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

Test URL

https://164.100.140.203

Level-2

12th January 2024

AAA
Accurate. Reliable. Innovative.

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

<table>
<tr><th colspan="4">Document Version Control</th></tr>
<tr><td colspan="2"><b>Data Classification</b></td><td colspan="2">CLASSIFIED</td></tr>
<tr><td colspan="2"><b>Client Name</b></td><td colspan="2">NICSI</td></tr>
<tr><td colspan="2"><b>Document Title</b></td><td colspan="2">Web Application Security Test Report</td></tr>
<tr><td colspan="2"><b>Author</b></td><td colspan="2">Neha</td></tr>
<tr><td><b>Version</b></td><td><b>Date of Issue</b></td><td><b>Issued by</b></td><td><b>Change Description</b></td></tr>
<tr><td>1.0</td><td>22-12-2023</td><td>AAA Technologies Ltd.</td><td>Initial Issue</td></tr>
</table>

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Outdated version of jQuery 13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.Path Not Set in Cookie Attribute 21
11.Web Server Information Disclosure 22
12.HSTS (HTTP Strict Transport Security) Misconfiguration 23
13.Cross-Origin resource sharing Misconfiguration 24
14.X-Frame Options Misconfiguration 25
15.Audit Trail is not maintained 26
16.Forbidden Resource 28
17.Insecure Transportation Security Protocol Supported (TLS 1.0) 29
18.User Enumeration 30
19.E-tag 32
20. Improper Input Validation 33
21.Password Replay attack is possible. 35
22.CAPTCHA is not validating at server side 37

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

S. No.	Vulnerability Description	Level-1	Level-2
1.	Session Hijacking Attack		Complied
2.	Dangerous Http Method Enabled		Complied
3.	Outdated version of jQuery		Complied
4.	Vulnerable version of Bootstrap		Complied
5.	SSL Certificate Date Expired		Complied
6.	Weak Ciphers Enabled		Not Complied
7.	Session Timeout Is Not Implemented		Complied
8.	Path Not Set in Cookie Attribute		Exception
9.	Web Server Information Disclosure		Not complied
10.	HSTS (HTTP Strict Transport Security) Misconfiguration		Complied
11.	Cross-Origin resource sharing Misconfiguration		Complied
12.	X-Frame Options Misconfiguration		Complied
13.	Audit Trail is not maintained		Complied
14.	Forbidden Resource		Complied
15.	Insecure Transportation Security Protocol Supported (TLS 1.0)		Complied
16.	User Enumeration		Not Complied
17.	Multiple Browser Login		Complied
18.	E-Tag		Complied
19.	HTTP Security Header not implemented		Complied

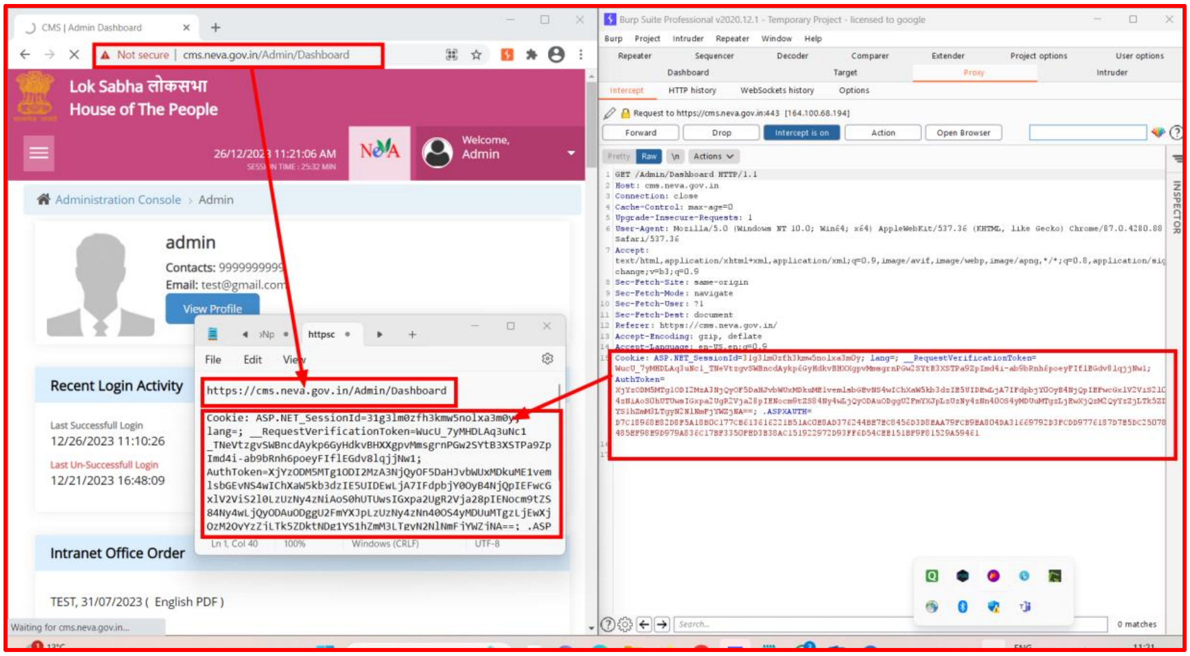
S. No.	Vulnerability Description	Level-1	Level-2
20.	Improper input validation		Complied
21.	CAPTCHA not validate in server side		New
22.	Password reply attack is possible		New

High

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

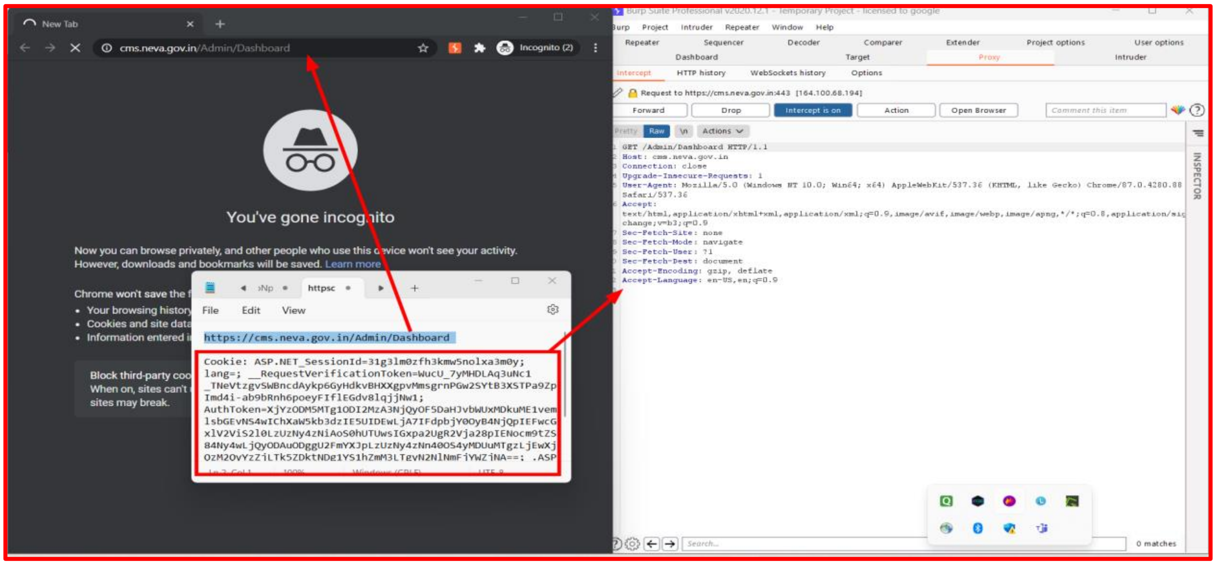
Step#1 -Login into application using valid credentials and now intercept the internal page in burp suite. Now, copy the authenticated cookie and internal URL in notepad as shown below.



```
https://cms.neva.gov.in/Admin/Dashboard

Cookie: ASP.NET_SessionId=31g3lm0zfh3kmw5nolxa3m0y;
lang=; __RequestVerificationToken=WucU_7yMHDLAq3uNc1
_TNeVtzgvSWBncdAykp6GyHdkvBHXXgpvMmsgrnPGw2SYtB3XSTPa9Zp
Imd4i-ab9bRnh6poeyFIflEGdv8lqjjNw1;
AuthToken=XjYzODM5MTg1ODI2MzA3NjQyOF5DaHJvbWUxMDkuME1vem
lsbGEvNS4wIChXaW5kb3dzIE5UIDEwLjA7IFdpbjY0OyB4NjQpIEFwcG
xlV2ViS2l0LzUzNy4zNiAoS0hUTUwsIGxpa2UgR2Vja28pIENocm9tZS
84Ny4wLjQyODAuODggU2FmYXJpLzUzNy4zNn40OS4yMDUuMTgzLjEwXj
OzM2OvYzZiLTk5ZDktNDg1YS1hZmM3LTgvN2NlNmFjYWZjNA==; .ASP
```

```
Request to https://cms.neva.gov.in:443  [164.100.68.194]

GET /Admin/Dashboard HTTP/1.1
Host: cms.neva.gov.in
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/sig
change;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://cms.neva.gov.in/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: ASP.NET_SessionId=31g3lm0zfh3kmw5nolxa3m0y; lang=; __RequestVerificationToken=
WucU_7yMHDLAq3uNc1_TNeVtzgvSWBncdAykp6GyHdkvBHXXgpvMmsgrnPGw2SYtB3XSTPa9ZpImd4i-ab9bRnh6poeyFIflEGdv8lqjjNw1;
AuthToken=
XjYzODM5MTg1ODI2MzA3NjQyOF5DaHJvbWUxMDkuME1vemlsbGEvNS4wIChXaW5kb3dzIE5UIDEwLjA7IFdpbjY0OyB4NjQpIEFwcGxlV2ViS2l0
4zNiAoS0hUTUwsIGxpa2UgR2Vja28pIENocm9tZS84Ny4wLjQyODAuODggU2FmYXJpLzUzNy4zNn40OS4yMDUuMTgzLjEwXjQzM2QyYzZjLTk5ZD
YS1hZmM3LTgyN2NlNmFjYWZjNA==; .ASPXAUTH=
D7C18968E82D8F5A18BDC177CB6136162218B51AC0E8AD376244BE7EC8456D3D8EAA79FCB9EA804DA3166979 2D3FCDD9776187D7B5DC25078
485EF98E9D979A836C17BF3350FED3B38AC151922972D93FF6D54CEE151BF9F81529A59461
```

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.



