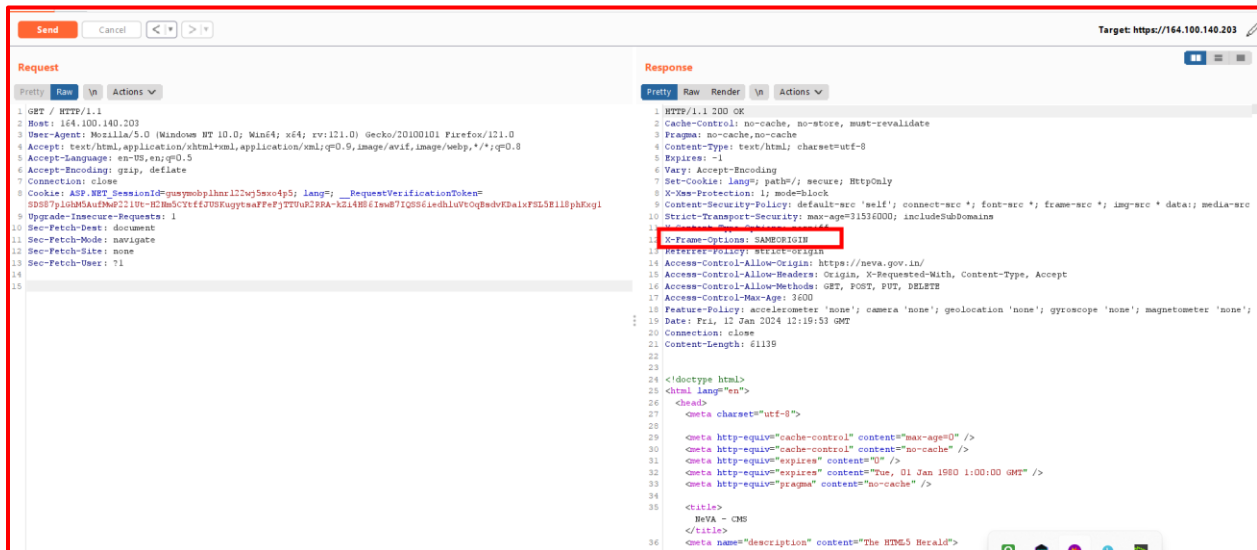
Response
1 HTTP/1.1 200 OK
2 Cache-Control: no-cache, no-store, must-revalidate
3 Pragma: no-cache
4 Content-Type: text/html; charset=utf-8
5 Expires: -1
6 X-Frame-Options: DENY
7 Set-Cookie: ASPXAUTH=; expires=Mon, 11-Oct-1999 18:10:00 GMT; path=/; HttpOnly; SameSite=Lax
8 Set-Cookie: __RequestVerificationToken=3jyew8Rgc5ndc1r9yudfba0k_cax-y8sgAGCYE8HRuq8f68f68LQ4MxM0401eqlqf; expires=Tue, 21-Feb-2023 11:22:59 GMT; path=/
9 Set-Cookie: ASP.NET_SessionId=; expires=Tue, 21-Feb-2023 11:22:59 GMT; path=/
10 Set-Cookie: Lang=; expires=Tue, 21-Feb-2023 11:22:59 GMT; path=/
11 Set-Cookie: lang=; expires=Tue, 21-Feb-2023 11:22:59 GMT; path=/
12 X-Powered-By: ASP.NET
13 Date: Thu, 21 Dec 2023 11:22:59 GMT
14 Connection: close
15 Content-Length: 60387
16
17
18
19 <!doctype html>
20 <html lang="en">
21 <head>
22 <meta charset="utf-8">
23
24 <meta http-equiv="cache-control" content="max-age=0" />
25 <meta http-equiv="cache-control" content="no-cache" />
26 <meta http-equiv="expires" content="0" />
27 <meta http-equiv="expires" content="Tue, 01 Jan 1980 1:00:00 GMT" />
28 <meta http-equiv="pragma" content="no-cache" />
29
30 <title>
31 NeVA - CMS
32 </title>
33 <meta name="description" content="The HDG5 Herald">
34 <meta name="author" content="JBL">
  
```

Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



16. X-Frame Options Misconfiguration

Vulnerability Title: X-Frame Option Header	
Risk	Low
Abstract	The X-Frame-Options header is used to control whether a browser should be allowed to render a page in a frame or iframe. When this header is set multiple times, it can cause conflicts and potential security issues.
