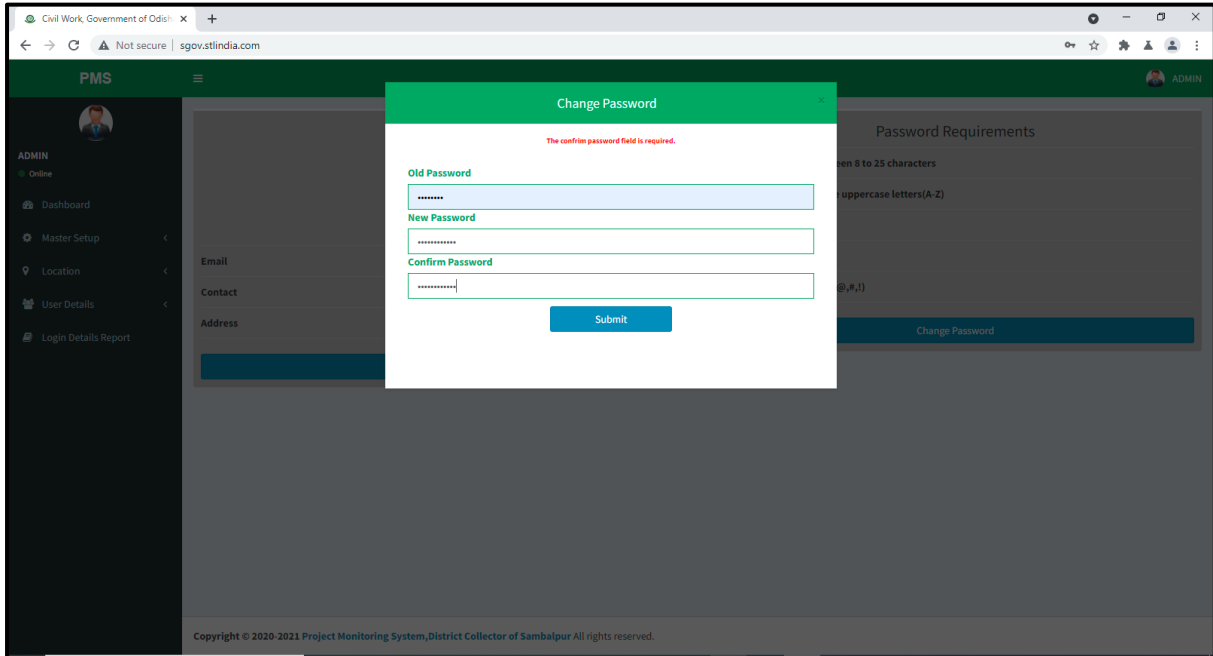
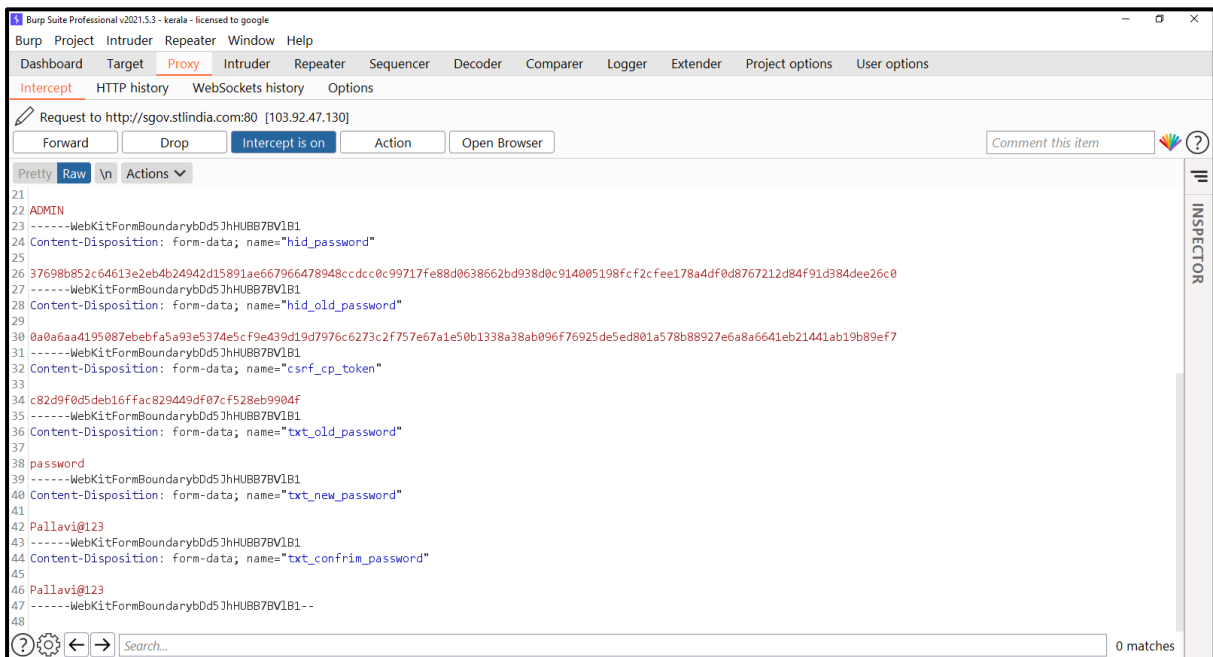