You've gone incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. Learn more

Chrome won't save the

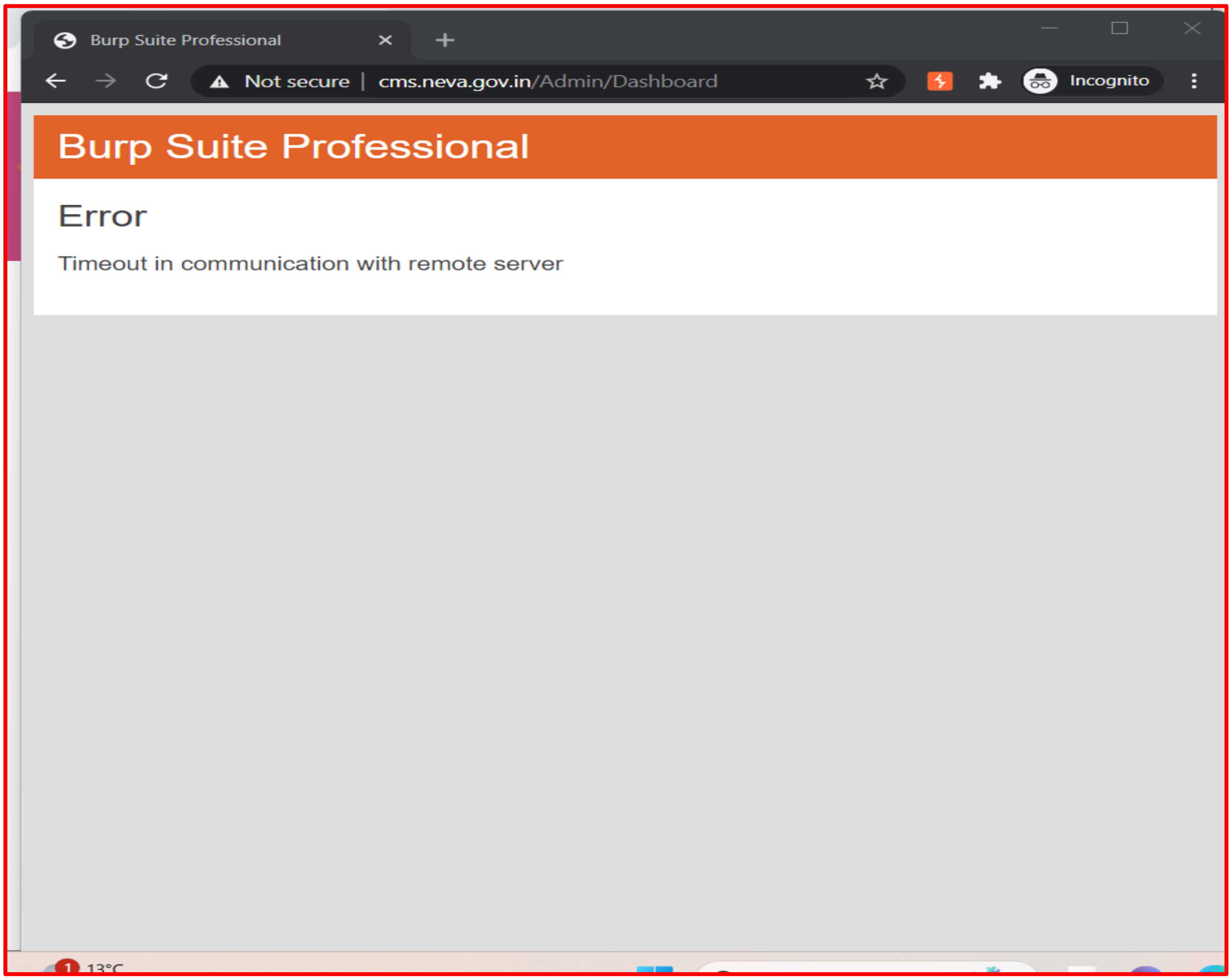
- Your browsing history
- Cookies and site data
- Information entered i

Block third-party coo
When on, sites can't
sites may break.

```
https://cms.neva.gov.in/Admin/Dashboard

Cookie: ASP.NET_SessionId=31g3lm0zfh3kmw5nolxa3m0y;
lang=; __RequestVerificationToken=WucU_7yMHDLAq3uNc1
_TNeVtzgvSWBncdAykp6GyHdkvBHXXgpvMmsgrnPGw2SYtB3XSTPa9Zp
Imd4i-ab9bRnh6poeyFIflEGdv8lqjjNw1;
AuthToken=XjYzODM5MTg1ODI2MzA3NjQyOF5DaHJvbWUxMDkuME1vem
lsbGEvNS4wIChXaW5kb3dzIE5UIDEwLjA7IFdpbjY0OyB4NjQpIEFwcG
xlV2ViS2l0LzUzNy4zNiAoS0hUTUwsIGxpa2UgR2Vja28pIENocm9tZS
84Ny4wLjQyODAuODggU2FmYXJpLzUzNy4zNn40OS4yMDUuMTgzLjEwXj
OzM2OvYzZiLTk5ZDktNDg1YS1hZmM3LTgvN2NlNmFjYWZjNA==; .ASP
```

```
Request to https://cms.neva.gov.in:443  [164.100.68.194]

GET /Admin/Dashboard HTTP/1.1
Host: cms.neva.gov.in
Connection: close
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/sig
change;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

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



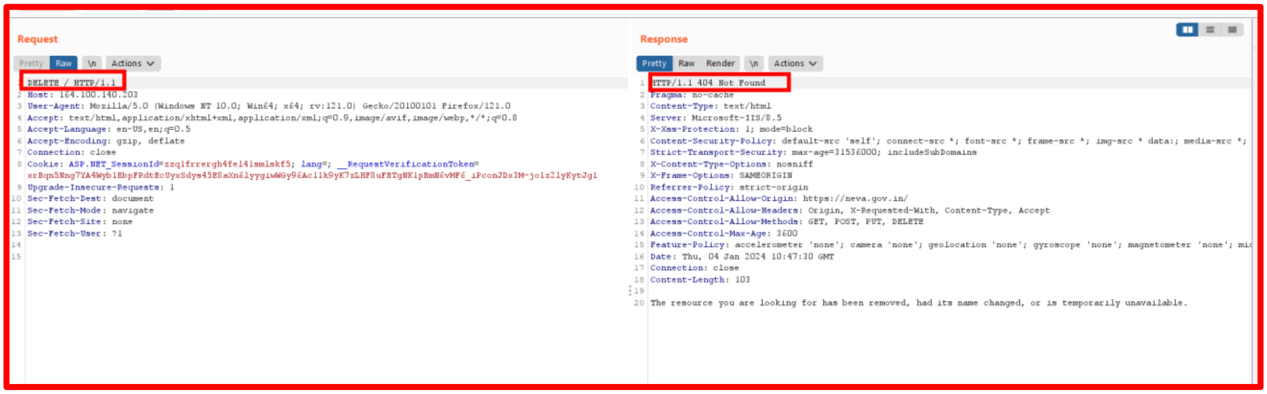
Burp Suite Professional

Error

Timeout in communication with remote server

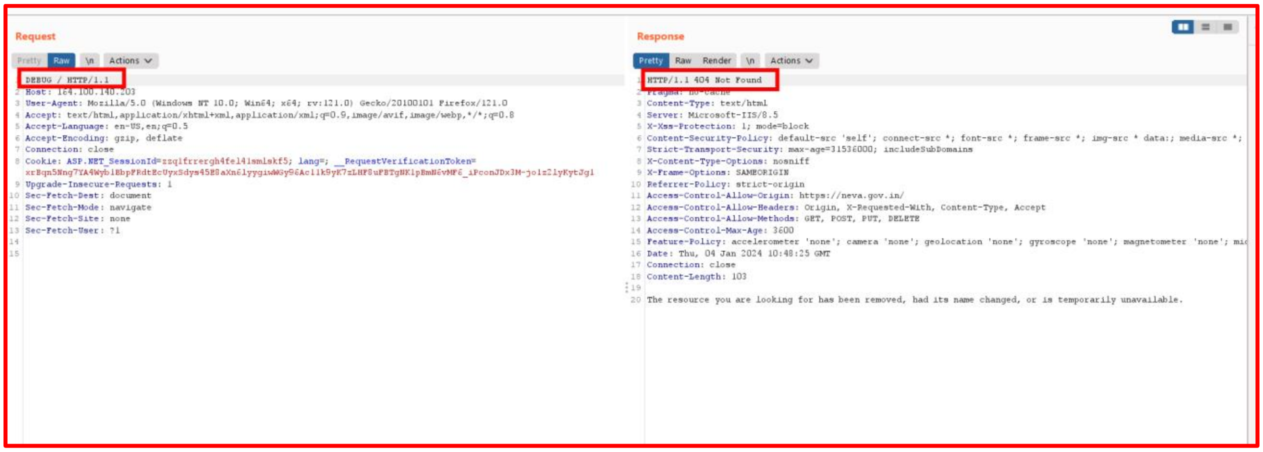
2. Dangerous Http Method Enabled

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	Complied



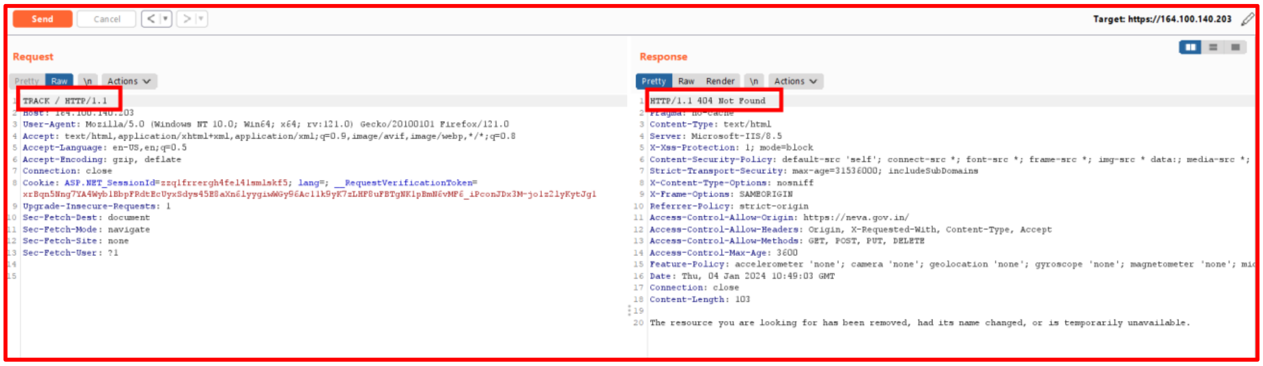
```
DELETE / HTTP/1.1
Host: 164.100.140.203
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ASP.NET_SessionId=zzqlfrrergh4fel4lsmlskf5; lang=; __RequestVerificationToken=
xrBqn5Nng7YA4Wyb1BbpFRdtEcUyxSdys45E8aXn6lyygiwWGy96Ac11k9yK7zLHF8uFBTgNK1pBmN6vMF6_iPconJDx3M-jolz2lyKytJgl
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

```
HTTP/1.1 404 Not Found
Pragma: no-cache
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Xss-Protection: 1; mode=block
Content-Security-Policy: default-src 'self'; connect-src *; font-src *; frame-src *; img-src * data:; media-src *;
Strict-Transport-Security: max-age=31536000; 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: 3600
Feature-Policy: accelerometer 'none'; camera 'none'; geolocation 'none'; gyroscope 'none'; magnetometer 'none'; mic
Date: Thu, 04 Jan 2024 10:47:30 GMT
Connection: close
Content-Length: 103

The resource you are looking for has been removed, had its name changed, or is temporarily unavailable.
```



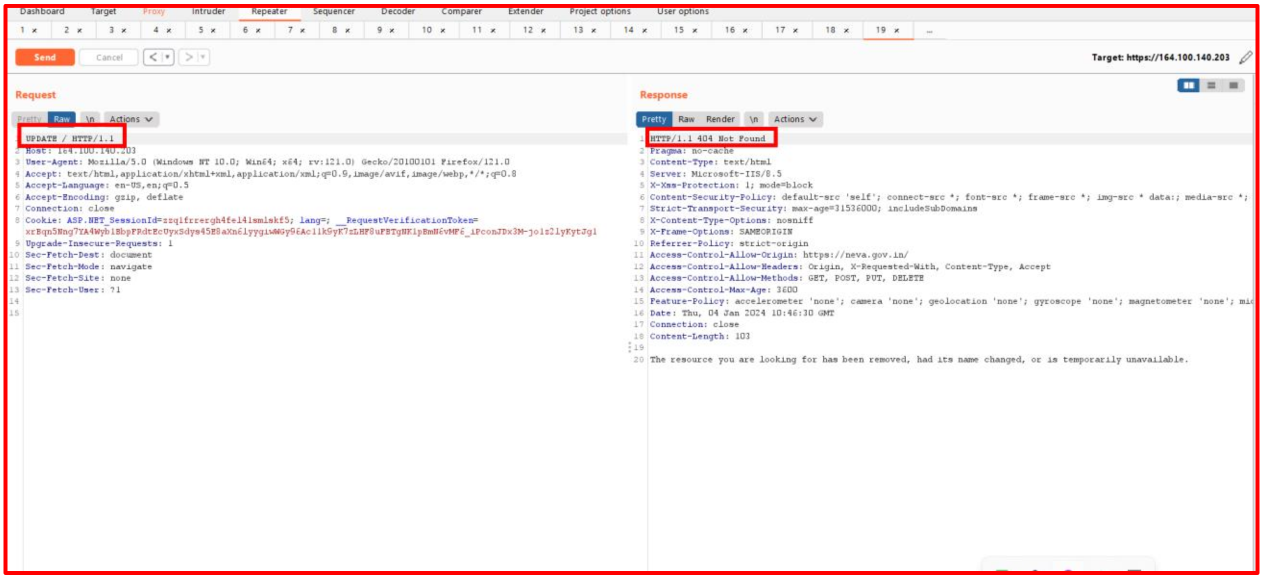
```
DEBUG / HTTP/1.1
Host: 164.100.140.203
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ASP.NET_SessionId=zzqlfrrergh4fel4lsmlskf5; lang=; __RequestVerificationToken=
xrBqn5Nng7YA4Wyb1BbpFRdtEcUyxSdys45E8aXn6lyygiwWGy96Ac11k9yK7zLHF8uFBTgNK1pBmN6vMF6_iPconJDx3M-jo1z2lyKytJg1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