Ease of Exploitation	Easy
Impact	The impact of setting X-Frame-Options multiple times can vary, but one possible consequence is that it may lead to inconsistent or unexpected behavior in different browsers. In some cases, it might result in the header being ignored altogether, potentially allowing the page to be embedded in frames when it shouldn't be.
Recommendations	Ensure that the X-Frame-Options header is set only once in the HTTP response. If it's set in multiple locations or at different stages of processing, conflicts may arise.
Snapshot	Attached Below
Affected Site	Throughout the application
Status	Complied



Web Application Security Test
 Report for National eVidhan Application
 (NeVA - CMS)



17. Audit Trail is not maintained

Vulnerability Title: Audit Trail is not implemented in properly	
Risk	Low
Abstract	The application does not maintain the logout action and status of user activity where all user activities have to be logged.
Ease of Exploitation	Easy
Impact	In-case a malicious user tries to attack the application; the application will not be able to trace the attacker
Recommendations	<p>An Audit trail should be incorporated in the application admin module, where all user activities have to be logged. Following points should be considered:</p> <ul style="list-style-type: none"> • Audits are to be generated at the time of resource access and by the same routines accessing the resource • Information to be logged including the following: IP of the originating client, Date, Time, username if any in addition to other details to be logged in the web server. • These IP, date, time, session details, user details (NO password), referrer, process id to be logged in application logs. • To create audit • logs, use auto numbering so that every logged entry has a log number, which is not editable. Then if one audit entry is deleted a gap in the numbering sequence will appear. • Log entries are to be hashed/ signed so that changes to audit log can be detected. • Audit trails to answer the following • Logging of Authentication Process. Success and failed attempts. • Logging Authentication details and changes. • Software error and failures logged. • Should not be possible to retrieve confidential authentication information from these logs (including passwords) • Is it possible to uniquely identify both client host and user from these logs? • What level of information is logged by the application (read/write access, modification data, and copy/paste data) Are log files time sequential and can they positively identify the time of action?
Snapshot	Attached given
Affected URLs	https://164.100.140.203/SuperAdmin/SuperAdmin
Status	Complied

Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



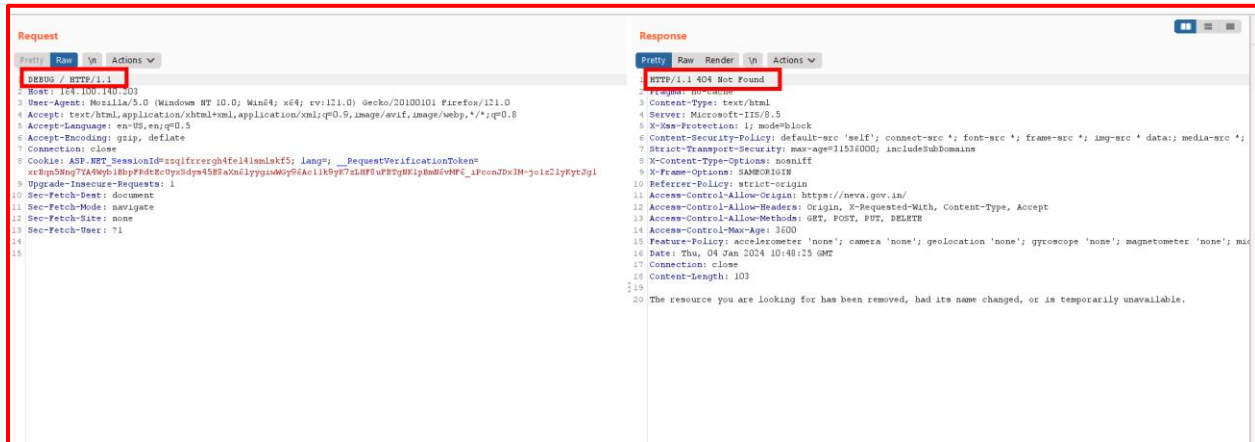
LogID	UserName	IPAddress	LoginDate/Time	LoginStatus	LogoutDate/Time	Module/Name	ActionName	ActionType	URL	ActionDate	FirstWrongAttemptTime	Block/Unit	UserId
969	1061	Kamal Dutt Verma	10.21.211.174	2019-06-28 17:24:49.410	Successful	1753-01-01 00:00:00.000	ListOfBusin... CreateLOB	GET	/ListOFBusiness/ListOFBusiness/CreateLOB	2019-06-28 17:24:49.583	NULL	NULL	NULL
970	1062	Kamal Dutt Verma	10.21.211.174	2019-06-28 17:24:49.410	Successful	1753-01-01 00:00:00.000	ListOFBusin... CreateLOB	GET	/ListOFBusiness/ListOFBusiness/CreateLOB	2019-06-28 17:24:53.220	NULL	NULL	NULL
971	1063	Kamal Dutt Verma	10.21.211.174	2019-06-28 17:24:49.410	Successful	2019-06-28 17:25:00.300	Account LogOff	POST	/Account/LogOff	2019-06-28 17:25:00.300	NULL	NULL	NULL
972	1064	admin	10.21.211.200	2019-07-01 10:50:07.643	Successful	1753-01-01 00:00:00.000	Dashboard Index	GET	/Admin/Dashboard	2019-07-01 10:50:09.457	NULL	NULL	NULL
973	1065	Kamal Dutt Verma	10.21.211.174	2019-07-01 11:00:38.057	Successful	1753-01-01 00:00:00.000	ListOFBusin... CreateLOB	GET	/ListOFBusiness/ListOFBusiness/CreateLOB	2019-07-01 11:00:38.230	NULL	NULL	NULL
974	1066	Kamal Dutt Verma	10.21.211.174	2019-07-01 11:00:38.057	Successful	2019-07-01 11:01:39.637	Account LogOff	POST	/Account/LogOff	2019-07-01 11:01:39.637	NULL	NULL	NULL
975	1067	admin	10.21.211.200	2019-07-01 11:27:34.503	Successful	1753-01-01 00:00:00.000	Dashboard Index	GET	/Admin/Dashboard	2019-07-01 11:27:34.590	NULL	NULL	NULL
976	1068	admin	10.21.211.224	2019-07-01 14:05:37.640	Unsuccessful	1753-01-01 00:00:00.000	User WrongAttemptAdminLoginData	Get	/Account/Login	2019-07-01 14:05:37.720	NULL	NULL	NULL
977	1069	admin	10.21.211.200	2019-07-02 10:07:31.667	Unsuccessful	1753-01-01 00:00:00.000	User WrongAttemptAdminLoginData	Get	/Account/Login	2019-07-02 10:07:33.260	NULL	NULL	NULL
978	1070	admin	10.21.211.200	2019-07-02 10:07:50.463	Successful	1753-01-01 00:00:00.000	Dashboard Index	GET	/Admin/Dashboard	2019-07-02 10:07:50.637	NULL	NULL	NULL
979	1071	admin	10.21.211.200	2019-07-02 10:07:50.463	Successful	2019-07-02 10:23:51.047	Account LogOff	POST	/Account/LogOff	2019-07-02 10:23:51.047	NULL	NULL	NULL
980	1072	admin	10.21.211.200	2019-07-02 10:35:35.350	Successful	1753-01-01 00:00:00.000	Dashboard Index	GET	/Admin/Dashboard	2019-07-02 10:35:36.157	NULL	NULL	NULL
981	1073	Jitender Singh Kanwar	10.21.211.200	2019-07-02 14:18:35.350	Successful	1753-01-01 00:00:00.000	Legislation... PaperLaidSummary	GET	/Notices/LegislationFixation/PaperLaidSummary	2019-07-02 14:18:35.553	NULL	NULL	NULL