## 1. Insecure Transmission of Password: Open

**Step #1:** A user navigates to the change password page of the application at URL: [http://sgov.stlindia.com/staging1/civil\\_work\\_test/my-account](http://sgov.stlindia.com/staging1/civil_work_test/my-account), enters the credentials and click's the add button as shown below:



**Step #2:** A malicious user present in the same network captures the request using an http interceptor and observes that the application is transmitting the password in the clear text format as shown below:



## 2. Business Rule Bypass:

**Step #1:** A malicious admin user logs into the application and navigates to the **'Add project setup'** page at the URL: [http://sgov.stlindia.com/staging1/civil\\_work\\_test/admin-project-setup](http://sgov.stlindia.com/staging1/civil_work_test/admin-project-setup) then clicks on edit option for updating the add project setup entered all the required fields and commencement date set as the past date and then clicks on **'Update'** button as shown below:

The screenshot shows the 'Add project setup' form in the PMS application. The form is filled with various project details. The 'Completion Date' field is highlighted with a red box and contains the date '27-12-2021'. The 'Update' button is visible at the bottom right of the form.

Block/ULB	Gram Panchayat/Ward	Village
JUJOMURA	KUKUDAPALI	Dumerpali

Project Name: CONS. OF C. C. AT DUMERPALI

Project Type	Sponsored Office	Executing Agency	Financial Year
COMMUNITY CENTER	Planning & Convergenc	BDO Jujomura	216-17

Scheme	Estimation Cost(In Lakhs)	Exp. Date of Completion	Assigned JE/AE
4th SFC	0.800	22-05-2021	CHIRANJIB K NATH, GP

Percentage of Completion	Project Status	Remarks	Case Record No
7.00	Not Approved	NOT STARTED	35677

Sanction Order No	Sanction Order Date	Case Opening Date	Commencement Date
6765332	12-01-2022	12-01-2022	12-01-2022

Completion Date	Latitude	Longitude	UC Status
27-12-2021	6	7	No

Balance UC	Project Handover	Is Functional	Stipulated Date
qwerjty	No	No	29-12-2021

Is Important Project

**Update** **Reset**

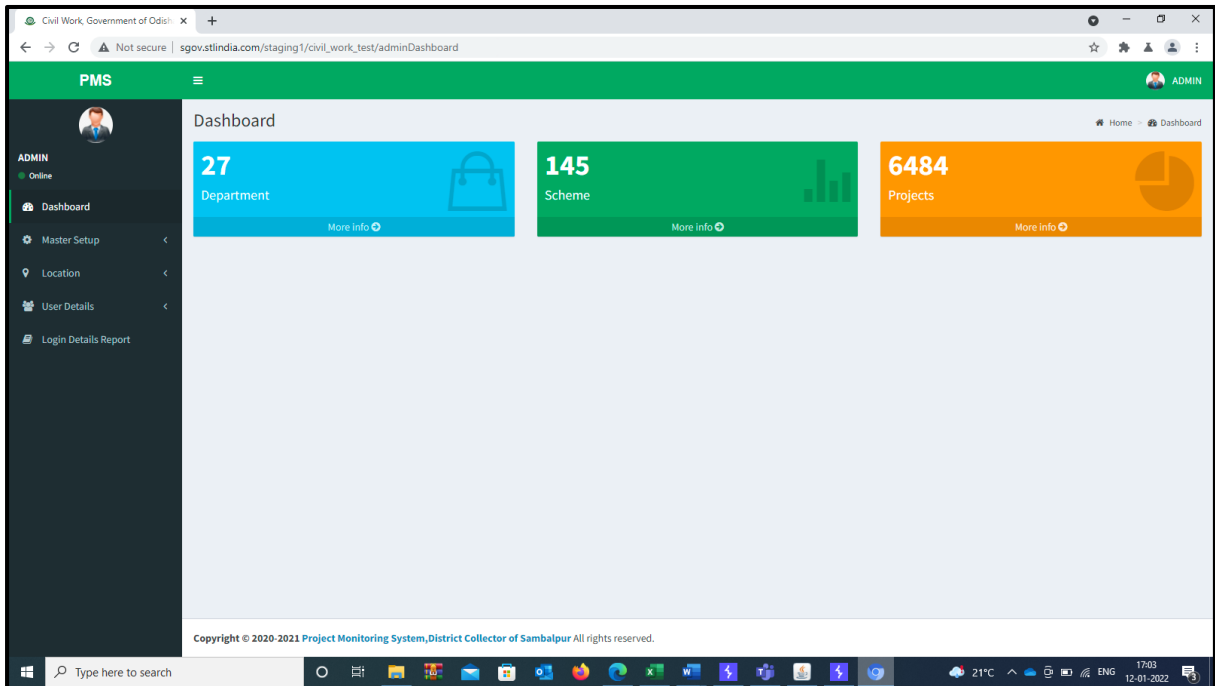
**Step #2:** Data Saved successfully.