```
HTTP/1.1 404 Not Found
Pragma: no-cache
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Xss-Protection: 1; mode=block
Content-Security-Policy: default-src 'self'; connect-src *; font-src *; frame-src *; img-src * data:; media-src *;
Strict-Transport-Security: max-age=31536000; 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: 3600
Feature-Policy: accelerometer 'none'; camera 'none'; geolocation 'none'; gyroscope 'none'; magnetometer 'none'; mic
Date: Thu, 04 Jan 2024 10:48:25 GMT
Connection: close
Content-Length: 103

The resource you are looking for has been removed, had its name changed, or is temporarily unavailable.
```



```
TRACK / HTTP/1.1
Host: 164.100.140.203
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
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
Connection: close
Cookie: ASP.NET_SessionId=zzqlfrrergh4fel4lsmlskf5; lang=; __RequestVerificationToken=
xrBqn5Nng7YA4Wyb1BbpFRdtEcUyxSdys45E8aXn6lyygiwWGy96Ac11k9yK7zLHF8uFBTgNK1pBmN6vMF6_iPconJDx3M-jo1z2lyKytJg1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

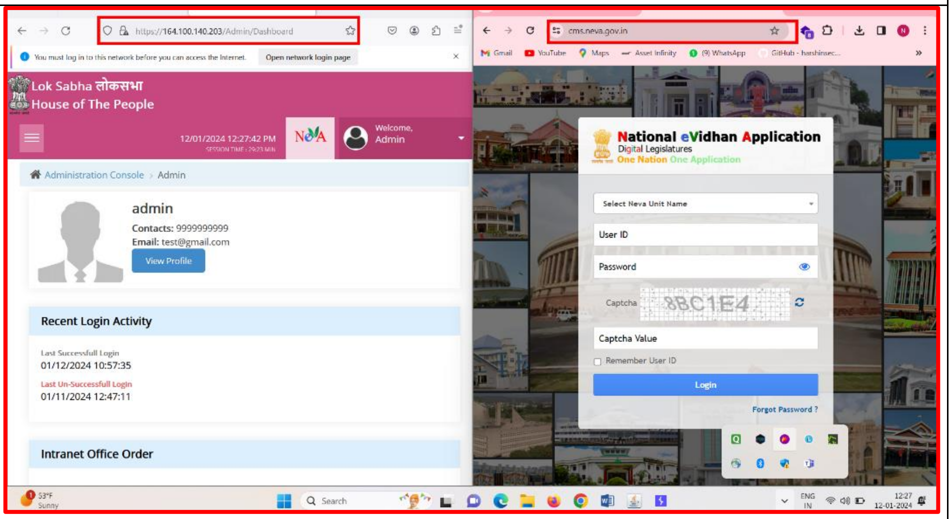
```
HTTP/1.1 404 Not Found
Pragma: no-cache
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Xss-Protection: 1; mode=block
Content-Security-Policy: default-src 'self'; connect-src *; font-src *; frame-src *; img-src * data:; media-src *;
Strict-Transport-Security: max-age=31536000; includeSubDomains
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: 3600
Feature-Policy: accelerometer 'none'; camera 'none'; geolocation 'none'; gyroscope 'none'; magnetometer 'none'; mic
Date: Thu, 04 Jan 2024 10:49:03 GMT
Connection: close
Content-Length: 103

The resource you are looking for has been removed, had its name changed, or is temporarily unavailable.
```



```
UPDATE / HTTP/1.1
Host: 164.100.140.203
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
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
Connection: close
Cookie: ASP.NET_SessionId=zzqlfrrergh4fel4lsmlskf5; lang=; __RequestVerificationToken=
xrBqn5Nng7YA4Wyb1BbpFRdtEcUyxSdys45E8aXn6lyygiwWGy96Ac11k9yK7zLHF8uFBTgNK1pBmN6vMF6_iPconJDx3M-jo1z2lyKytJg1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

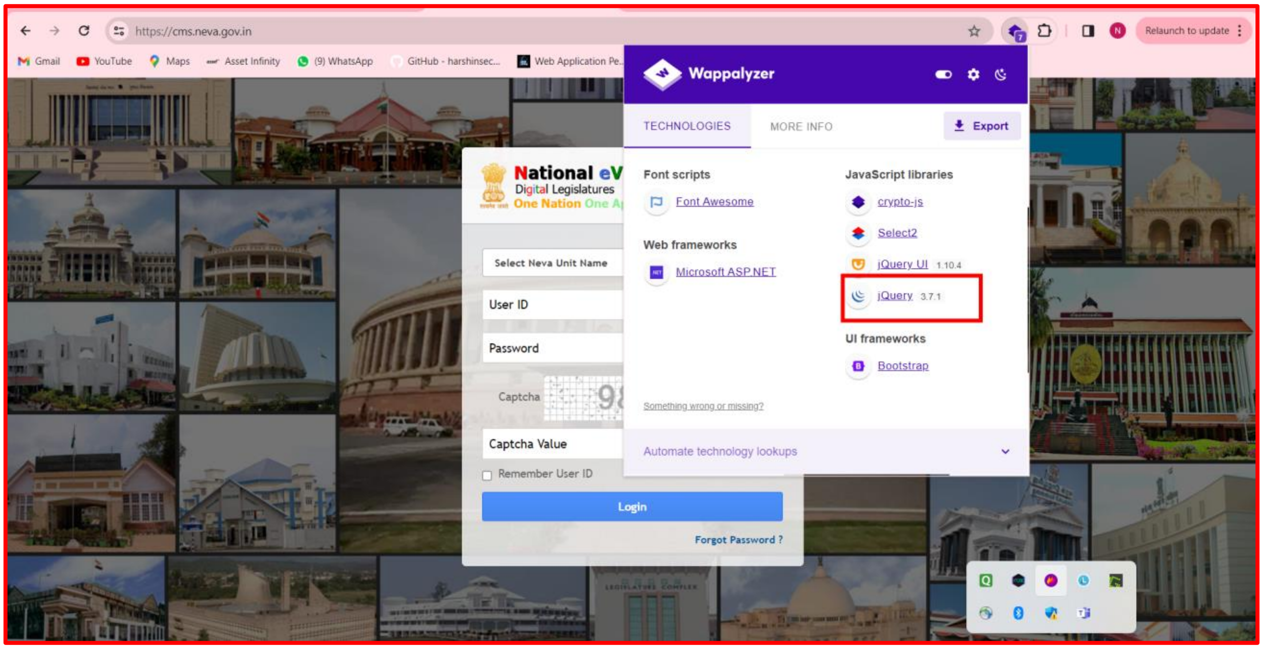
```
HTTP/1.1 404 Not Found
Pragma: no-cache
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Xss-Protection: 1; mode=block
Content-Security-Policy: default-src 'self'; connect-src *; font-src *; frame-src *; img-src * data:; media-src *;
Strict-Transport-Security: max-age=31536000; includeSubDomains
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: 3600
Feature-Policy: accelerometer 'none'; camera 'none'; geolocation 'none'; gyroscope 'none'; magnetometer 'none'; mic
Date: Thu, 04 Jan 2024 10:46:30 GMT
Connection: close
Content-Length: 103