982	1074	Jitender Singh Kanwar	10.21.211.200	2019-07-02 14:18:35.350	Successful	2019-07-02 14:41:53.337	Account LogOff	POST	/Account/LogOff	2019-07-02 14:41:53.337	NULL	NULL	NULL
983	1075	Jitender Singh Kanwar	10.21.211.200	2019-07-02 14:50:17.657	Successful	1753-01-01 00:00:00.000	Legislation... PaperLaidSummary	GET	/Notices/LegislationFixation/PaperLaidSummary	2019-07-02 14:50:17.830	NULL	NULL	NULL
984	1076	Jitender Singh Kanwar	10.21.211.200	2019-07-02 14:50:17.657	Successful	1753-01-01 00:00:00.000	Legislation... PaperLaidSummary	GET	/Notices/LegislationFixation/PaperLaidSummary	2019-07-02 15:23:22.953	NULL	NULL	NULL
985	1077	admin	10.21.211.174	2019-07-02 15:29:19.560	Successful	1753-01-01 00:00:00.000	Dashboard Index	GET	/Admin/Dashboard	2019-07-02 15:29:19.730	NULL	NULL	NULL
986	1078	admin	10.21.211.174	2019-07-02 15:29:19.560	Successful	2019-07-02 15:29:28.000	Account LogOff	POST	/Account/LogOff	2019-07-02 15:29:28.000	NULL	NULL	NULL
987	1079	Sanjeev Kumar	10.21.211.174	2019-07-02 15:30:03.023	Successful	1753-01-01 00:00:00.000	Danies DanesDashboard	GET	/Notices/Danies/DanesDashboard	2019-07-02 15:30:03.163	NULL	NULL	NULL
988	1080	Sanjeev Kumar	10.21.211.174	2019-07-02 15:30:03.023	Successful	1753-01-01 00:00:00.000	Danies SavePaperEntry	POST	/Notices/Danies/SavePaperEntry	2019-07-02 15:30:29.477	NULL	NULL	NULL
989	1081	Sanjeev Kumar	10.21.211.174	2019-07-02 15:30:03.023	Successful	1753-01-01 00:00:00.000	Danies DanesDashboard	GET	/Notices/Danies/DanesDashboard	2019-07-02 15:30:29.557	NULL	NULL	NULL
990	1082	Sanjeev Kumar	10.21.211.174	2019-07-02 15:30:03.023	Successful	1753-01-01 00:00:00.000	Danies SaveFile	POST	/Notices/Danies/SaveFile	2019-07-02 15:31:46.507	NULL	NULL	NULL
991	1083	Sanjeev Kumar	10.21.211.174	2019-07-02 15:30:03.023	Successful	2019-07-02 15:31:54.963	Account LogOff	POST	/Account/LogOff	2019-07-02 15:31:54.963	NULL	NULL	NULL
992	1084	Jitender Singh Kanwar	10.21.211.174	2019-07-02 15:33:02.540	Successful	1753-01-01 00:00:00.000	Legislation... PaperLaidSummary	GET	/Notices/LegislationFixation/PaperLaidSummary	2019-07-02 15:33:02.663	NULL	NULL	NULL
993	1085	Jitender Singh Kanwar	10.21.211.174	2019-07-02 15:33:02.540	Successful	2019-07-02 15:34:49.657	Account LogOff	POST	/Account/LogOff	2019-07-02 15:34:49.657	NULL	NULL	NULL
994	1086	Puran Chand Thakur	10.21.211.174	2019-07-02 15:35:12.327	Successful	1753-01-01 00:00:00.000	NoticeDetails Index	GET	/Notices/NoticeDetails/Index	2019-07-02 15:35:12.470	NULL	NULL	NULL
995	1087	Puran Chand Thakur	10.21.211.174	2019-07-02 15:35:12.327	Successful	2019-07-02 15:36:51.800	Account LogOff	POST	/Account/LogOff	2019-07-02 15:36:51.800	NULL	NULL	NULL