The screenshot shows the 'Project Setup' page in the PMS application. A modal dialog box is displayed in the center of the screen with a green checkmark and the text 'Data Operation success'. The 'OK' button is visible at the bottom of the dialog box. The background shows the project setup form and a table of project entries.

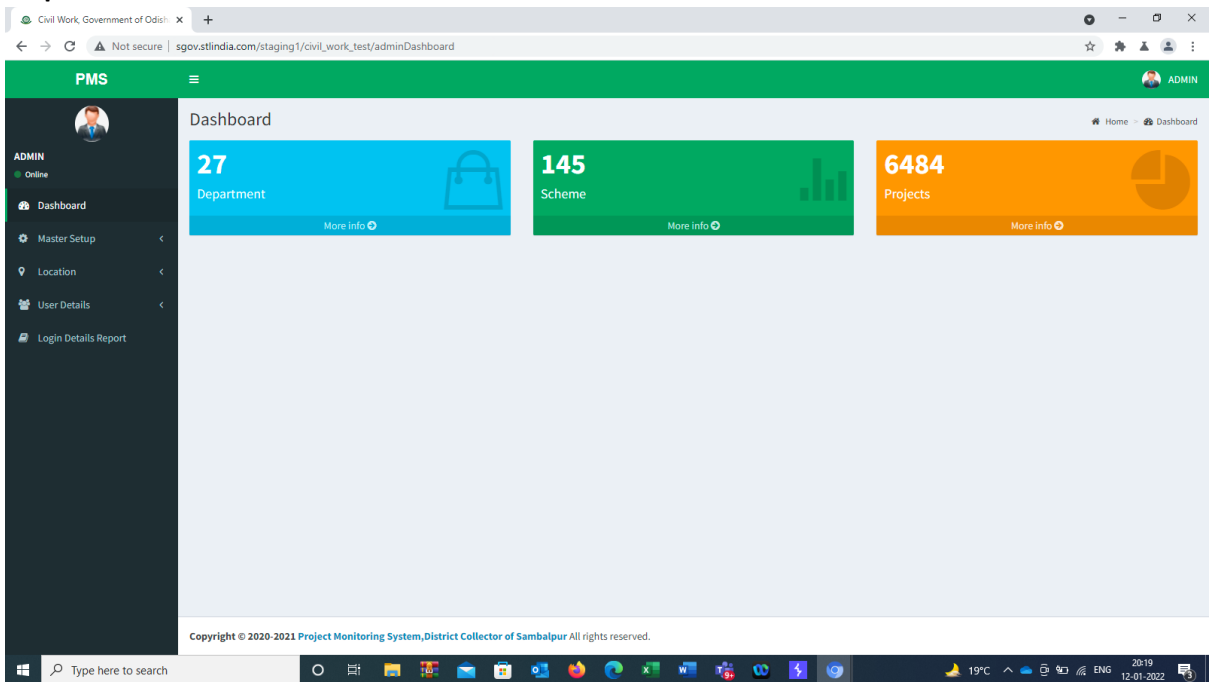
#	Action	Project Status
1		Not Approved
2		Not Started
3		Completed
4		Ongoing Project
5		Completed
6		Not Started
7		Not Started
8		Ongoing Project
9		Ongoing Project

### 3.Improper Session Time Out:

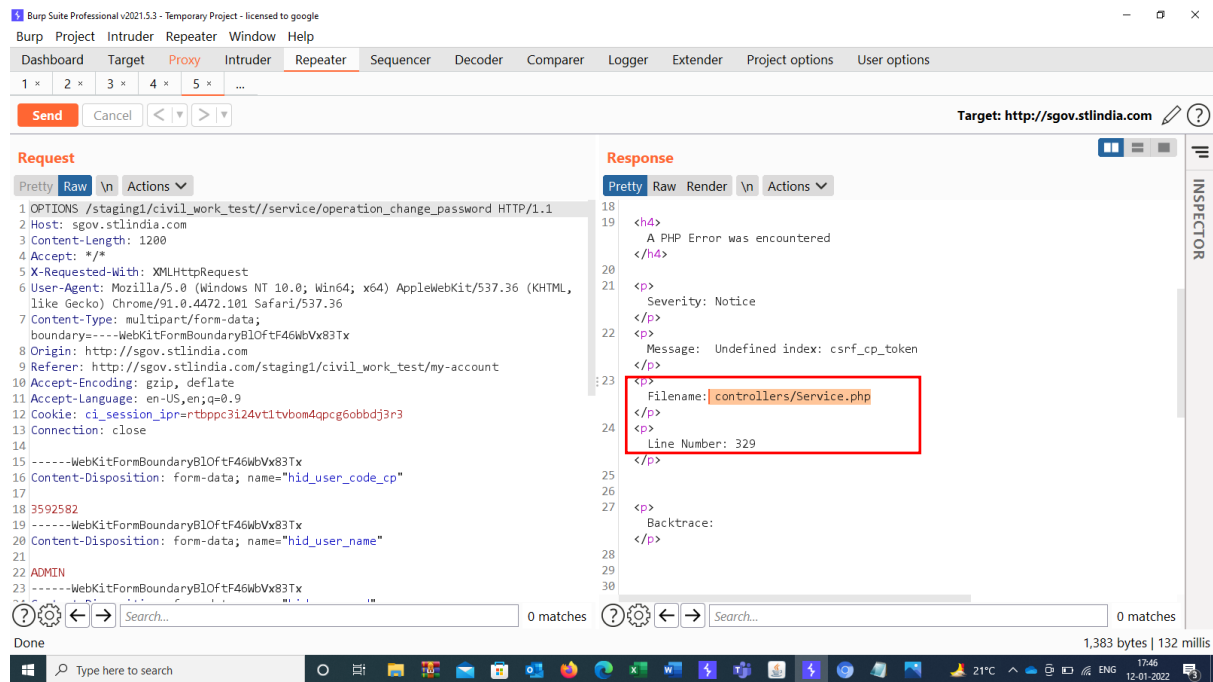
#### Step #1:



#### Step #2:



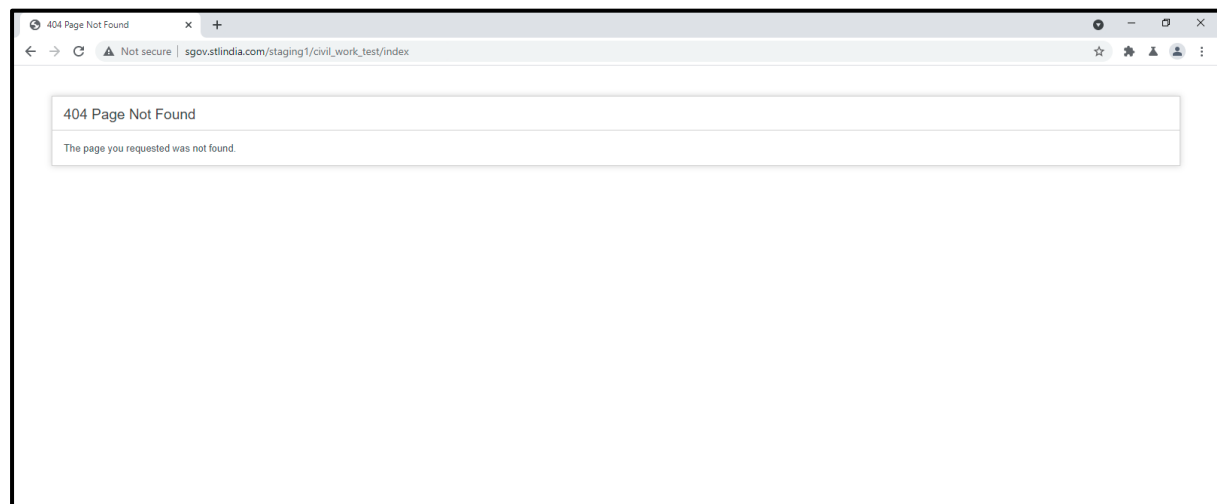
## 4. Improper Error Handling:



The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane on the left displays the raw HTTP request, and the 'Response' pane on the right displays the raw HTTP response. The response contains a PHP error message:

```
18 <h4>
19   A PHP Error was encountered
20 </h4>
21 <p>
22   Severity: Notice
23 </p>
24   Message: Undefined index: csrf_cp_token
25 </p>
26   Filename: controllers/Service.php
27 </p>
28   Line Number: 329
29 </p>
30 <p>
31   Backtrace:
32 </p>
```

The filename 'controllers/Service.php' is highlighted with a red box, indicating a disclosure of internal file paths.



The screenshot shows a web browser window displaying a 404 Page Not Found error. The message reads: "404 Page Not Found. The page you requested was not found." This is a typical response for a missing page, which in this context is a result of the error handling in the application.

## 5. Internal Path Disclosure:

It can be observed that from the error page of the response the '**controllers/Services.php**' is disclosed as shown below:

Burp Suite Professional v2021.5.3 - Temporary Project - licensed to google

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options

1 x 2 x 3 x 4 x 5 x ...

Send Cancel < >

Target: http://sgov.stlindia.com

### Request

```

1 OPTIONS /staging1/civil_work_test//service/operation_change_password HTTP/1.1
2 Host: sgov.stlindia.com
3 Content-Length: 1200
4 Accept: */*
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/91.0.4472.101 Safari/537.36
7 Content-Type: multipart/form-data;
  boundary=---WebKitFormBoundaryB1OfTf46WbVx83Tx
8 Origin: http://sgov.stlindia.com
9 Referer: http://sgov.stlindia.com/staging1/civil_work_test/my-account
10 Accept-Encoding: gzip, deflate
11 Accept-Language: en-US,en;q=0.9
12 Cookie: ci_session_ipr=rtbpc3i24vtltvbom4apcg6obbdj3r3
13 Connection: close
14
15 -----WebKitFormBoundaryB1OfTf46WbVx83Tx
16 Content-Disposition: form-data; name="hid_user_code_cp"
17
18 3592582
19 -----WebKitFormBoundaryB1OfTf46WbVx83Tx
20 Content-Disposition: form-data; name="hid_user_name"
21
22 ADMIN
23 -----WebKitFormBoundaryB1OfTf46WbVx83Tx