The resource you are looking for has been removed, had its name changed, or is temporarily unavailable.
```

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	 https://164.100.140.203/Admin/Dashboard You must log in to this network before you can access the Internet. Open network login page Lok Sabha लोकसभा House of The People 12/01/2024 12:27:42 PM SESSION TIME : 29:23 MIN NeVA Welcome, Admin Administration Console › Admin admin Contacts: 9999999999 Email: test@gmail.com View Profile Recent Login Activity Last Successfull Login 01/12/2024 10:57:35 Last Un-Successfull Login 01/11/2024 12:47:11 Intranet Office Order cms.neva.gov.in Gmail YouTube Maps Asset Infinity (9) WhatsApp GitHub - harshinsec... National eVidhan Application Digital Legislatures One Nation One Application Select Neva Unit Name User ID Password Captcha 8BC1E4 Captcha Value □ Remember User ID Login Forgot Password ? 53°F Sunny Search ENG IN 12:27 12-01-2024
Affected Site	https://164.100.140.203
Status	Complied

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



https://cms.neva.gov.in

Font scripts
- Font Awesome

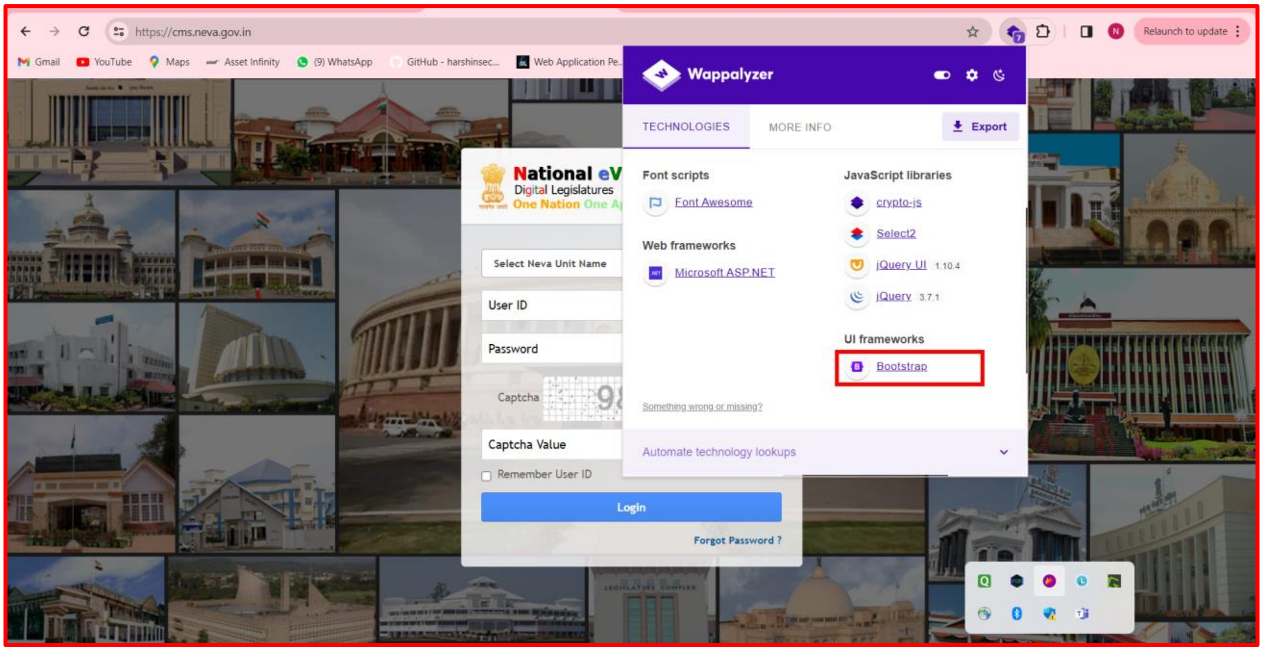
Web frameworks
- Microsoft ASP.NET

JavaScript libraries
- crypto-js
- Select2
- jQuery UI 1.10.4
- jQuery 3.7.1

UI frameworks
- Bootstrap

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



Font scripts
Font Awesome

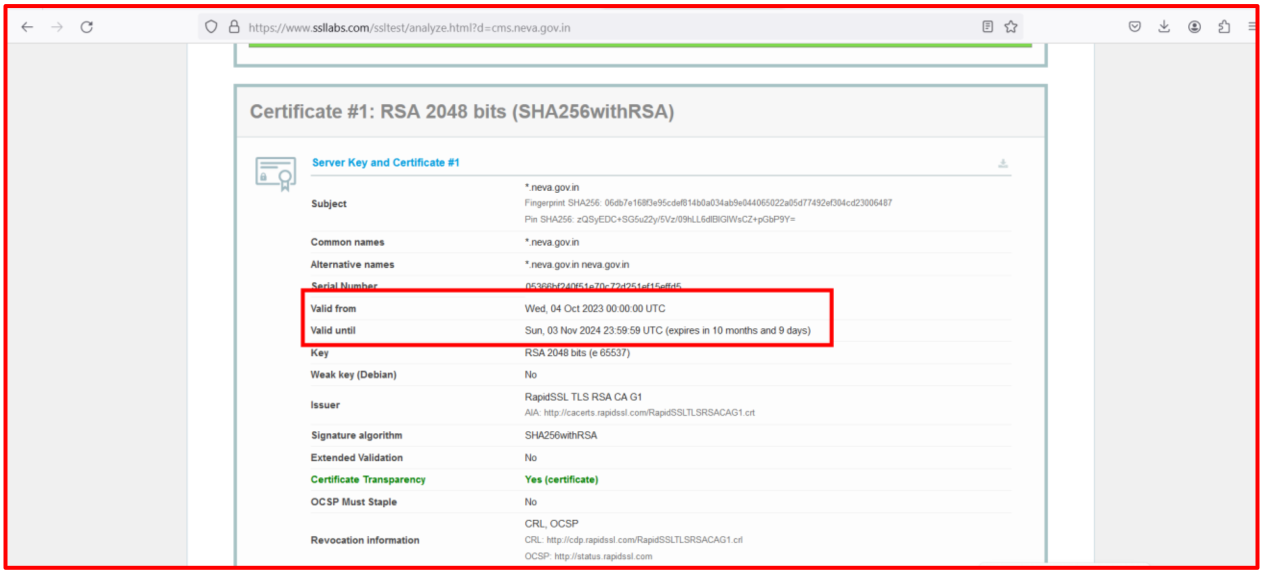
Web frameworks
Microsoft ASP.NET

JavaScript libraries
crypto-js
Select2
jQuery UI 1.10.4
jQuery 3.7.1

UI frameworks
Bootstrap

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



https://www.ssllabs.com/ssltest/analyze.html?d=cms.neva.gov.in

Certificate #1: RSA 2048 bits (SHA256withRSA)

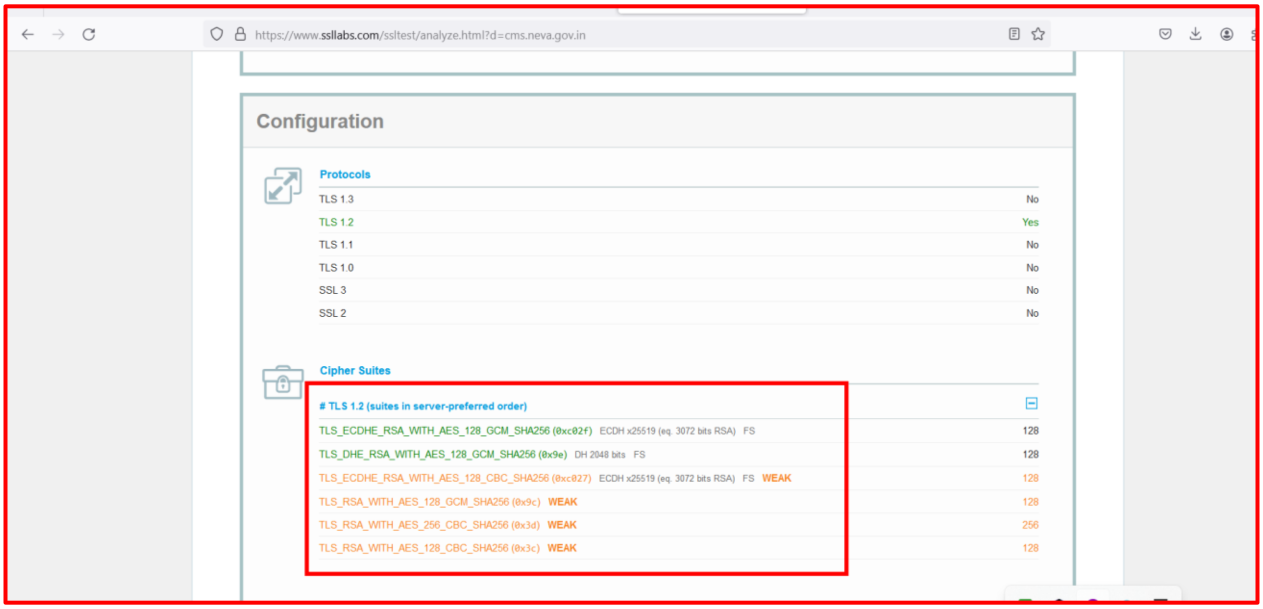
Server Key and Certificate #1

Subject	*.neva.gov.in Fingerprint SHA256: 06db7e168f3e95cdef814b0a034ab9e044065022a05d77492ef304cd23006487 Pin SHA256: zQSyEDC+SG5u22y/5Vz/09hLL6dlBIGIWsCZ+pGbP9Y=
Common names	*.neva.gov.in
Alternative names	*.neva.gov.in neva.gov.in
Serial Number	05366bf240f51e70c72d251ef15effd5
Valid from	Wed, 04 Oct 2023 00:00:00 UTC
Valid until	Sun, 03 Nov 2024 23:59:59 UTC (expires in 10 months and 9 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	RapidSSL TLS RSA CA G1 AIA: http://cacerts.rapidssl.com/RapidSSLTLSRSACAG1.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://cdp.rapidssl.com/RapidSSLTLSRSACAG1.crl OCSP: http://status.rapidssl.com

Medium

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



https://www.ssllabs.com/ssltest/analyze.html?d=cms.neva.gov.in

Configuration

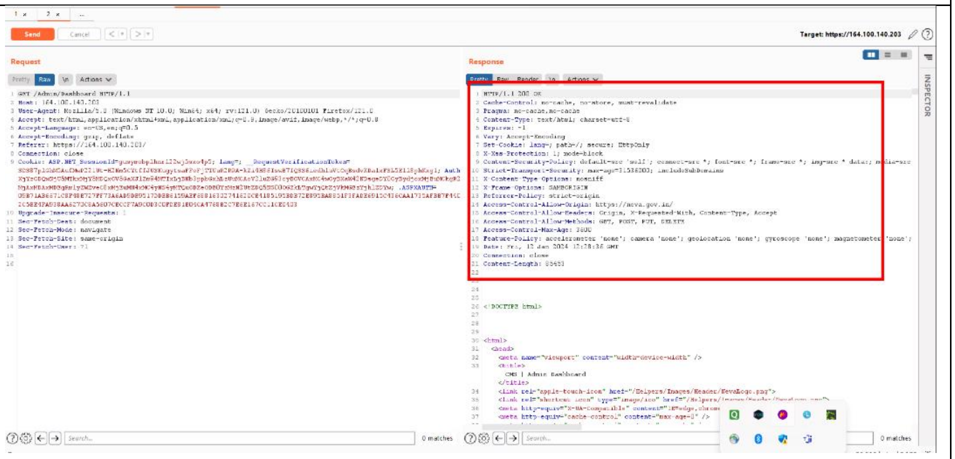
Protocols

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

Cipher Suites

# TLS 1.2 (suites in server-preferred order)	
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK	128

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**

Request:

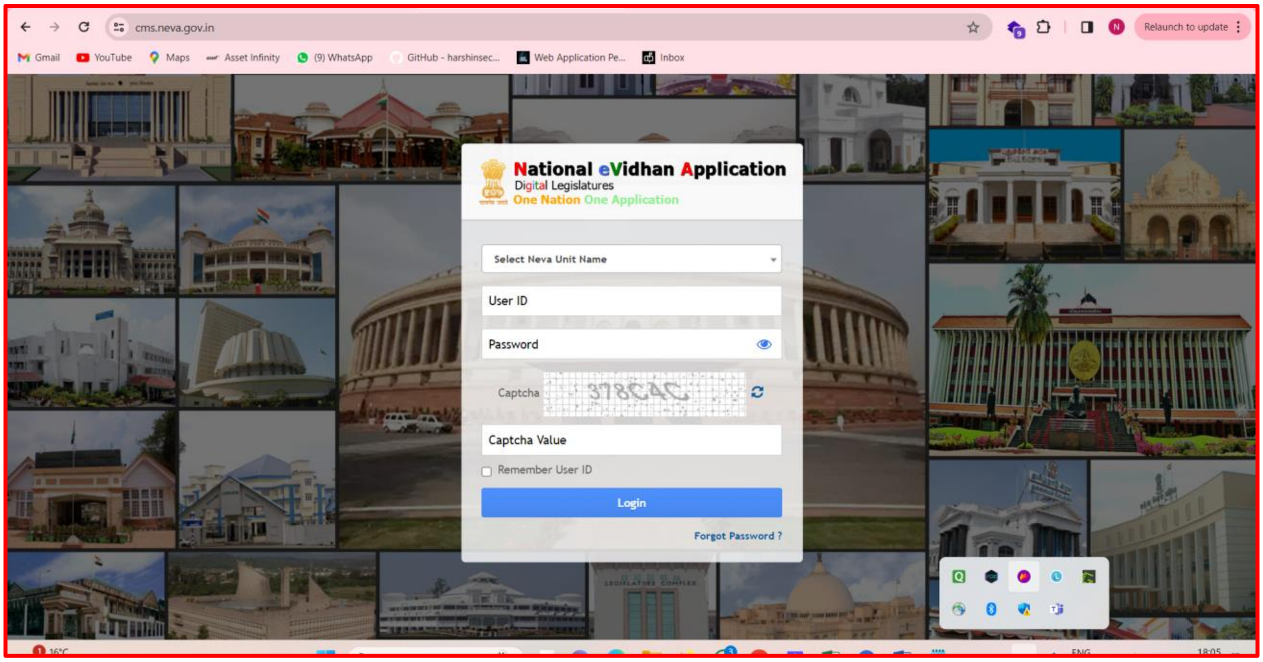
```
GET /Admin/Dashboard HTTP/1.1
Host: 164.100.140.203
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://164.100.140.203/
Connection: close
Cookie: ASP.NET_SessionId=gumymobplhmr122wj5mxo4p5; lang=; __RequestVerificationToken=
SDS87plGbMSAuCWmP22lUt-H2Nm5CYtfIJUSKugytaaFPoFjTTUuR2RDA-k2i4HS6Isw87IQS86LedhluVcOqBadvXDalxFSL5E118phKxg1; Auth
XjYzODQwMjU5MTkxMjY5MDQxOV5GaXJlZm94MTIxLjBNb3ppbGxhLzUuMCAoV2luZG93cyBOVCAxMC4wOyBXaW42NDsgeDY0OyBydjoxMjEuMCkgR2
MjAxMDAxMDEgRmlyZWZveC8xMjEuMDQxMC4yNS4yMTQuODZeODE0YzMzN2UtZDQ5ZS00OGZkLTgwYjQtZjVkMGEzYjhlZDYw; .ASPXAUTH=
05B71AB6671C8F48E727FF73A6AD5DE95173D8B6155A2F6881633274162DC8418519580372E895BA8851F3FAD26915C436CAA1735AFBB7F45C
2C5BE4FA938AA627DC8A5607CECCF7A9C0D3CDFDEB1BD4CA4768B2C7E6E167CC11CE0403
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

Response:

```
HTTP/1.1 200 OK
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 * data:; media-src
Strict-Transport-Security: max-age=31536000; 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: 3600
Feature-Policy: accelerometer 'none'; camera 'none'; geolocation 'none'; gyroscope 'none'; magnetometer 'none';
Date: Fri, 12 Jan 2024 12:28:36 GMT
Connection: close
Content-Length: 85453



<!DOCTYPE html>



<html>
  <head>
    <meta name="viewport" content="width=device-width" />
    <title>
      CMS | Admin Dashboard
    </title>
    <link rel="apple-touch-icon" href="/Helpers/Images/Header/NevaLogo.png">
    <link rel="shortcut icon" type="image/ico" href="/Helpers/Images/Header/NevaLogo.png">
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome
    <meta http-equiv="cache-control" content="max-age=0" />
```

9. Session Timeout Is Not Implemented

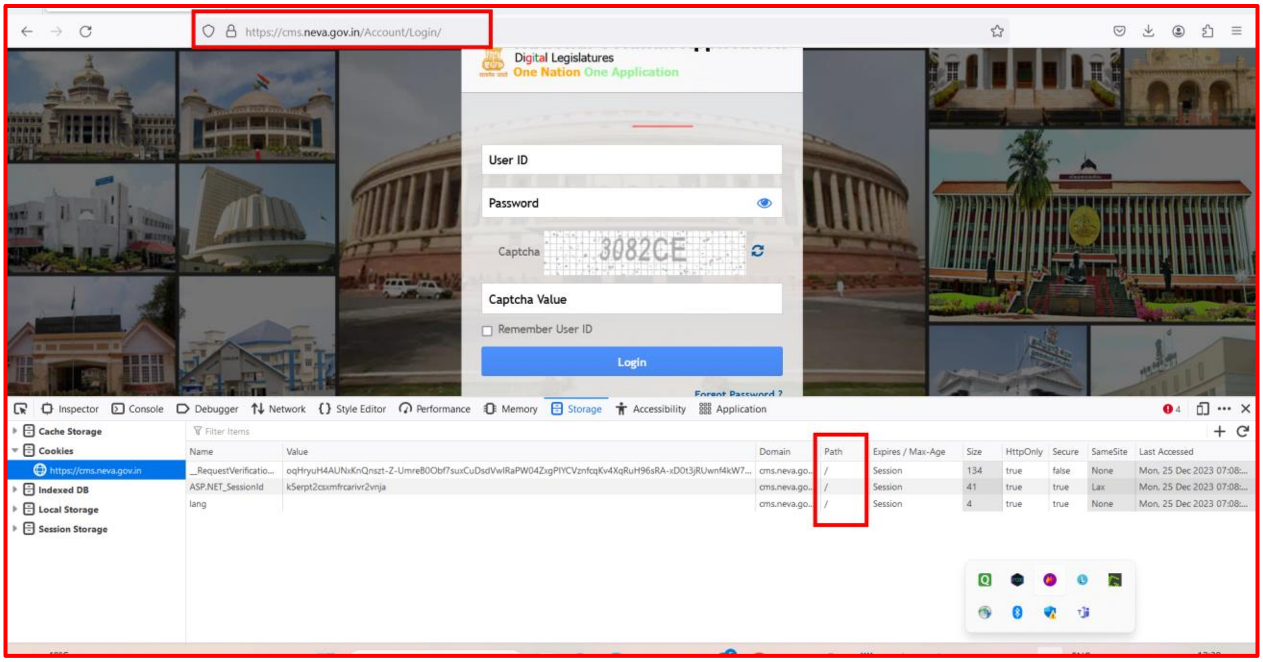
Vulnerability Title: Session Timeout not implemented	
Risk	**Medium**
Abstract	It was observed that even if the Browser is logged in and idle it does not logout the session automatically.
Ease of Exploitation	Easy
Impact	It is possible to access authenticated pages.
Recommendations	Application should 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



Low

10.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

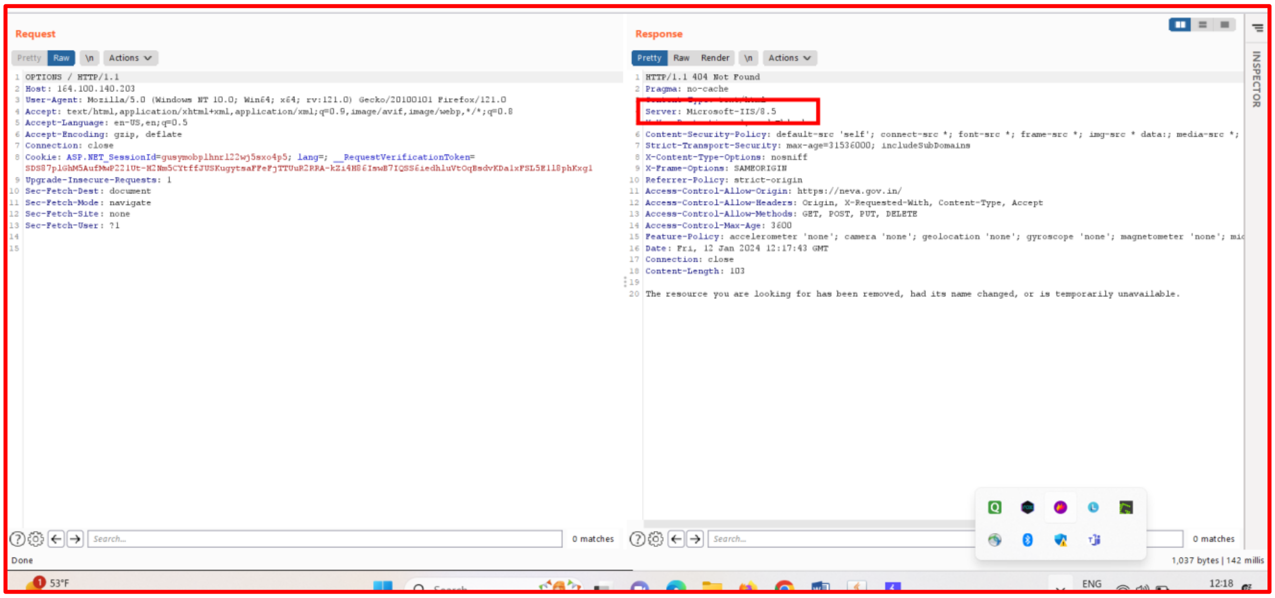


Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
_RequestVerificatio...	oqHryuH4AUNxKnQnszt-Z-UmreB0Obf7suxCuDsdVwIRaPW04ZxgPIYCVznfcqKv4XqRuH96sRA-xD0t3jRUwnf4kW7...	cms.neva.go...	/	Session	134	true	false	None	Mon, 25 Dec 2023 07:08:...
ASP.NET_SessionId	k5erpt2csxmfrcarivr2vnja	cms.neva.go...	/	Session	41	true	true	Lax	Mon, 25 Dec 2023 07:08:...
lang		cms.neva.go...	/	Session	4	true	true	None	Mon, 25 Dec 2023 07:08:...

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

11.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

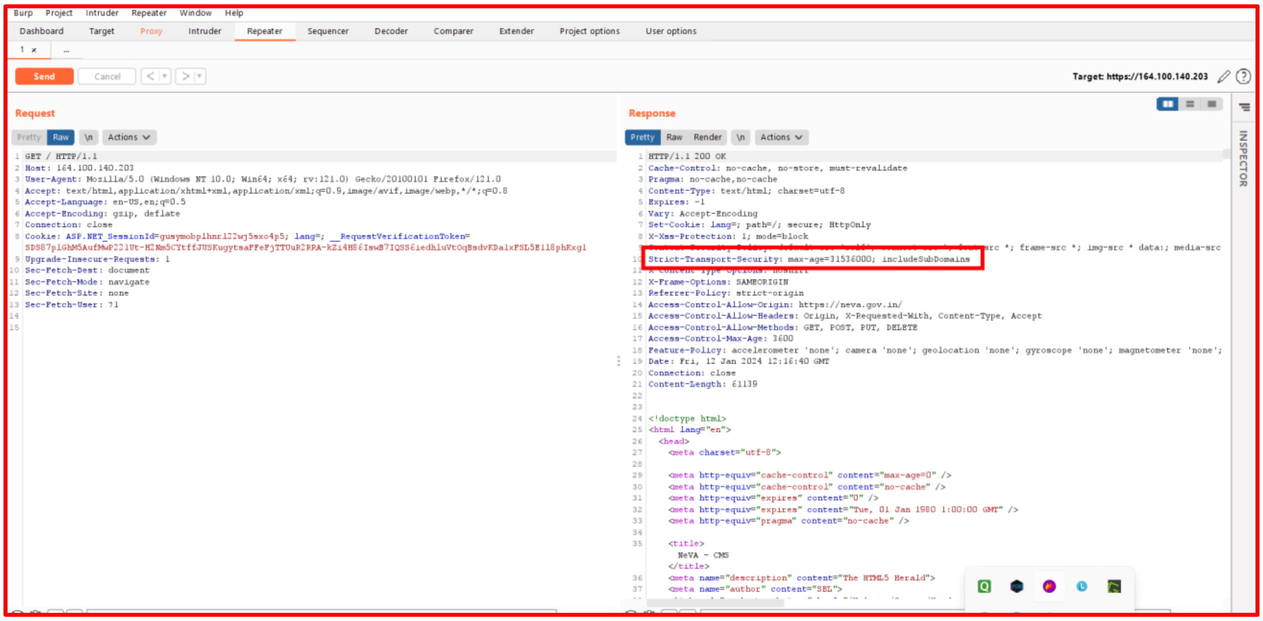


```
OPTIONS / HTTP/1.1
Host: 164.100.140.203
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ASP.NET_SessionId=gusymobplhnr122wj5sxo4p5; lang=; __RequestVerificationToken=
SDS87plGhM5AufMwP221Ut-H2Nm5CYtffJUSKugytsaFFeFjTTUuR2RRA-kZi4H86IswB7IQSS6iedhluVtOqBsdvKDalxFSL5E118phKxgl
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

```
HTTP/1.1 404 Not Found
Pragma: no-cache
Content-Type: text/html
Server: Microsoft-IIS/8.5
Content-Security-Policy: default-src 'self'; connect-src *; font-src *; frame-src *; img-src * data:; media-src *;
Strict-Transport-Security: max-age=31536000; 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: 3600
Feature-Policy: accelerometer 'none'; camera 'none'; geolocation 'none'; gyroscope 'none'; magnetometer 'none'; mic
Date: Fri, 12 Jan 2024 12:17:43 GMT
Connection: close
Content-Length: 103

The resource you are looking for has been removed, had its name changed, or is temporarily unavailable.
```

12.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


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 ×
...
Send
Cancel
Target: https://164.100.140.203
Request
Pretty Raw \n Actions
Response
Pretty Raw Render \n Actions
INSPECTOR

Request

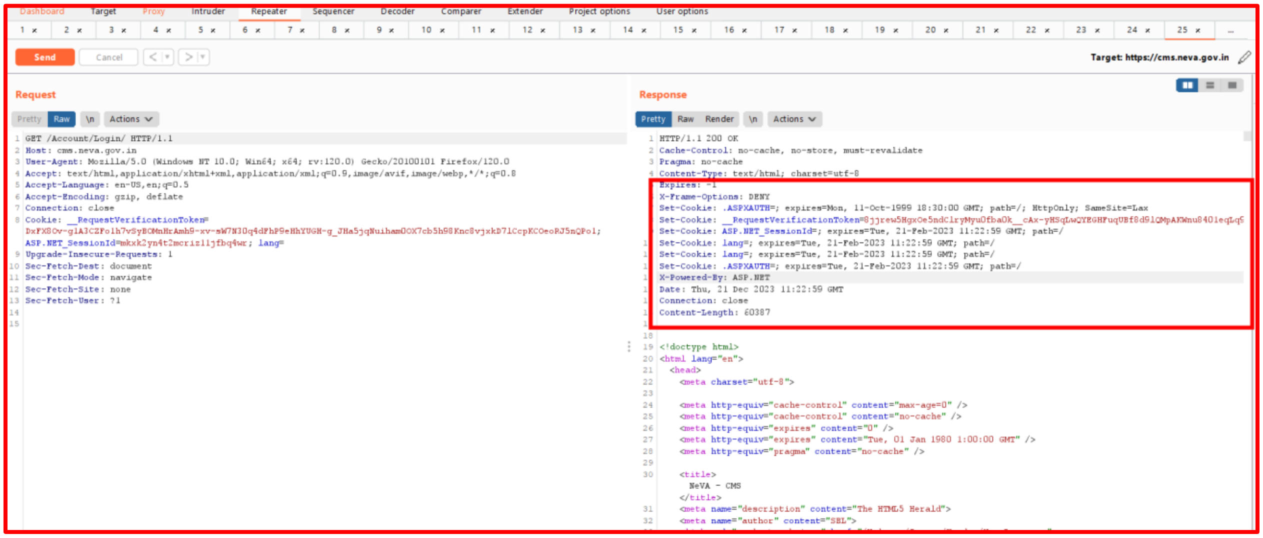
```
GET / HTTP/1.1
Host: 164.100.140.203
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ASP.NET_SessionId=gusymobplhnr122wj5sxo4p5; lang=; __RequestVerificationToken=
SDS87plGhM5AufMwP221Ut-H2Nm5CYtffJUSKugytsaFFeFjTTUuR2RRA-kZi4H86IswB7IQSS6iedhluVtOqBsdvKDalxFSL5E118phKxgl
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1


```

Response

```
HTTP/1.1 200 OK
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 * data:; media-src
Strict-Transport-Security: max-age=31536000; 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: 3600
Feature-Policy: accelerometer 'none'; camera 'none'; geolocation 'none'; gyroscope 'none'; magnetometer 'none';
Date: Fri, 12 Jan 2024 12:16:40 GMT
Connection: close
Content-Length: 61139


<!doctype html>
<html lang="en">
  <head>
    <meta charset="utf-8">

    <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" />

    <title>
      NeVA - CMS
    </title>
    <meta name="description" content="The HTML5 Herald">
    <meta name="author" content="SBL">
```

13.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

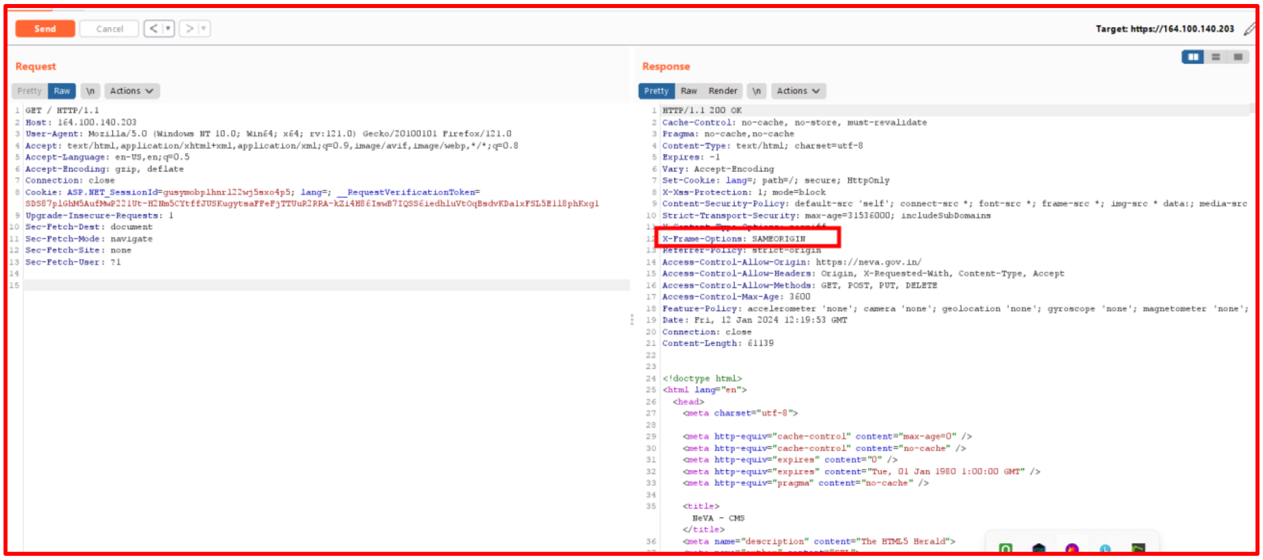


```
GET /Account/Login/ HTTP/1.1
Host: cms.neva.gov.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: __RequestVerificationToken=
DxFX8Ov-glA3CZFolh7vSyBOMnHrAmh9-xv-sW7N30q4dFhP9eHhYUGH-g_JHa5jqNuihamOOX7cb5h98Knc8vjxkD71CcpKCOeoRJ5nQPol;
ASP.NET_SessionId=mkxk2yn4t2mcriz11jfbq4wr; lang=
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
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
X-Frame-Options: DENY
Set-Cookie: .ASPXAUTH=; expires=Mon, 11-Oct-1999 18:30:00 GMT; path=/; HttpOnly; SameSite=Lax
Set-Cookie: __RequestVerificationToken=8jjrew5HgxOe5ndClryMyuOfbaOk__cAx-yHSqLwQYEGHFuqUBf8d9lQMpAKWnu840leqLq5
Set-Cookie: ASP.NET_SessionId=; expires=Tue, 21-Feb-2023 11:22:59 GMT; path=/
Set-Cookie: lang=; expires=Tue, 21-Feb-2023 11:22:59 GMT; path=/
Set-Cookie: lang=; expires=Tue, 21-Feb-2023 11:22:59 GMT; path=/
Set-Cookie: .ASPXAUTH=; expires=Tue, 21-Feb-2023 11:22:59 GMT; path=/
X-Powered-By: ASP.NET
Date: Thu, 21 Dec 2023 11:22:59 GMT
Connection: close
Content-Length: 60387

<!doctype html>
<html lang="en">
  <head>
    <meta charset="utf-8">

    <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" />

    <title>
      NeVA - CMS
    </title>
    <meta name="description" content="The HTML5 Herald">
    <meta name="author" content="SBL">
```

14.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

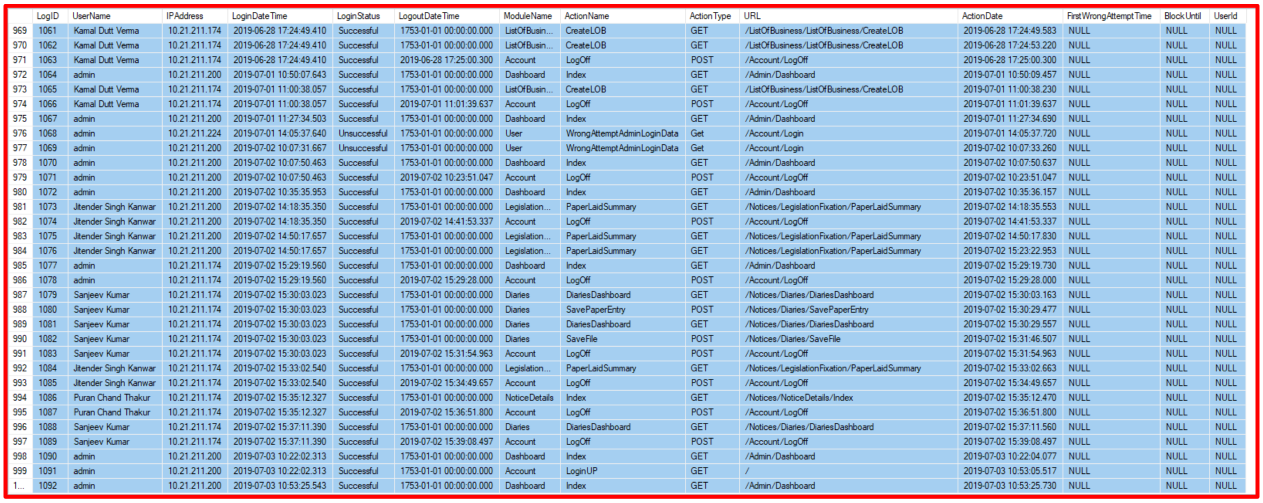


```
GET / HTTP/1.1
Host: 164.100.140.203
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ASP.NET_SessionId=gusymobplhnr122wj5sxo4p5; lang=; __RequestVerificationToken=
SDS87plGhM5AufMwP221Ut-H2Nm5CYtffJUSKugytsaFFeFjTTUuR2RRA-kZi4H86IswB7IQSS6iedhluVtOqBsdvKDa1xFSL5E118phKxg1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

```
HTTP/1.1 200 OK
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 * data:; media-src
Strict-Transport-Security: max-age=31536000; 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: 3600
Feature-Policy: accelerometer 'none'; camera 'none'; geolocation 'none'; gyroscope 'none'; magnetometer 'none';
Date: Fri, 12 Jan 2024 12:19:53 GMT
Connection: close
Content-Length: 61139


<!doctype html>
<html lang="en">
  <head>
    <meta charset="utf-8">

    <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" />

    <title>
      NeVA - CMS
    </title>
    <meta name="description" content="The HTML5 Herald">
```

15.Audit Trail is not maintained

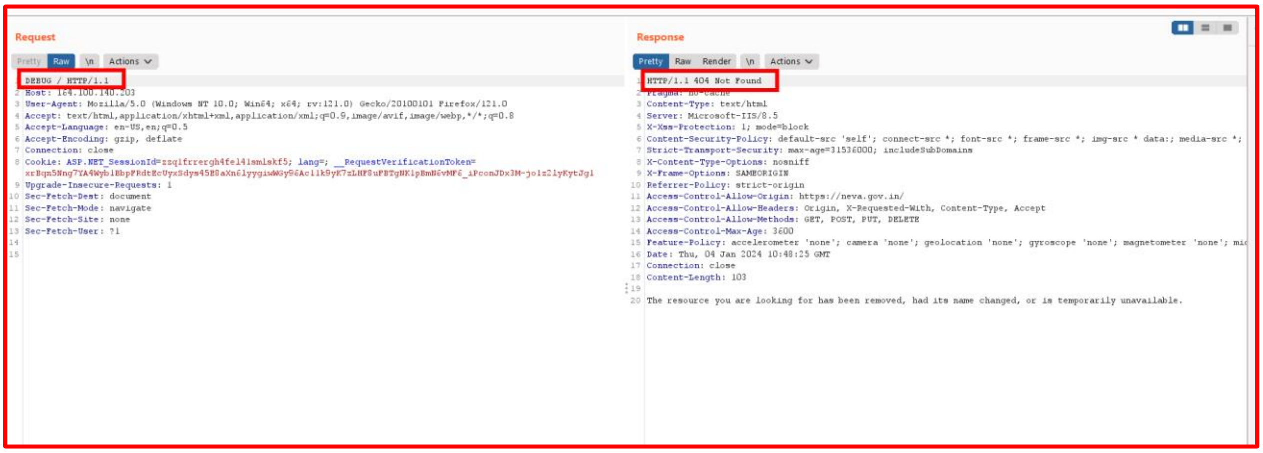
Vulnerability Title: Audit Trail is not implemented in properly	
Risk	**Low**
Abstract	The application does not maintain the logout action and status of user activity where all user activities have to be logged.
Ease of Exploitation	Easy
Impact	In-case a malicious user tries to attack the application; the application will not be able to trace the attacker
Recommendations	An Audit trail should be incorporated in the application admin module, where all user activities have to be logged. Following points should be considered: • 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



	LogID	UserName	IPAddress	LoginDateTime	LoginStatus	LogoutDateTime	ModuleName	ActionName	ActionType	URL	ActionDate	FirstWrongAttemptTime	BlockUntil	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 11:27:34.690	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 10:35:35.953	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	Diaries	DiariesDashboard	GET	/Notices/Diaries/DiariesDashboard	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	Diaries	SavePaperEntry	POST	/Notices/Diaries/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	Diaries	DiariesDashboard	GET	/Notices/Diaries/DiariesDashboard	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	Diaries	SaveFile	POST	/Notices/Diaries/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	Diaries	DiariesDashboard	GET	/Notices/Diaries/DiariesDashboard	2019-07-02 15:37:11.560	NULL	NULL	NULL
997	1089	Sanjeev Kumar	10.21.211.174	2019-07-02 15:37:11.390	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

16.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

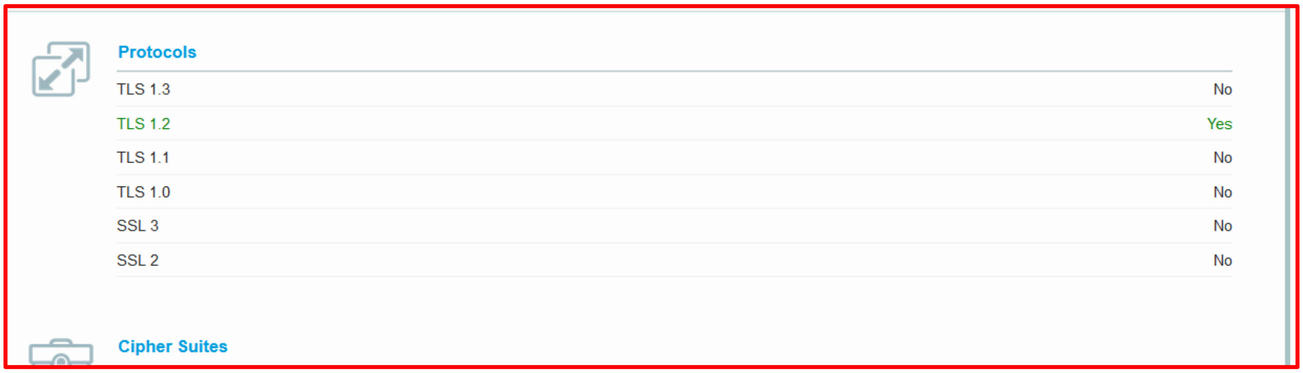


```
DEBUG / HTTP/1.1
Host: 164.100.140.203
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ASP.NET_SessionId=zzqlfrrergh4fel4lsmlskf5; lang=; __RequestVerificationToken=
xrBqn5Nng7YA4Wyb1BbpFRdtEcUyxSdys45E8aXn6lyygiwWGy96Acl1k9yK7zLHF8uFBTgNKlpBmN6vMF6_iPconJDx3M-jo1z2lyKytJg1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

```
HTTP/1.1 404 Not Found
Pragma: no-cache
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Xss-Protection: 1; mode=block
Content-Security-Policy: default-src 'self'; connect-src *; font-src *; frame-src *; img-src * data:; media-src *;
Strict-Transport-Security: max-age=31536000; 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: 3600
Feature-Policy: accelerometer 'none'; camera 'none'; geolocation 'none'; gyroscope 'none'; magnetometer 'none'; mic
Date: Thu, 04 Jan 2024 10:48:25 GMT
Connection: close
Content-Length: 103

The resource you are looking for has been removed, had its name changed, or is temporarily unavailable.
```

17.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



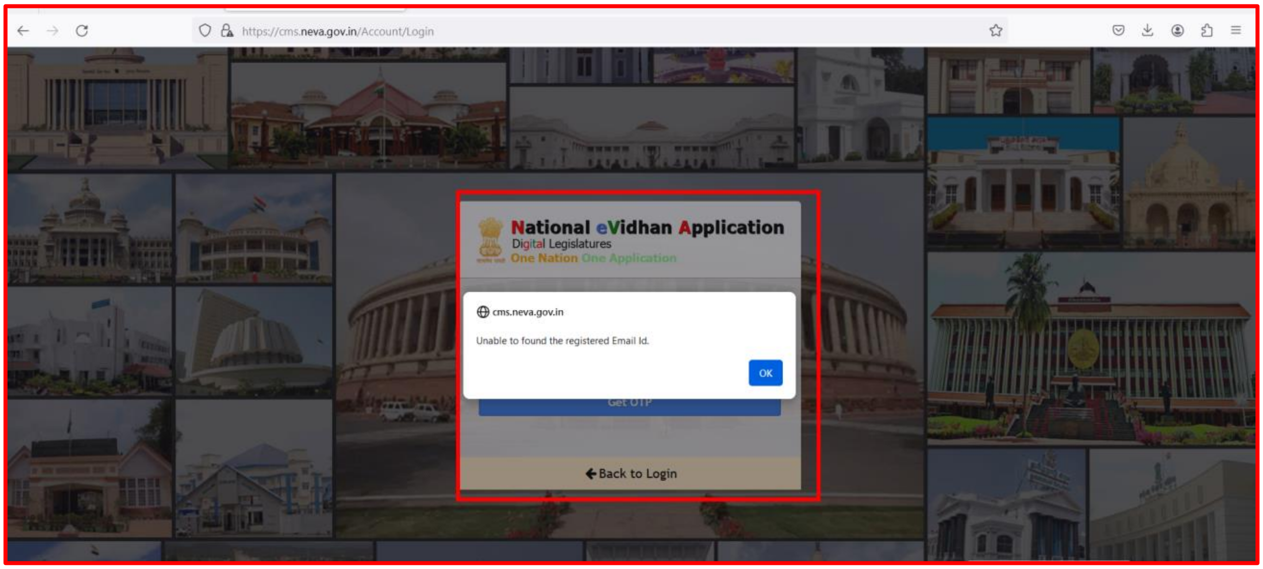
Protocols

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

Cipher Suites

18.User Enumeration

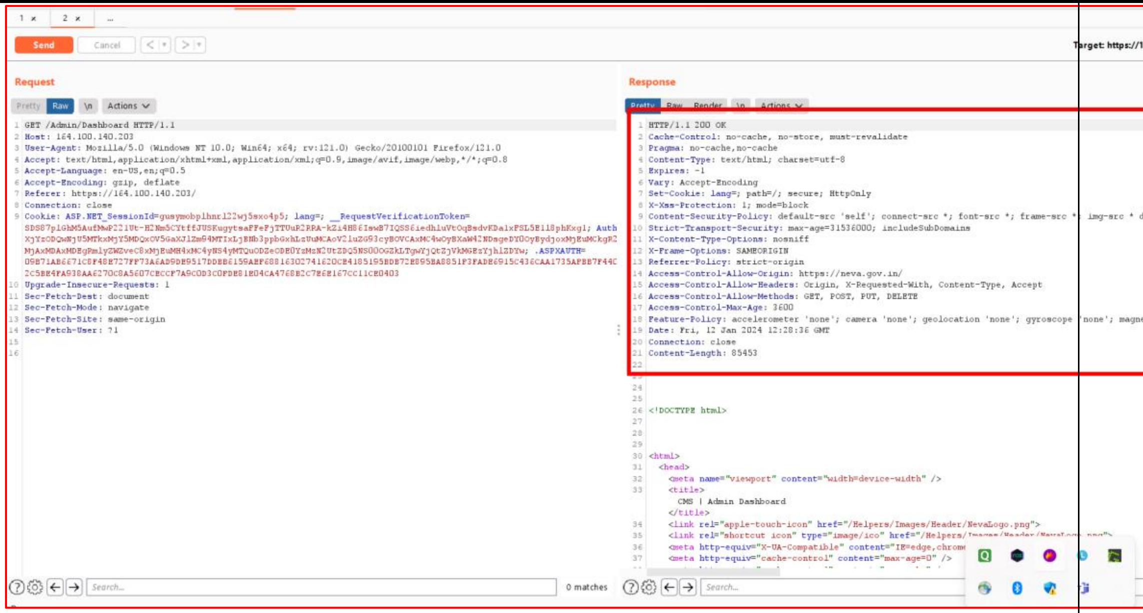
Vulnerability Title: User Enumeration is possible in application	
Risk	**Low**
Abstract	User enumeration is a security vulnerability that occurs when an attacker can determine whether a specific username or email address is valid or not within a system, application, or service.
Ease of Exploitation	Easy
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	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: 1. User-ID or password is Invalid. Or 2.Please enter valid credentials. Or 3.Wrong Username or Password. 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."
Snapshot	Attached Below
Affected URLs	https://164.100.140.203
Status	Not Complied


https://cms.neva.gov.in/Account/Login
National eVidhan Application
Digital Legislatures
One Nation One Application
Get OTP
Back to Login

cms.neva.gov.in

Unable to found the registered Email Id.

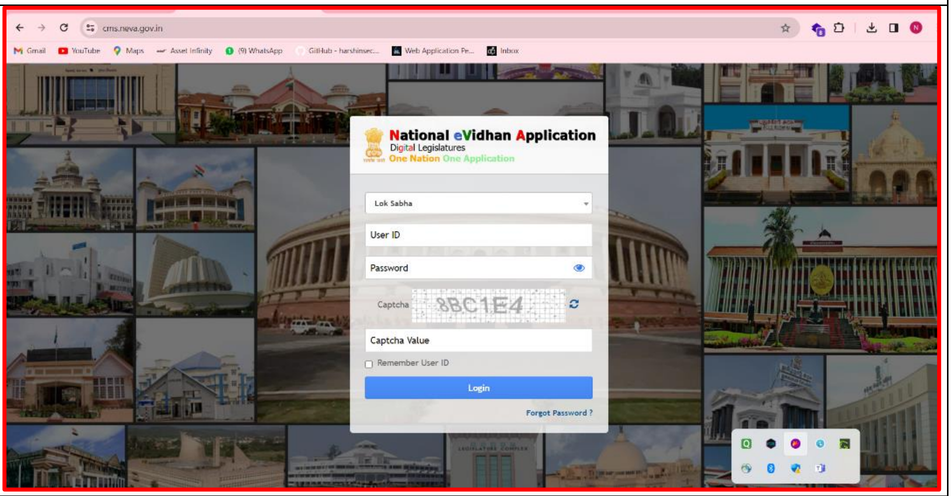
19.E-tag

Vulnerability Title: E-tag Information Disclosure	
Risk	**Low**
Abstract	It was observed that the Server Responds with E-tag Information Disclosure Vulnerabilit
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 in the ETag header calculation
Snapshot	
Affected Site	https://164.100.140.203
Status	Complied

```
GET /Admin/Dashboard HTTP/1.1
Host: 164.100.140.203
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
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://164.100.140.203/
Connection: close
Cookie: ASP.NET_SessionId=gusymobplhnrl22wj5sxo4p5; lang=; __RequestVerificationToken=
SDS87plGhM5AufMwP221Ut-H2Nm5CYtffJUSKugytsaFFeFjTTUuR2RPA-kZi4H86IswB7IQSS6iedhluVtOqBsdvKDalxPSL5E1l8phKxgl; Auth
XjYzODQwNjU5MTkxMjY5MDQxOV5GaXJlZm94MTIxLjBNb3ppbGxhLzUuMCAoV2luZG93cyBOVCAxMC4wOyBXaW42NDsgeDY0OyBydjoxMjEuMCkgR2
MjAxMDAxMDEgRmlyZWZveC8xMjEuMH4xMC4yNS4yMTQuODZeODE0YzMzN2UtZDQ5NS00OGZkLTgwYjQtZjVkMGEzYjhlZDYw; .ASPXAUTH=
09B71AB6671C8F48E727FF73A6AD9DE9517DDBB6159AEF6881630274162OCE4185195BDE72E895BA8851F3FADE6915C436CAA1735AFBB7F44C
2C5BE4FA938AA6270C8A5607CECCF7A9C0D3C0FDE81E04CA4768B2C7E6E167CC11CE0403
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,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 * d
Strict-Transport-Security: max-age=31536000; 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: 3600
Feature-Policy: accelerometer 'none'; camera 'none'; geolocation 'none'; gyroscope 'none'; magne
Date: Fri, 12 Jan 2024 12:28:36 GMT
Connection: close
Content-Length: 85453