996	1088	Sanjeev Kumar	10.21.211.174	2019-07-02 15:37:11.390	Successful	1753-01-01 00:00:00.000	Danies DanesDashboard	GET	/Notices/Danies/DanesDashboard	2019-07-02 15:37:11.560	NULL	NULL	NULL
997	1089	Sanjeev Kumar	10.21.211.174	2019-07-02 15:39:08.497	Successful	2019-07-02 15:39:08.497	Account LogOff	POST	/Account/LogOff	2019-07-02 15:39:08.497	NULL	NULL	NULL
998	1090	admin	10.21.211.200	2019-07-03 10:22:02.313	Successful	1753-01-01 00:00:00.000	Dashboard Index	GET	/Admin/Dashboard	2019-07-03 10:22:04.077	NULL	NULL	NULL
999	1091	admin	10.21.211.200	2019-07-03 10:22:02.313	Successful	1753-01-01 00:00:00.000	Account LoginUP	GET	/	2019-07-03 10:53:05.517	NULL	NULL	NULL
1...	1092	admin	10.21.211.200	2019-07-03 10:53:25.543	Successful	1753-01-01 00:00:00.000	Dashboard Index	GET	/Admin/Dashboard	2019-07-03 10:53:25.730	NULL	NULL	NULL

Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



18. Forbidden Resource

Vulnerability Title: Forbidden Resource	
Risk	Low
Abstract	A forbidden resource, in the context of web security, typically refers to a resource or action that a user is not authorized to access or perform. It's often associated with HTTP status code 403, which means "Forbidden".
Ease of Exploitation	Medium
Impact	Attacker can gain unauthorized access to resources or functionality that should be off-limits to them. The impact of forbidden resource vulnerabilities can be significant, potentially leading to unauthorized data access, privilege escalation, and other security breaches.
Recommendations	Implement appropriate error handling to ensure that error messages do not leak sensitive information about the system's structure or access controls.
Snapshot	Attached Below
Affected URL	Throughout the Application
Status	Complied




Web Application Security Test
 Report for National eVidhan Application
 (NeVA - CMS)




19. Insecure Transportation Security Protocol Supported (TLS 1.0)

Vulnerability Title: Insecure Transportation Security Protocol Supported (TLS 1.0)	
Risk	Low
Abstract	It was observed that this application is using an outdated and insecure version of the TLS protocol
Impact	TLS 1.0 uses weak encryption algorithms compared to the newer versions, making it susceptible to attacks such as brute force and cryptographic attacks. TLS 1.0 has known security vulnerabilities, including BEAST (Browser Exploit Against SSL/TLS) and POODLE (Padding Oracle On Downgraded Legacy Encryption), which can be exploited to intercept or manipulate encrypted data.
Recommendations	Upgrade your systems to use TLS 1.2 or preferably TLS 1.3, which offer better security and performance. TLS 1.3 includes improvements such as stronger cipher suites, enhanced handshakemechanisms, and improved resilience against attacks.