```

### Response

```

18 <h4>
19 A PHP Error was encountered
20 </h4>
21 <p>
22 Severity: Notice
23 </p>
24 <p>
25 Message: Undefined index: csrf_cp_token
26 </p>
27 <p>
28 Filename: controllers/Service.php
29 </p>
30 <p>
31 Line Number: 329
32 </p>
33 <p>
34 Backtrace:
35 </p>

```

Done 1,383 bytes | 132 millis

Burp Suite Professional v2021.5.3 - Temporary Project - licensed to google

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options

1 x 2 x 3 x 4 x ...

Send Cancel < >

Target: http://sgov.stlindia.com

### Request

```

1 POST /staging1/civil_work_test/service/default HTTP/1.1
2 Host: sgov.stlindia.com
3 Content-Length: 619
4 Accept: */*
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/91.0.4472.101 Safari/537.36
7 Content-Type: multipart/form-data;
  boundary=---WebKitFormBoundarylpEGTEoQ7ALXydTL
8 Origin: http://sgov.stlindia.com
9 Referer: http://sgov.stlindia.com/staging1/civil_work_test/financial-year
10 Accept-Encoding: gzip, deflate
11 Accept-Language: en-US,en;q=0.9
12 Cookie: ci_session_ipr=k4udsufcj05pd9h0vb71rfdl8soslr
13 Connection: close
14
15 -----WebKitFormBoundarylpEGTEoQ7ALXydTL
16 Content-Disposition: form-data; name="op_type"
17
18 edit_Financial_master
19 -----WebKitFormBoundarylpEGTEoQ7ALXydTL
20 Content-Disposition: form-data; name="csrf_op_financial_token"
21
22 7fc32fe5d9a32b5712bbd47ffabd18473231821c
23 -----WebKitFormBoundarylpEGTEoQ7ALXydTL

```

### Response

```

17
18
19 aught Exception was encountered
20
21 Error
22
23 e: Call to undefined method Service::default()
24
25
26
27 me: /var/www/html/staging1/civil_work_test/application/controllers/Service.php
28
29
30 umber: 17
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

```

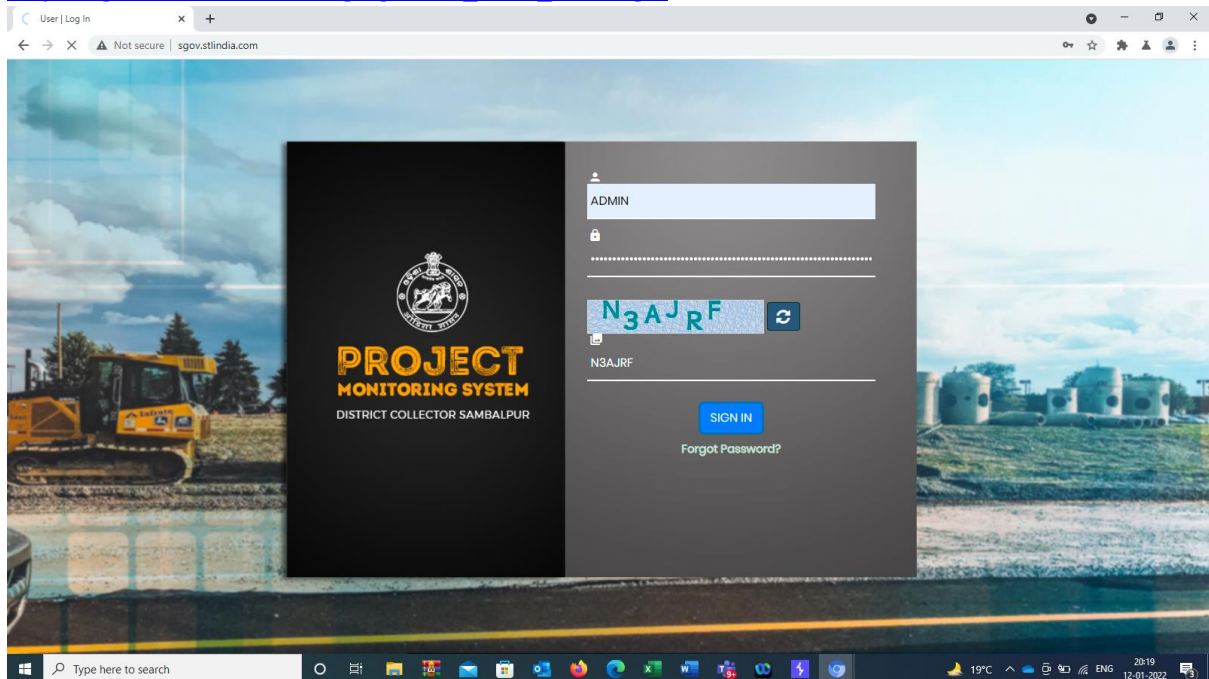
Done 1,009 bytes | 116 millis

## 6. Session Fixation: Open

Pre and Post Session ID are Same.