<!DOCTYPE html>



<html>
  <head>
    <meta name="viewport" content="width=device-width" />
    <title>
      CMS | Admin Dashboard
    </title>
    <link rel="apple-touch-icon" href="/Helpers/Images/Header/NevaLogo.png">
    <link rel="shortcut icon" type="image/ico" href="/Helpers/Images/Header/NevaLogo.png">
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome
    <meta http-equiv="cache-control" content="max-age=0" />
```

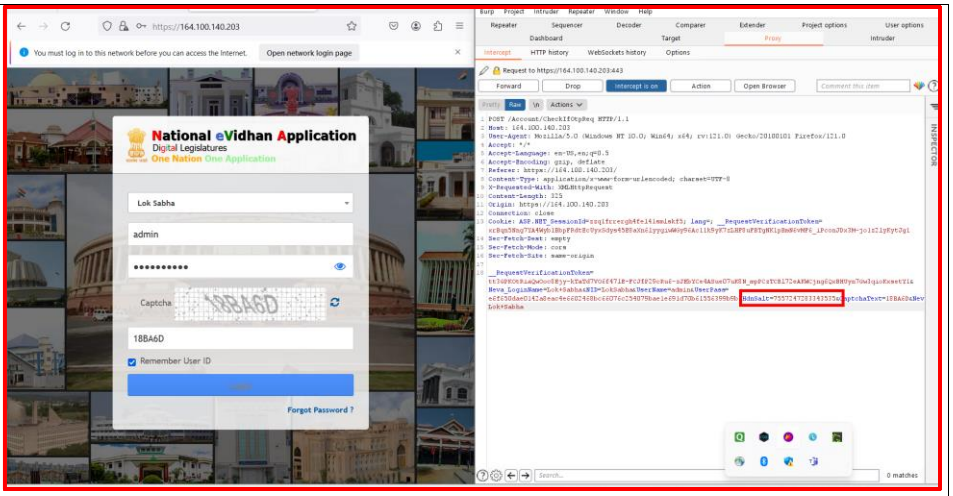
20. Improper Input Validation

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	 cms.neva.gov.in Gmail YouTube Maps Asset Infinity (9) WhatsApp GitHub - harshinsec... Web Application Pe... Inbox National eVidhan Application Digital Legislatures One Nation One Application Lok Sabha User ID Password Captcha 8BC1E4 Captcha Value □ Remember User ID Login Forgot Password ?
Affected Site	**throughout the application**
Status	**Complied**

New Vulnerabilities

21.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	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). 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. 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: • 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.

Snapshot	
Affected URLs	**throughout the application**
Status	**New**

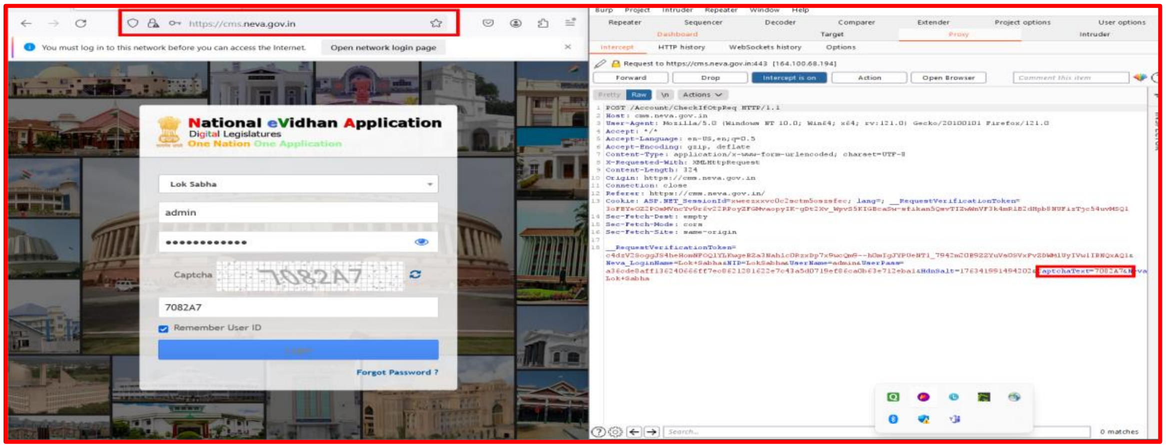
https://164.100.140.203
You must log in to this network before you can access the Internet.
Open network login page
National eVidhan Application
Digital Legislatures
One Nation One Application
Lok Sabha
admin
Captcha
18BA6D
Remember User ID
Forgot Password ?
Burp Project Intruder Repeater Window Help
Repeater Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder
Intercept HTTP history WebSockets history Options
Request to https://164.100.140.203:443
Forward Drop Intercept is on Action Open Browser
Comment this item
Pretty Raw \n Actions
INSPECTOR
0 matches

```
POST /Account/CheckIfOtpReq HTTP/1.1
Host: 164.100.140.203
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://164.100.140.203/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 325
Origin: https://164.100.140.203
Connection: close
Cookie: ASP.NET_SessionId=zzqifrrergh4fe14lemlkf5; lang=; __RequestVerificationToken=
xrBqn5Nng7YA4Wyb1BbpFRdtEcUyxSdys45B8aXn6lyygiwWGy96Ac11kSyK7zLHF8uFBTgNKlpBmN6vMP6_1PconJDx3M-jolz2lyEytJgl
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

__RequestVerificationToken=
tt3GPKO6RiaQwOoc8Bjy-kTaTd7VOf4718-FCJfP25cRuE-zJMbYCe4ASueO7uK8N_mpPCzTC8172eAKWcjng6QxBHUyn7Gw3qioKxsetYi&
Neva_LoginName=Lok+Sabha&NID=LokSabha&UserName=admin&UserPass=
e6f650dae0142a8eac4e66024e8bc66076c254075bae1e691d70b61556399b9b&HdnSalt=755724728334353 5&CaptchaText=18BA6D&Nev
Lok+Sabha
```

22.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:



https://cms.neva.gov.in

You must log in to this network before you can access the Internet. Open network login page

National eVidhan Application
Digital Legislatures
One Nation One Application

Lok Sabha
admin
•••••••••••••
Captcha 7082A7
7082A7
☑ Remember User ID
Login
Forgot Password ?

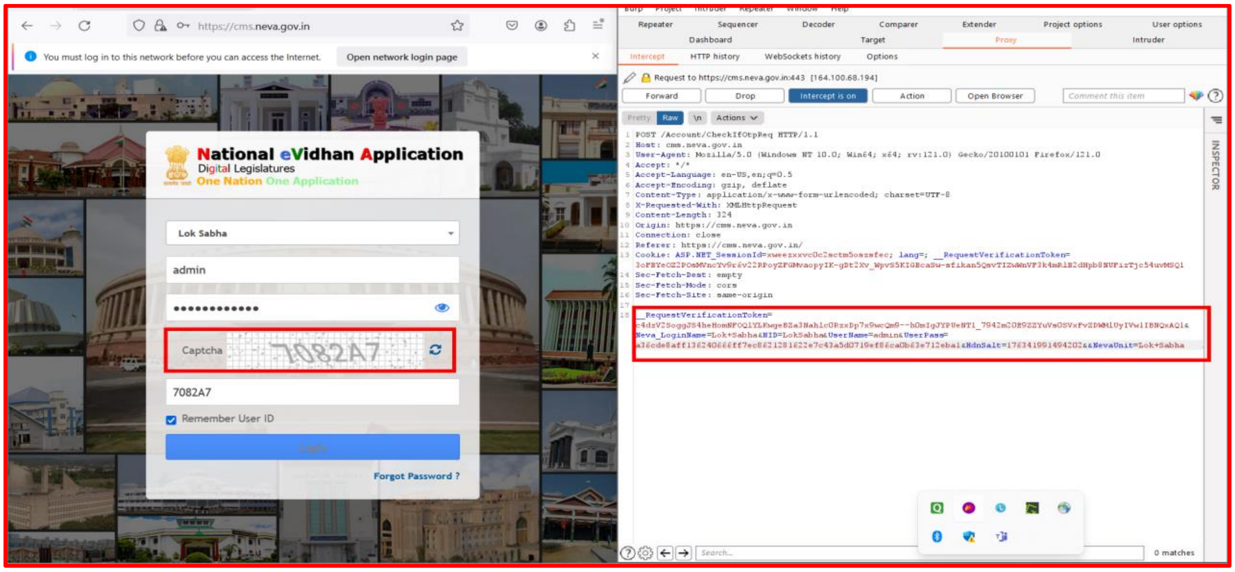
Burp Project Intruder Repeater Window Help
Repeater Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Comment this item
Pretty Raw \n Actions

Request to https://cms.neva.gov.in:443 [164.100.68.194]

```
POST /Account/CheckIfOtpReq HTTP/1.1
Host: cms.neva.gov.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 324
Origin: https://cms.neva.gov.in
Connection: close
Referer: https://cms.neva.gov.in/
Cookie: ASP.NET_SessionId=xweezxxvc0c2sctm5ozzsfec; lang=; __RequestVerificationToken=
3oFBYeOZ2POmMVncYv9r&v22RPoyZFGMvaopyIK-gDt2Xv_WpvS5KIGBca5w-sfikan5QevTIZwWnVF3k4mRlB2dMpb8NUFizTjc54uvMSQ1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

__RequestVerificationToken=
c4dzVZSoggJS4heHomNFOQlYLKwgeRZa3NahlcORzxDp7x9wcQm8--hOmIgJYP0eNT1_7942m20B922YuVeOSVxFvZ0WMlUyIVwlIBNQxAQl&
Neva_LoginName=Lok+Sabha&NID=LokSabha&UserName=admin&UserPass=
a36ode8aff13624066ff7ec8621281622e7c43a5d0719ef86ca0b63e712eba1&HdnSalt=176341991494202&CaptchaText=7082A7&Neva
Lok+Sabha
```

0 matches

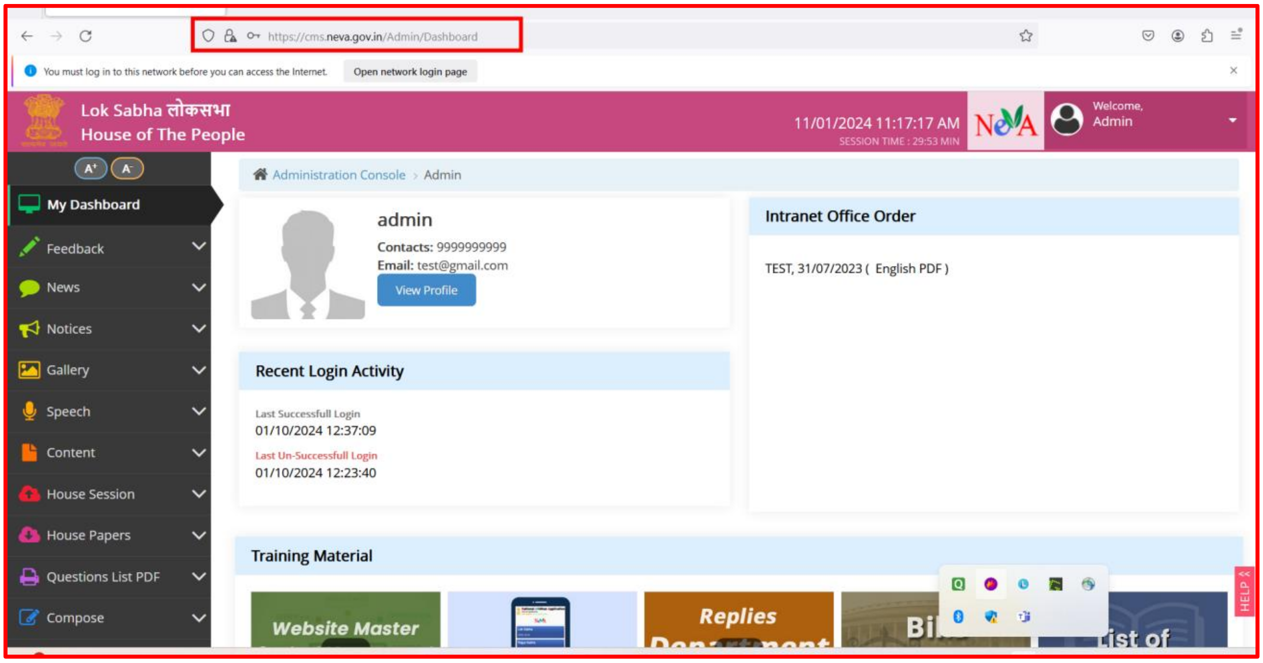
Step#2: Now delete the complete field of captcha in the burp and forward the request as shown below.



Request to https://cms.neva.gov.in:443 [164.100.68.194]

```
POST /Account/CheckIfOtpReq HTTP/1.1
Host: cms.neva.gov.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 324
Origin: https://cms.neva.gov.in
Connection: close
Referer: https://cms.neva.gov.in/
Cookie: ASP.NET_SessionId=xweezxxvcOcZectm5ozzsfec; lang=; __RequestVerificationToken=
3oFBYeOZ2POmMVncYv9r6v22RPoyZFGMvaopyIK-gDt2Xv_WpvS5KIGBcaSw-sfikan5QavTIZwWnVF3k4mRlB2dHpb8NUFizTjc54uvMSQ1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

__RequestVerificationToken=
c4dzVZSoggJS4heHomNFOQlYLKwgeBZa3NahlcORzxDp7x9wcQm9--hOmIgJYPUeNTl_7942m2O8922YuVsOSVxFvZDWMlUyIVwlIBNQxAQl&
Neva_LoginName=Lok+Sabha&NID=LokSabha&UserName=admin&UserPass=
a36cde8aff13624066ff7ec8621281622e7c43a5d0719ef86ca0b63e712eba1&HdnSalt=1763419914942O2&&NevaUnit=Lok+Sabha
```

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



11/01/2024 11:17:17 AM
SESSION TIME : 29:53 MIN

admin
Contacts: 9999999999
Email: test@gmail.com

Intranet Office Order
TEST, 31/07/2023 (English PDF)

Recent Login Activity
Last Successfull Login
01/10/2024 12:37:09
Last Un-Successfull Login
01/10/2024 12:23:40

Training Material