Snapshot	Attached Below
Affected Site	Throughout the application
Status	Complied



Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No



Cipher Suites

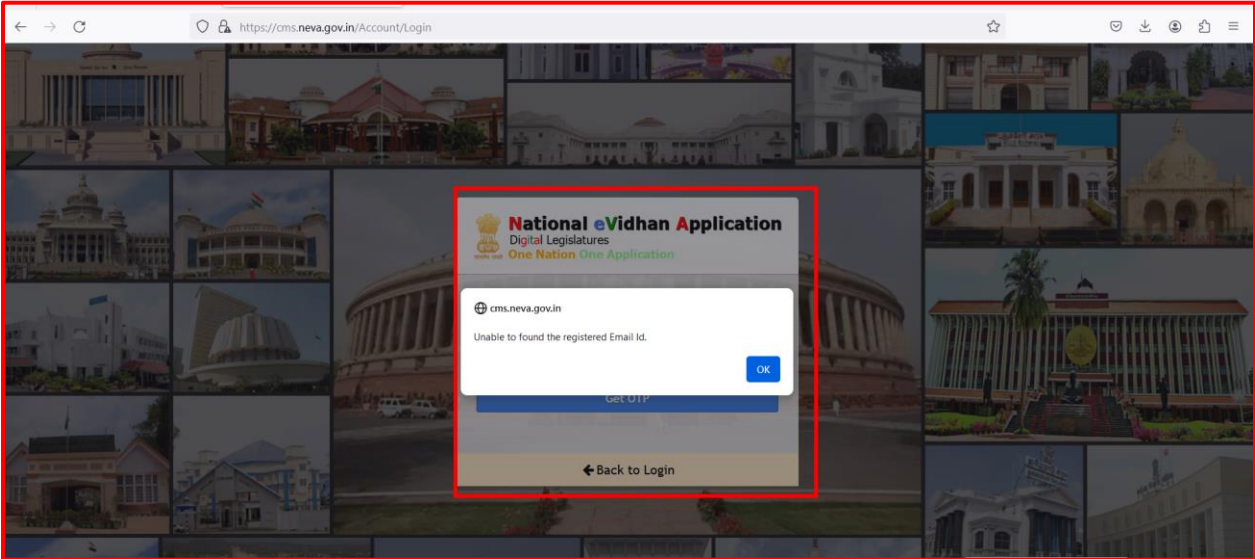
Web Application Security Test
 Report for National eVidhan Application
 (NeVA - CMS)



20. User Enumeration

Vulnerability Title: User Enumeration is possible in application	
Risk	Low
Abstract	User enumeration is a security vulnerability that occurs when an attacker can determine whether a specific username or email address is valid or not within a system, application, or service.
Ease of Exploitation	Easy
Impact	Having a list of valid usernames makes it easier for attackers to launch brute-force attacks. They can focus their efforts on trying to crack the passwords for these known accounts, potentially gaining unauthorized access.
Recommendations	<p>The application should display only one error message when the login credentials are invalid. An attacker can gain knowledge of valid usernames/ids if the application displays different error message for incorrect username and another error message when the username is correct but password is wrong. It is recommended to display a generic message for all the cases where either password or username or both are wrong like:</p> <ol style="list-style-type: none"> 1. User-ID or password is Invalid. Or 2. Please enter valid credentials. Or 3. Wrong Username or Password. <p>And it is recommended to display a generic message at forget password module for all cases whether user exists or not i.e., "If the email address is known to us, we'll send a password recovery link in a few minutes."</p>
Snapshot	Attached Below
Affected URLs	https://164.100.140.203
Status	Not Complied

Web Application Security Test
Report for National eVidhan Application
(NeVA - CMS)



Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



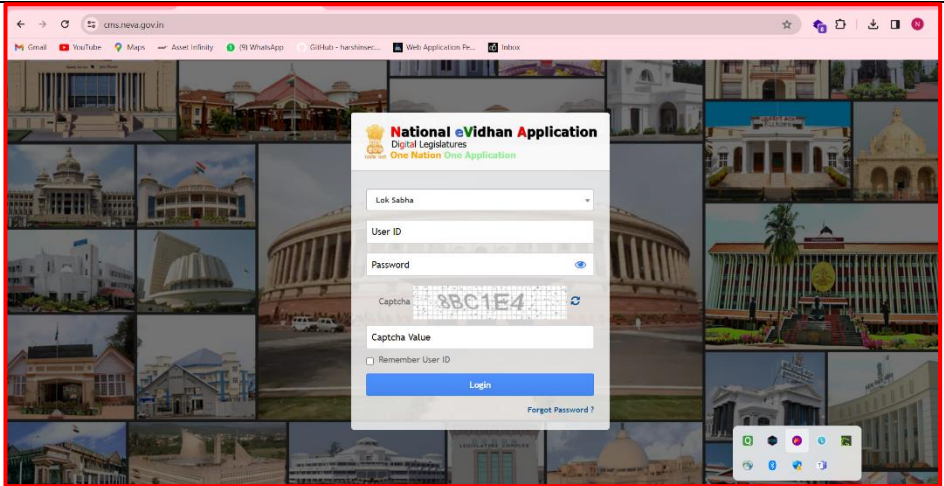
21. E-tag

Vulnerability Title: E-tag Information Disclosure	
Risk	Low
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	
Affected Site	https://164.100.140.203
Status	Complied

Web Application Security Test
 Report for National eVidhan Application
 (NeVA - CMS)



22. Improper Input Validation

Vulnerability Title : Input Validation	
Risk	Low
Abstract	It was observed that there was vital information leakage on website.