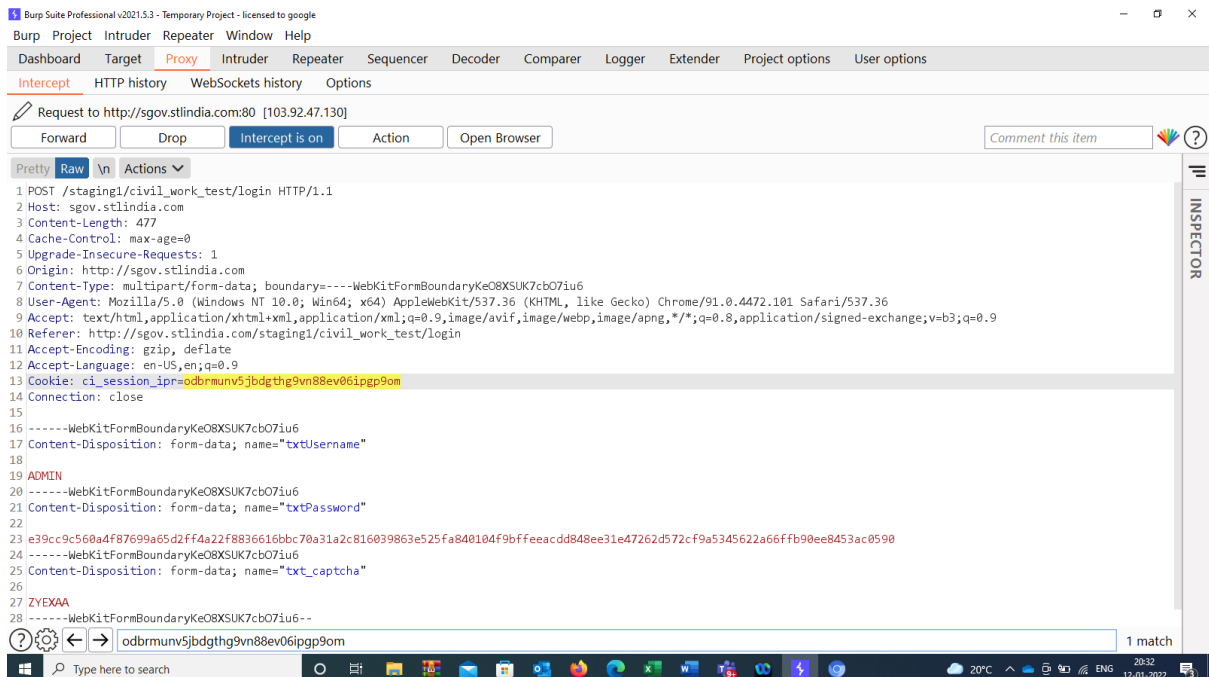
**Step #1:** An attacker navigates to the application login page at the URL:

[http://sgov.stlindia.com/staging1/civil\\_work\\_test/login](http://sgov.stlindia.com/staging1/civil_work_test/login) and refresh the URL as shown below:

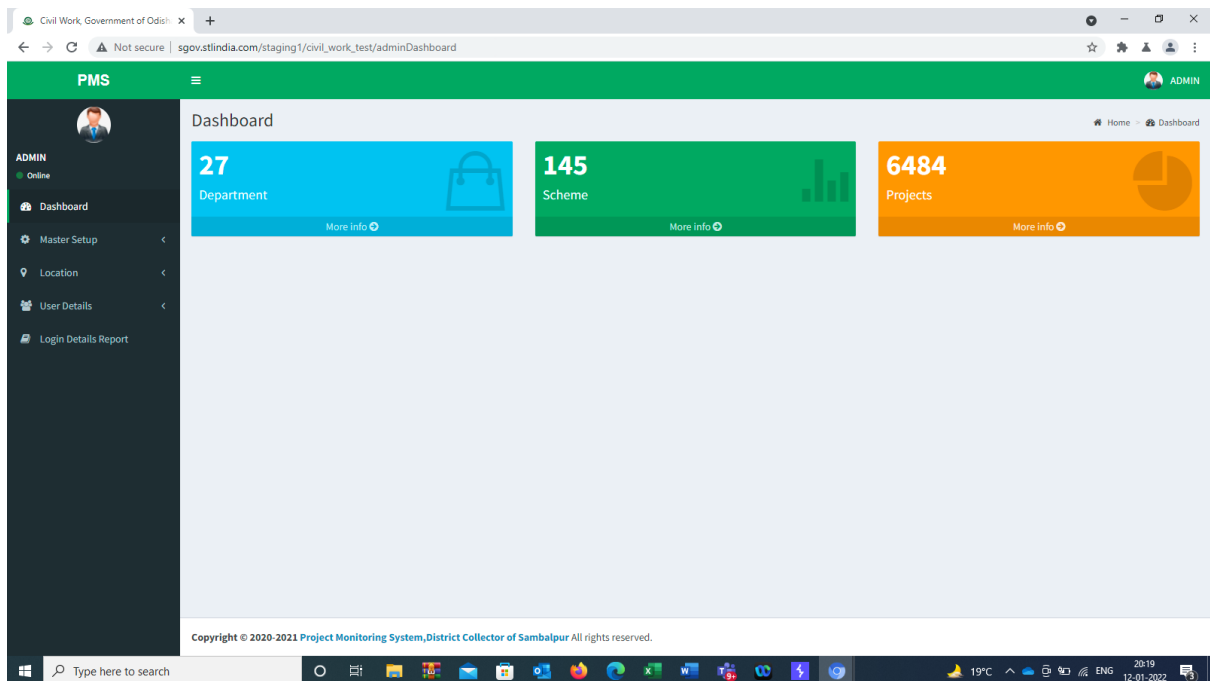


The login page is refreshed, and the request is captured in an HTTP interceptor. The attacker copies the pre-authenticated session-id as shown below.

Pre Session ID

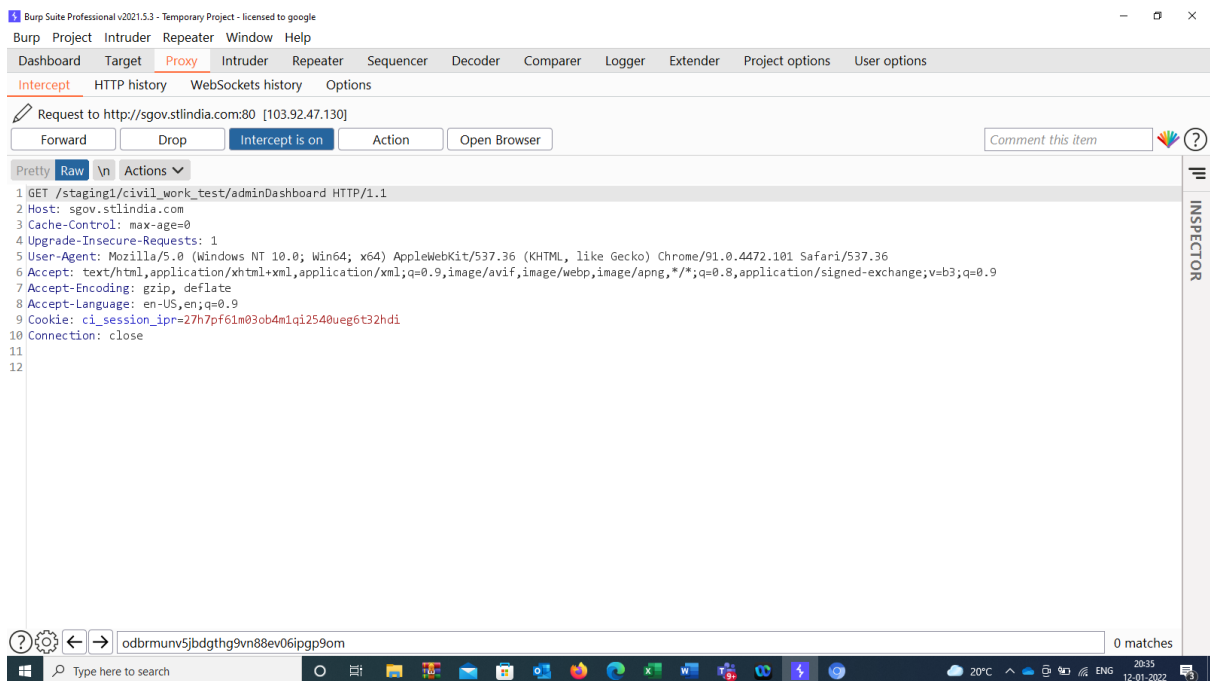


Then the victim navigates to the internal page as shown below:

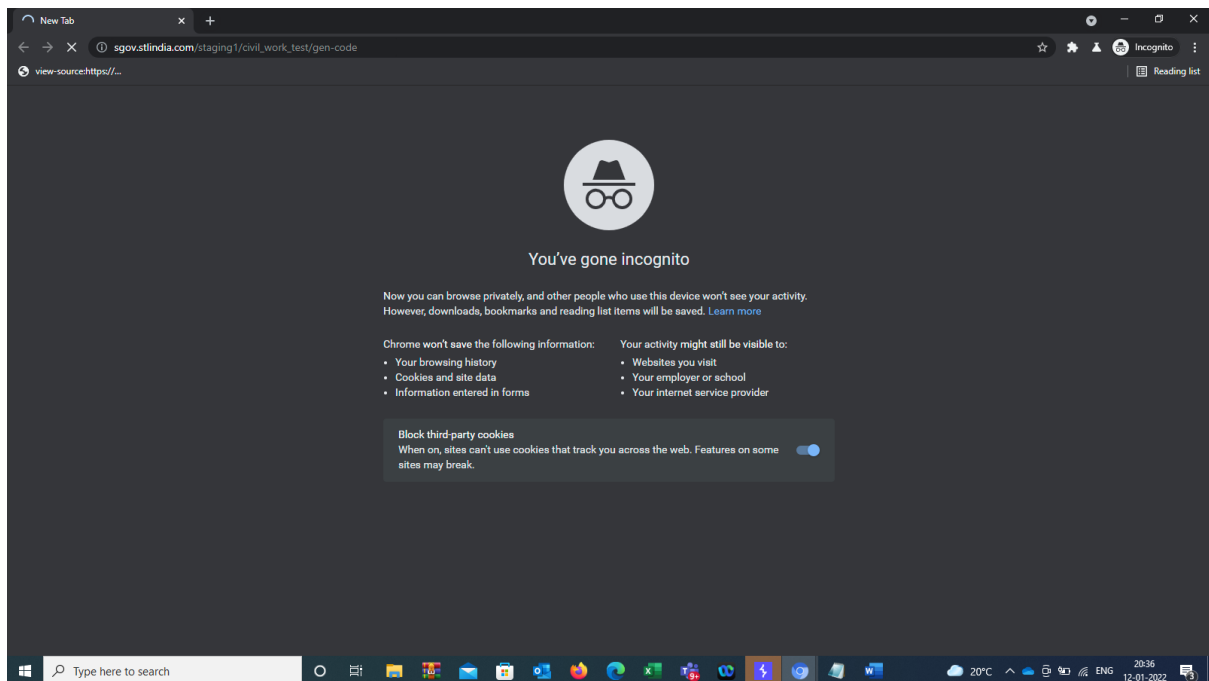


: Attacker capture the request and observed that same Session id is travelling in the request as shown below:

Post Session ID

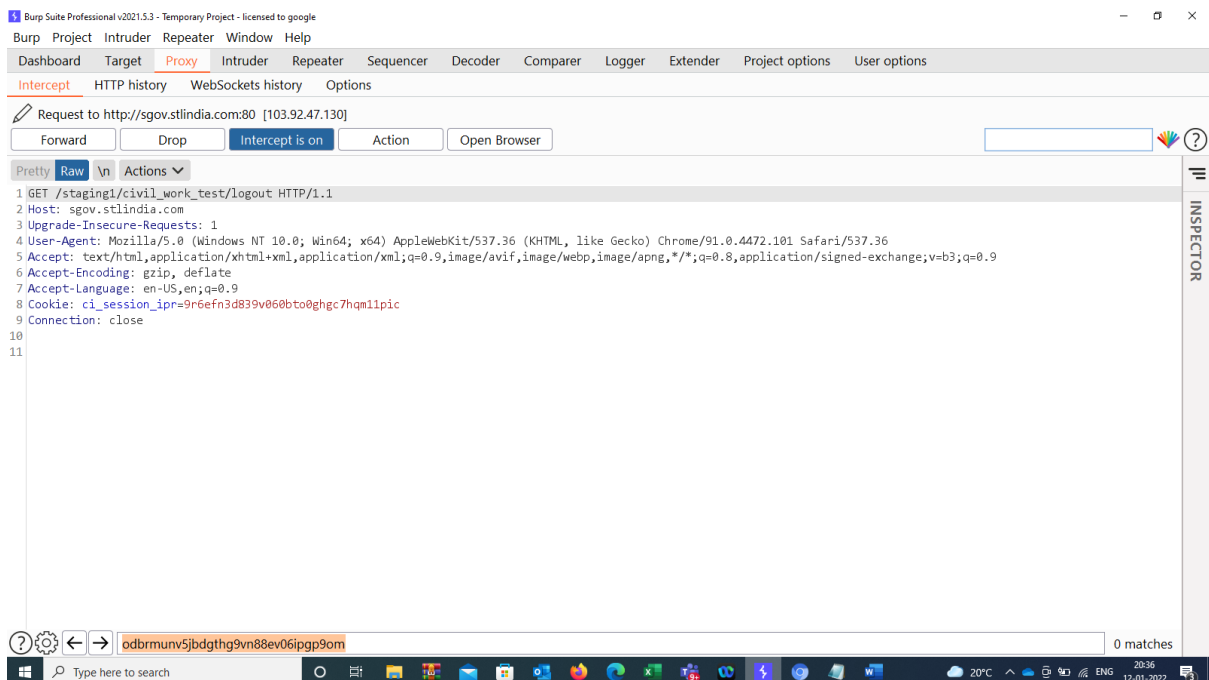


At the same time, the attacker navigates to the application login page from incognito browser as shown below.



The login page is refreshed, and the request is captured in an HTTP interceptor.

**Original Request:** The request contains the new session-id and the URL (indexpage.jsp) for the login page as shown below.



Modified request with session ID



Request to http://sgov.stlindia.com:80 [103.92.47.130]  
Forward Drop Intercept is on Action Open Browser Comment this item

```
1 GET /staging1/civil_work_test/logout HTTP/1.1
2 Host: sgov.stlindia.com
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.101 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: ci_session_ipr=odbrmunv5jbdgthg9vn88ev06ipgp9om
9 Connection: close
10
11
```

```
odbrmunv5jbdgthg9vn88ev06ipgp9om
odbrmunv5jbdgthg9vn88ev06ipgp9om
```