Ease of Exploitation	Easy
Impact	It is possible to gather sensitive debugging information.
Recommendations	It is recommended to implement proper validations on all input fields of the web application.
Snapshot	
Affected Site	throughout the application
Status	Complied

New Vulnerabilities

23. Password Replay attack is possible.

Vulnerability Title: Password replay attack is possible.	
Risk	High
Abstract	It was observed that Password replay attack is possible in the application.
Ease of Exploitation	Easy
Impact	A Malicious user can reuse the encrypted value of password .
Recommendations	<p>It is recommended that SHA-256 with Salted Hashing technique in authentication or login module should be implemented. The pre-requisite to this is that the backend database stores a SHA-256 or hash of the password. (SHA-256 hash is a cryptographic technique in which the actual value can never be recovered).</p> <p>Here is how the salted hash technique works: When a client requests for the login page, the server generates a random number, the salt, and sends it to the client along with the page. A JavaScript code on the client computes the (SHA-256) hash of the password entered by the user. It then concatenates the salt to the hash and re-computes the (SHA-256) hash. This result is then sent to the server. The server picks the hash of the password from its database, concatenates the salt and computes the (SHA-256) hash. If the user entered the correct password these two hashes should match. The server compares the two and if they match, the user is authenticated.</p> <p>Please note that every time a new salt value must be generated at the call of login page at the server end. As this „salt? is used it should be expired & deleted at the server end. If it is not used for login for more than a standard time (say 5 minutes), the „salt? value again should be expired & deleted. The SALT value should be properly implemented such that it meets the following conditions:</p> <ul style="list-style-type: none"> • SALT value should not be visible in the POST request. • SALT value should be alphanumeric and minimum of 16 characters. • SALT value should not be generated on the client side but always on the server side.

Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



<p>Snapshot</p>	
<p>Affected URLs</p>	<p>throughout the application</p>
<p>Status</p>	<p>New</p>

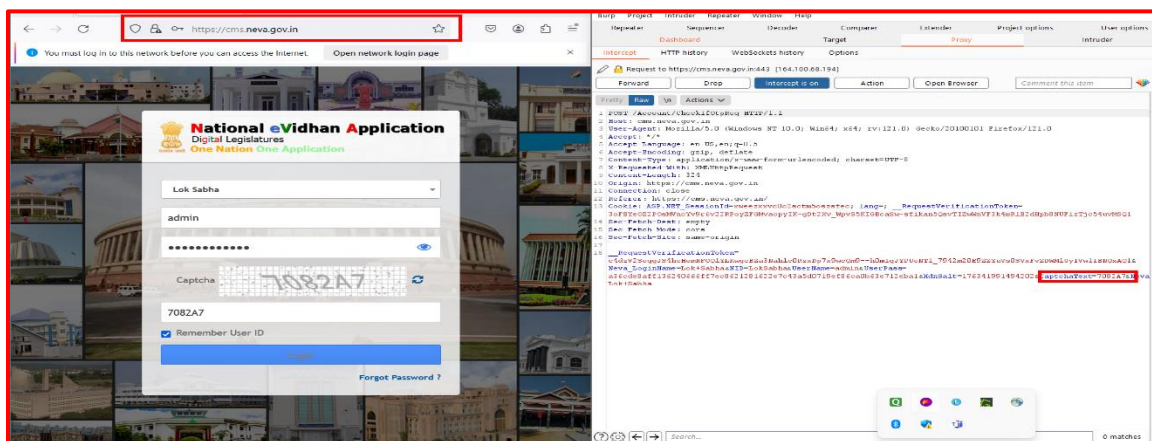
Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



24. CAPTCHA is not validating at server side

Vulnerability Title: CAPTCHA is not validated at server side	
Risk	Medium
Abstract	It was observed that the CAPTCHA is not validate at server side use in login page, as impact could be read by an automated tool.
Ease of Exploitation	Easy
Impact	It is Easily possible to Flood the attack.
Recommendations	CAPTCHA should follow the following condition: a) The combination of alphanumeric value. b) Combination of Upper case and lower-case letters. c) Case-Sensitive d) Its length should be minimum 6 characters. e) Should not be a third-party CAPTCHA: f) Should be Random and not follow a pattern. g) Example: Ab73jy, PT34h8, Hos3t3, nic23n etc.
Snapshot	Attached below
Affected URLs	throughout the application
Status	New

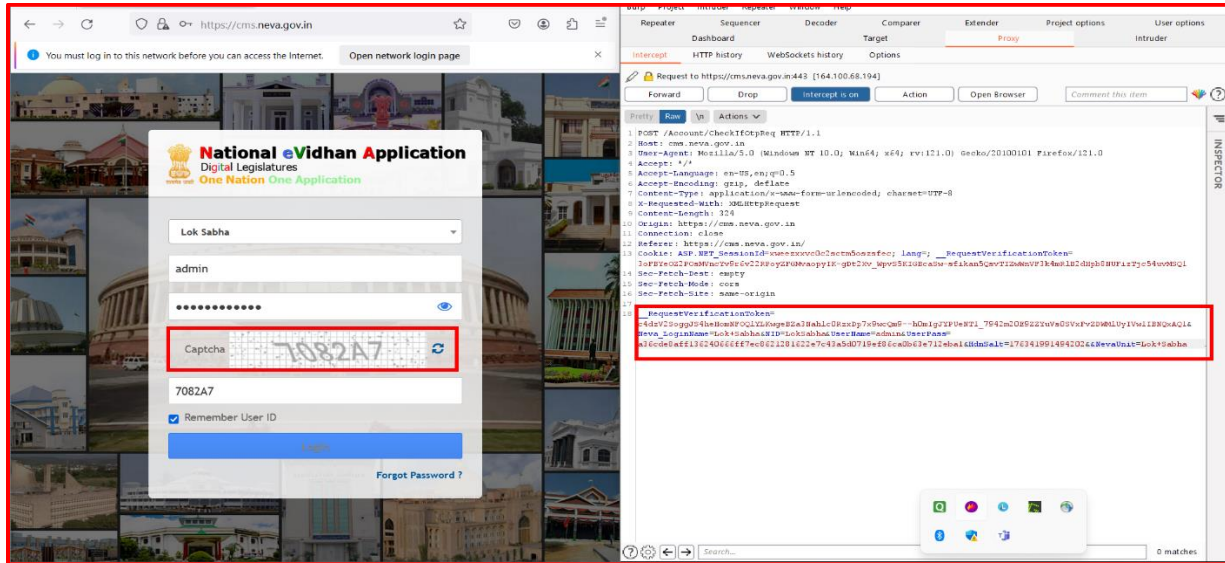
Step#1: Enter the valid CAPTCHA at login page and submit the request while submitting capture the request as shown below:



Web Application Security Test Report for National eVidhan Application (NeVA - CMS)



Step#2: Now delete the complete field of captcha in the burp and forward the request as shown below.



Step#3: As we can see that we are still login in the application .Therefore, CAPTCHA is not validating at server side:

