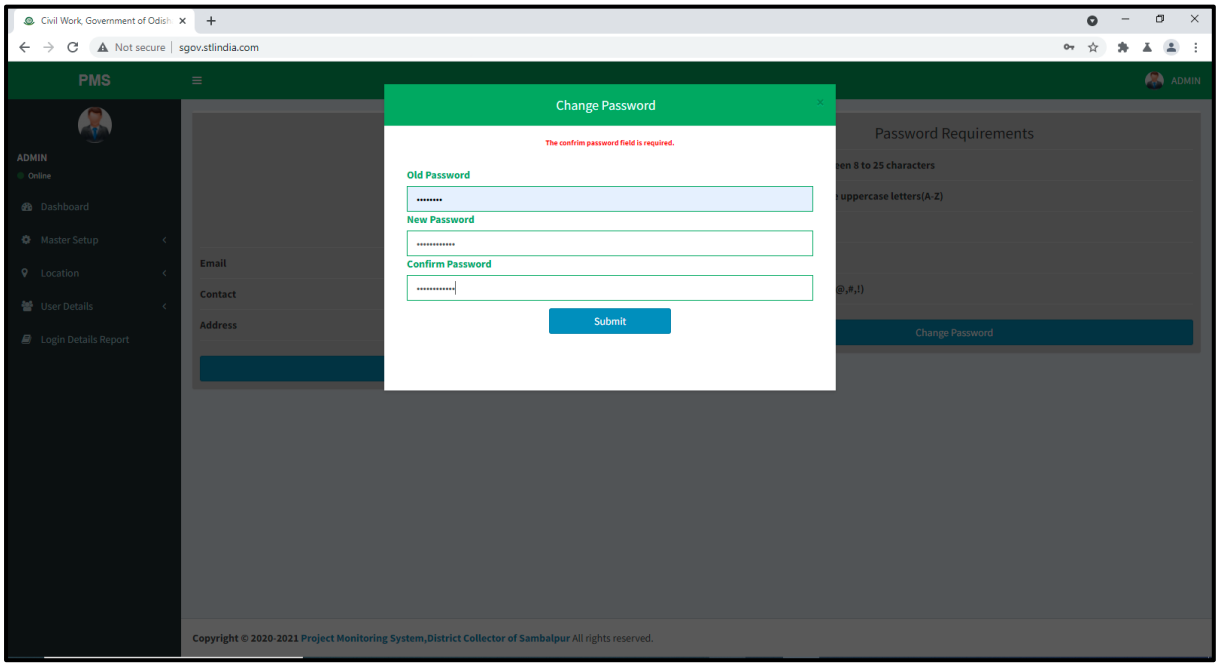
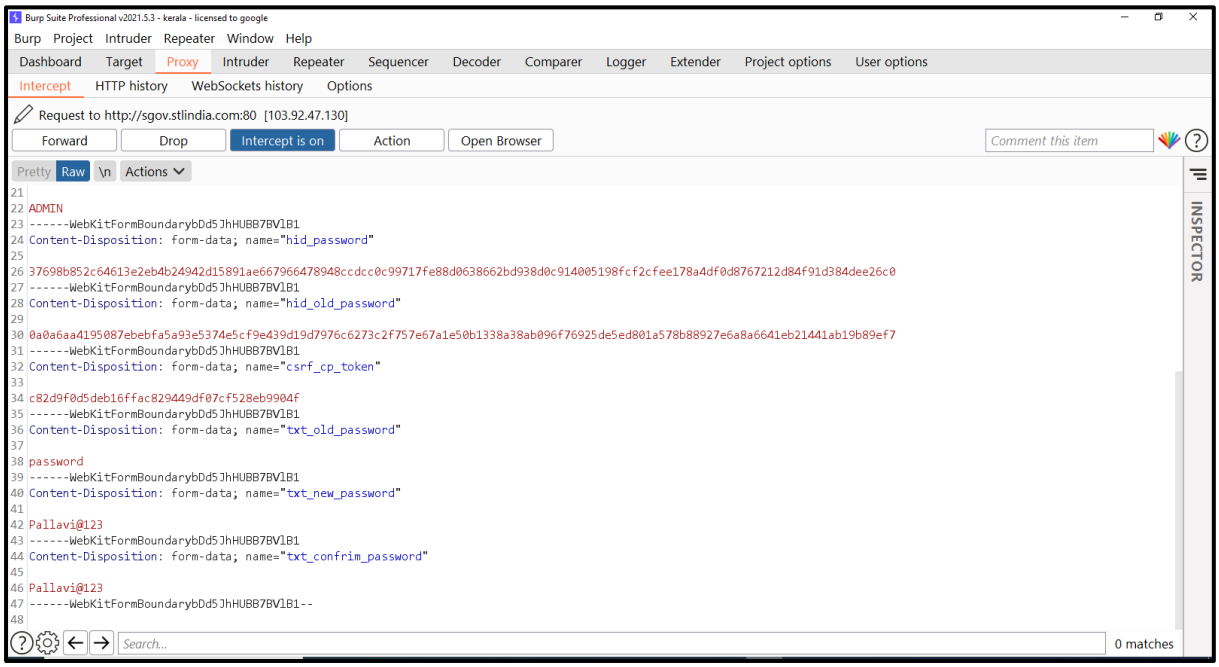
1. Insecure Transmission of Password: Open

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 **,**enters the credentials and click's the add button as shown below:

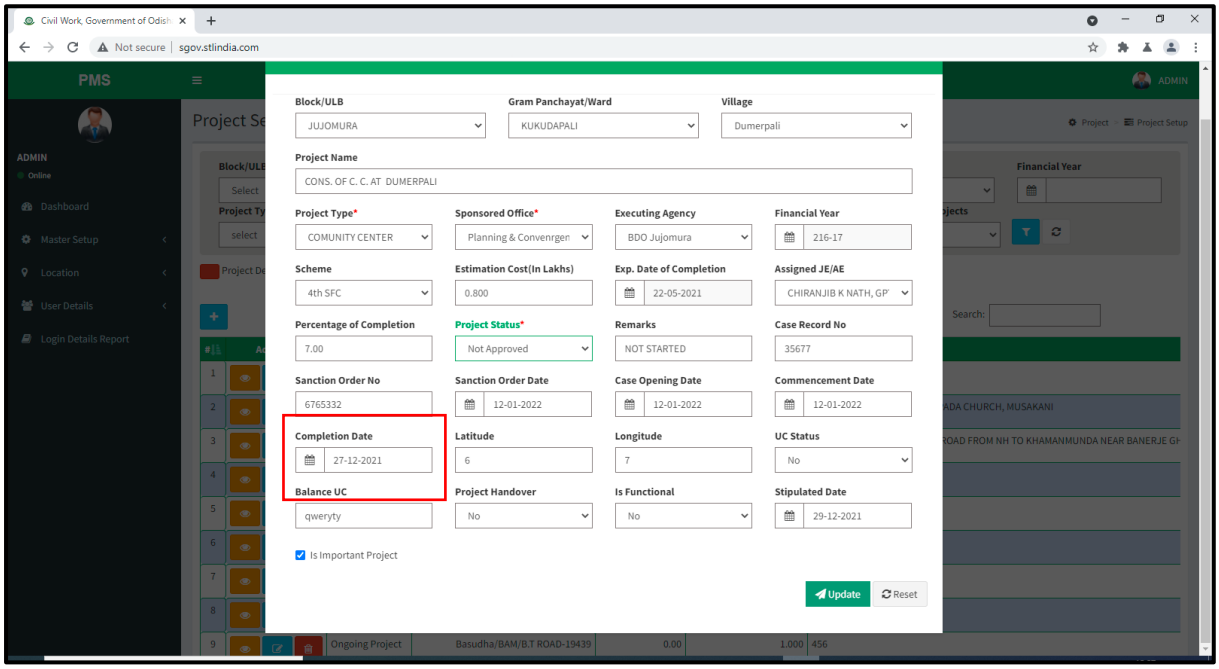


Step #2: A malicious user present in the same network captures the request using an http interceptor and observes that the application is transmitting the password in the clear text format as shown below:

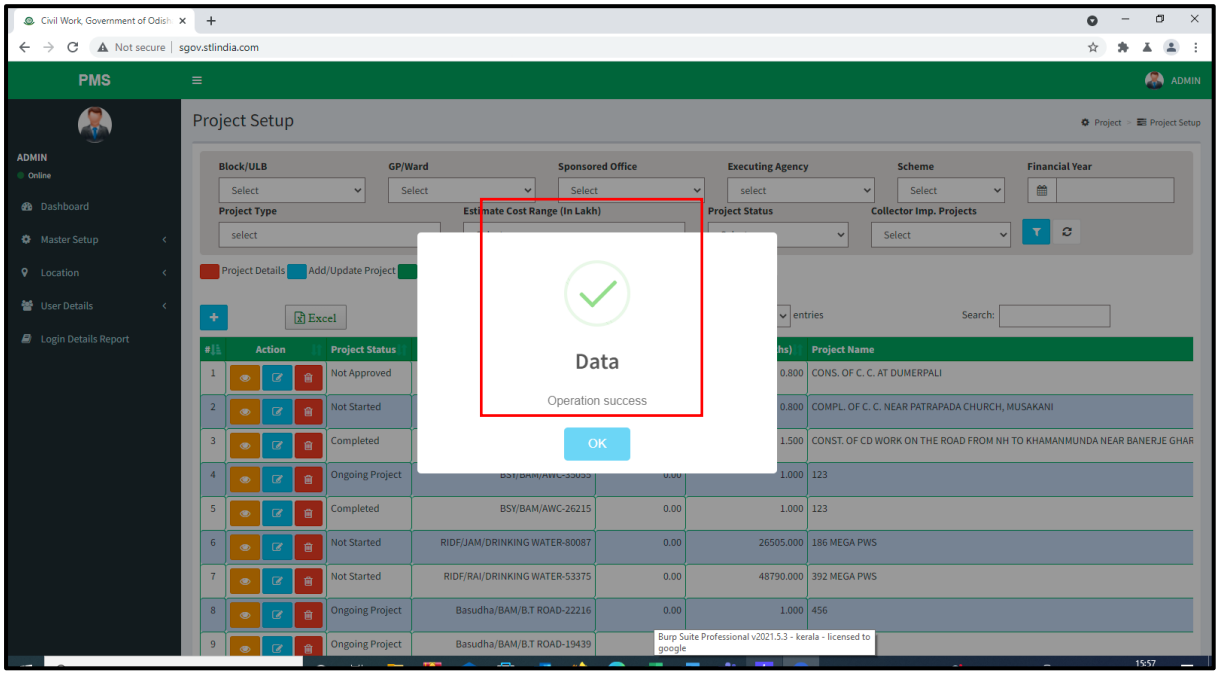


2.Business Rule Bypass:

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 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:

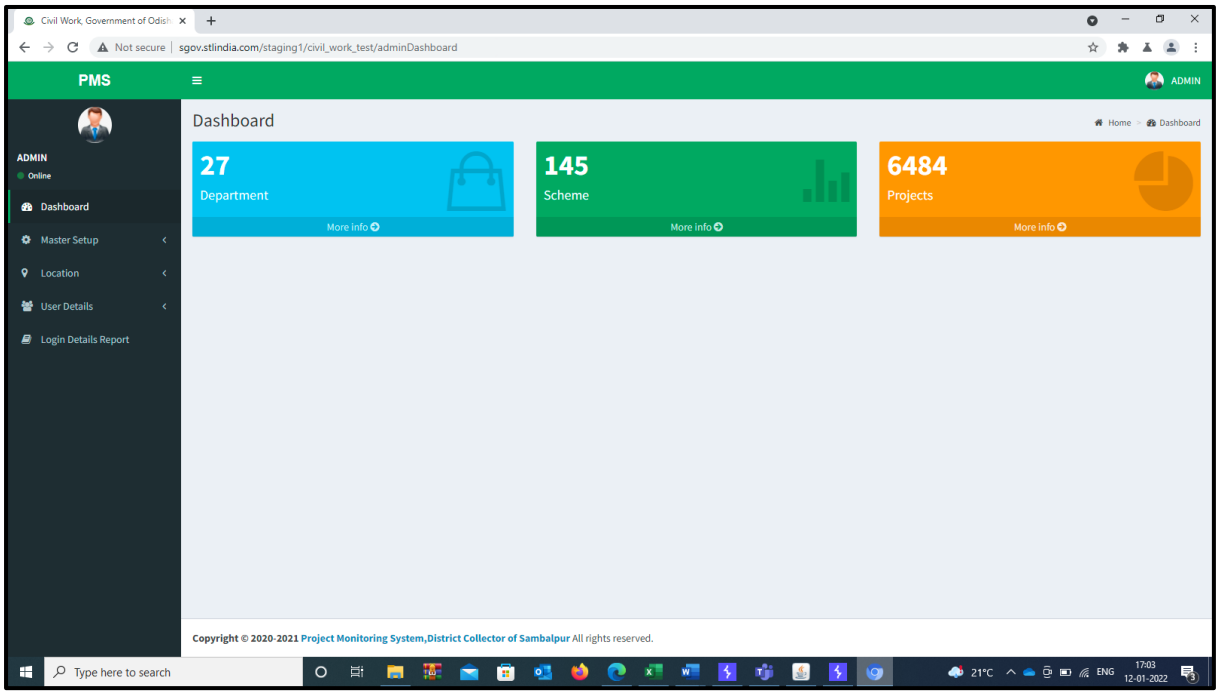


Step #2: Data Saved successfully.

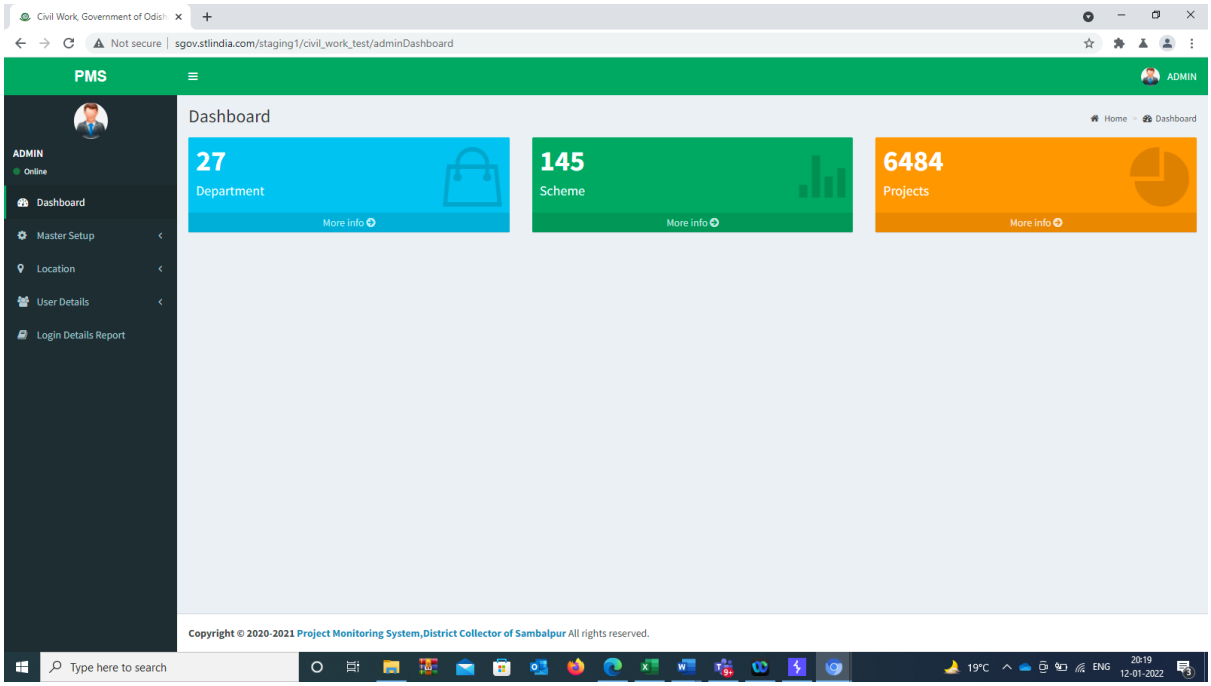


3.Improper Session Time Out:

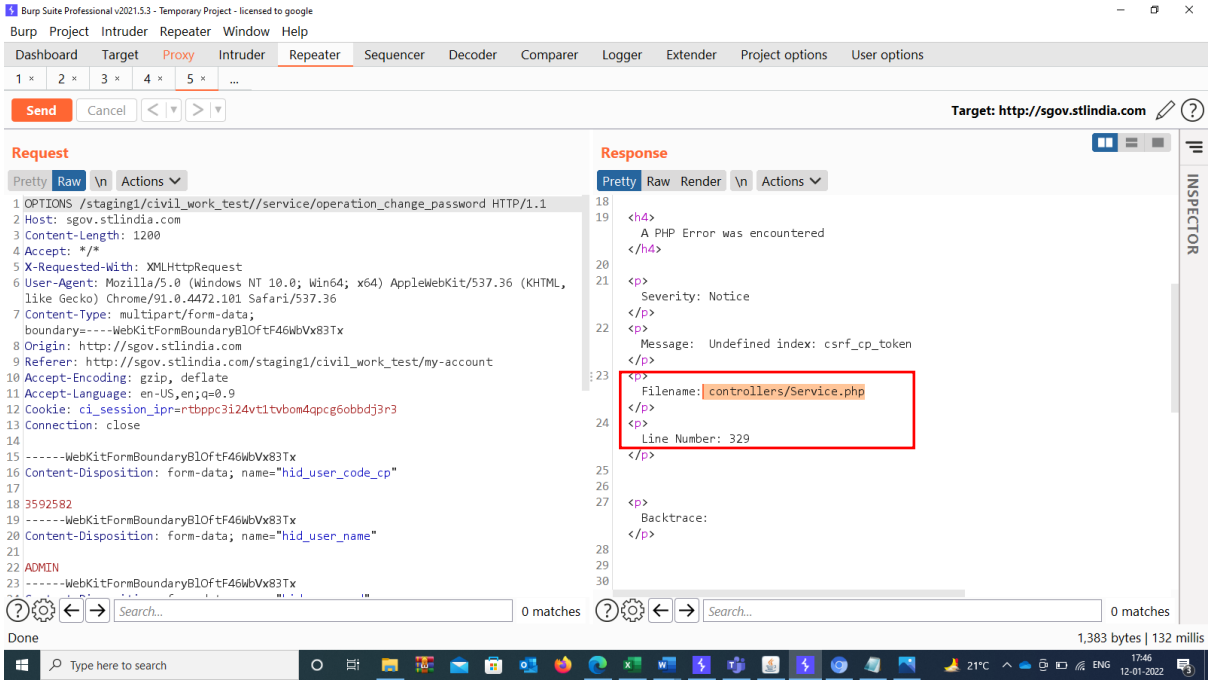
Step #1:

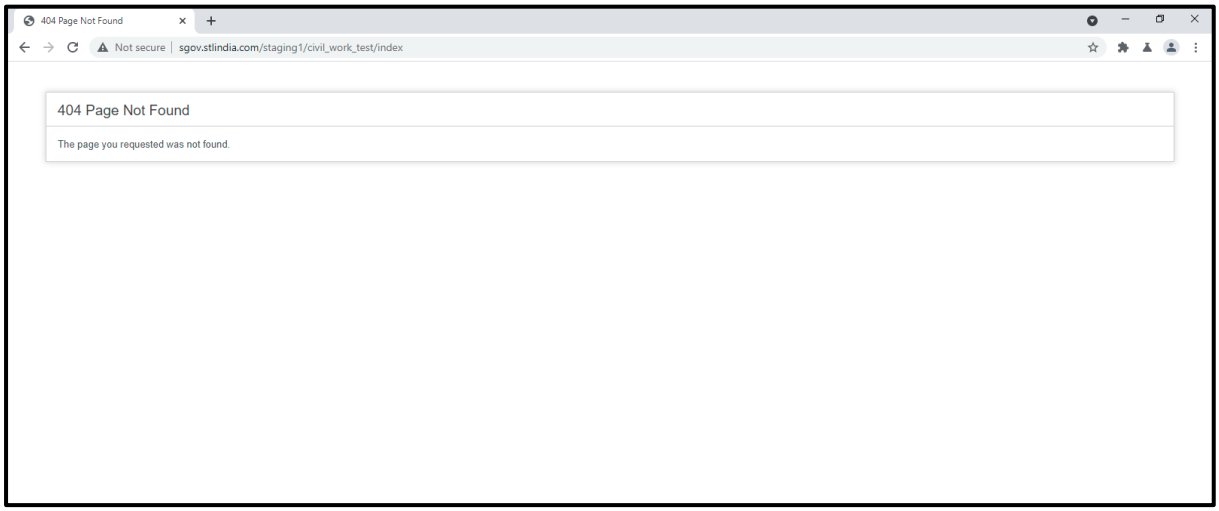


Step #2:



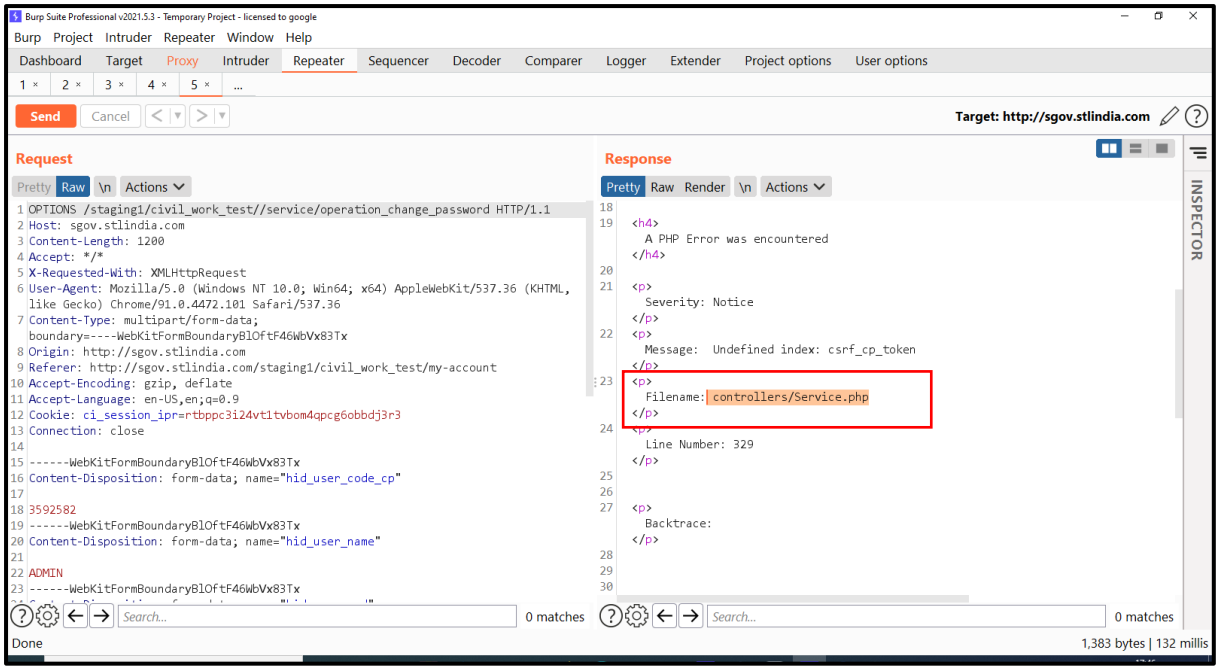
4. Improper Erroe Handling:

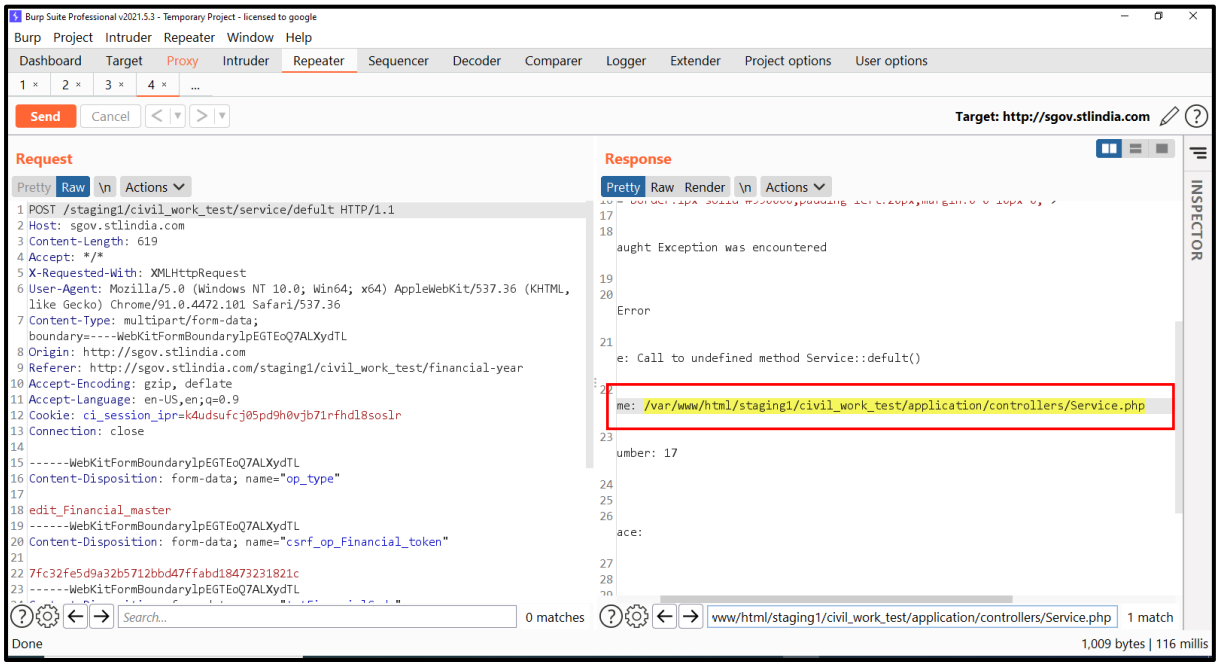




5. Internal Path Disclosure:

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

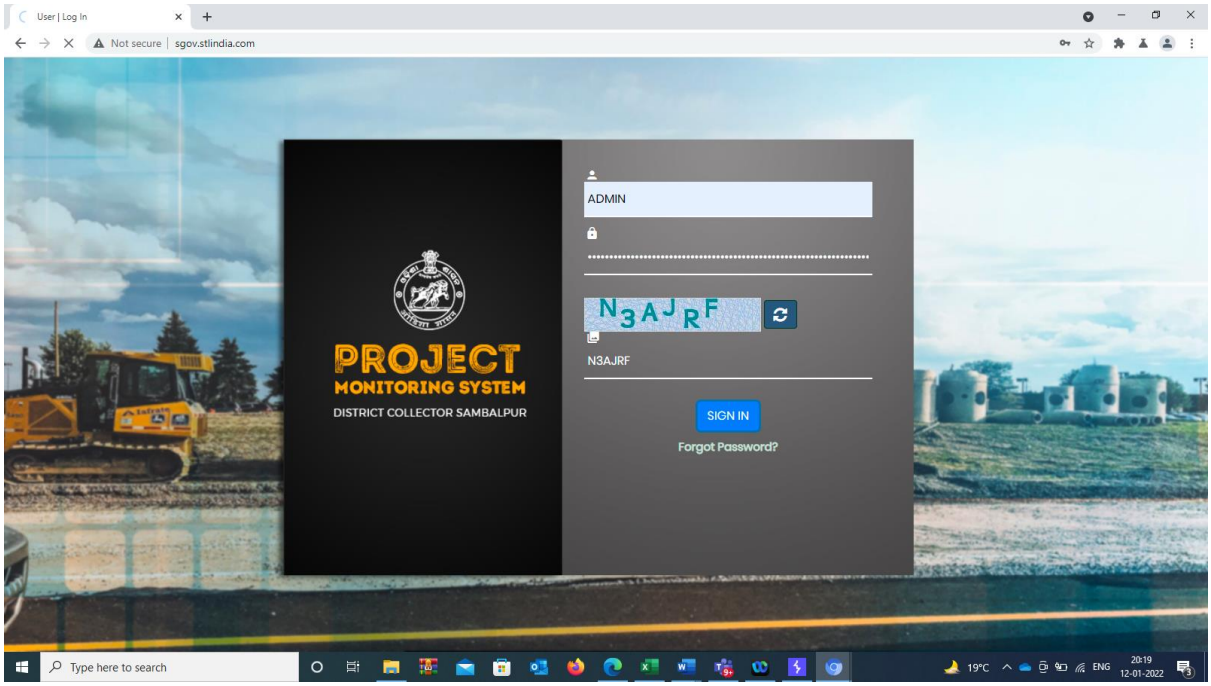

Burp Suite Professional v2021.5.3 - Temporary Project - licensed to google
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Send Cancel
Target: http://sgov.stlindia.com
Request
Pretty Raw \n Actions
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=----WebKitFormBoundaryBlOftF46WbVx83Tx
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=rtbppc3i24vt1tvbom4qpcg6obbdj3r3
13 Connection: close
15 ------WebKitFormBoundaryBlOftF46WbVx83Tx
16 Content-Disposition: form-data; name="hid_user_code_cp"
18 3592582
19 ------WebKitFormBoundaryBlOftF46WbVx83Tx
20 Content-Disposition: form-data; name="hid_user_name"
22 ADMIN
23 ------WebKitFormBoundaryBlOftF46WbVx83Tx
Response
Pretty Raw Render \n Actions
<h4> A PHP Error was encountered </h4>
 Severity: Notice
 Message: Undefined index: csrf_cp_token
 Filename: controllers/Service.php
 Line Number: 329
 Backtrace:
Search... 0 matches
Done
1,383 bytes | 132 millis
INSPECTOR


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
Send Cancel
Target: http://sgov.stlindia.com
Request
Pretty Raw \n Actions
1 POST /staging1/civil_work_test/service/defult 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=k4udsufcj05pd9h0vjb71rfhdl8soslr
13 Connection: close
15 ------WebKitFormBoundarylpEGTEoQ7ALXydTL
16 Content-Disposition: form-data; name="op_type"
18 edit_Financial_master
19 ------WebKitFormBoundarylpEGTEoQ7ALXydTL
20 Content-Disposition: form-data; name="csrf_op_Financial_token"
22 7fc32fe5d9a32b5712bbd47ffabd18473231821c
23 ------WebKitFormBoundarylpEGTEoQ7ALXydTL
Response
Pretty Raw Render \n Actions
aught Exception was encountered
Error
e: Call to undefined method Service::defult()
me: /var/www/html/staging1/civil_work_test/application/controllers/Service.php
umber: 17
ace:
Search... 0 matches
ww/html/staging1/civil_work_test/application/controllers/Service.php 1 match
Done
1,009 bytes | 116 millis
INSPECTOR

6. Session Fixation: Open

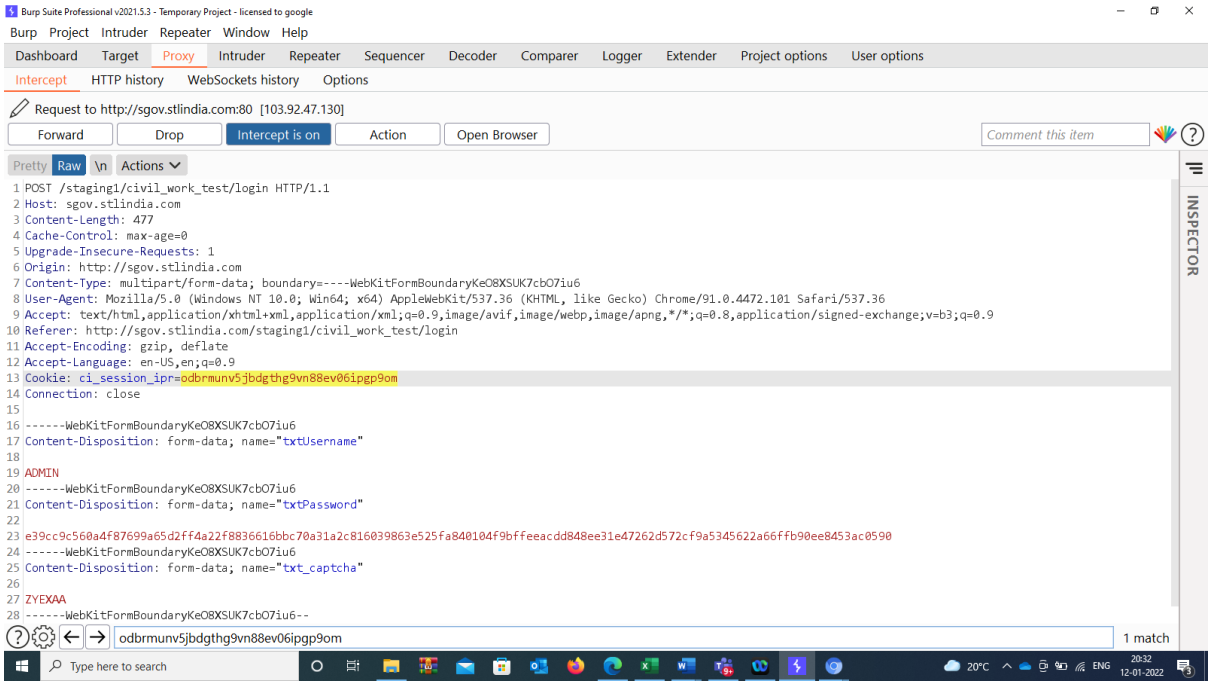
Pre and Post Session ID are Same.

Step #1: An attacker navigates to the application login page at the URL: http://sgov.stlindia.com/staging1/civil_work_test/login and refresh the URL as shown below:

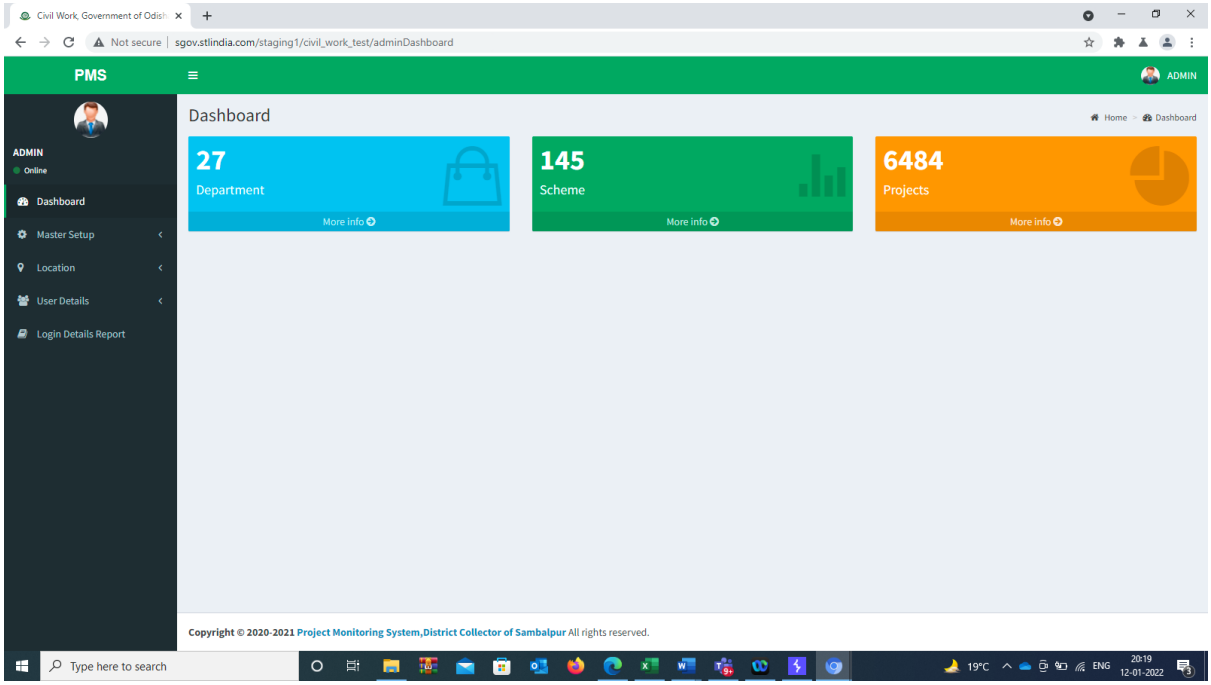


The login page is refreshed, and the request is captured in an HTTP interceptor. The attacker copies the pre-authenticated session-id as shown below.

Pre Session ID

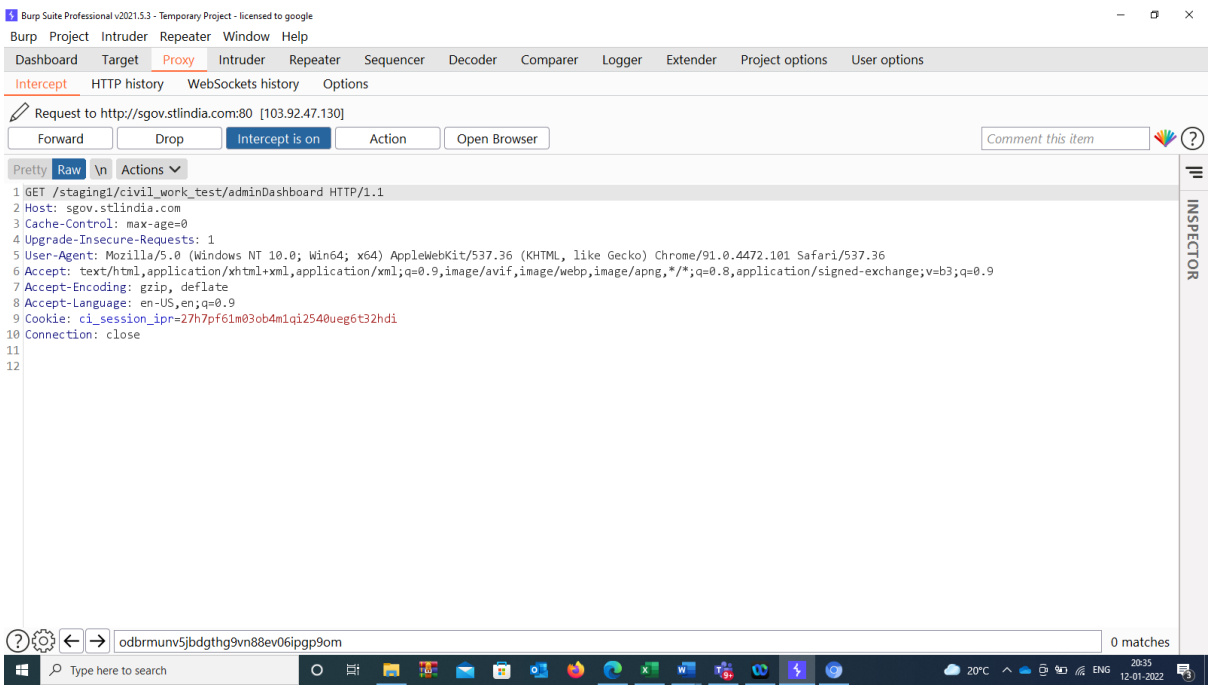


Then the victim navigates to the internal page as shown below:

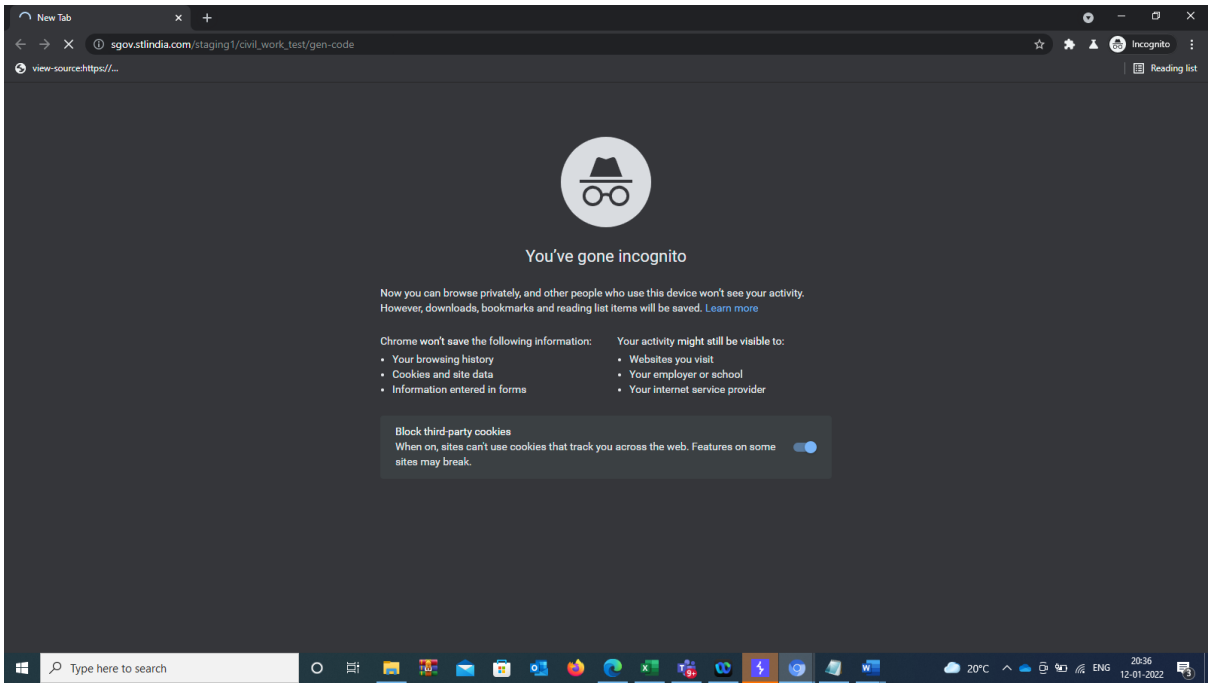


: Attacker capture the request and observed that same Session iD is travelling in the request as shown below:

Post Session ID

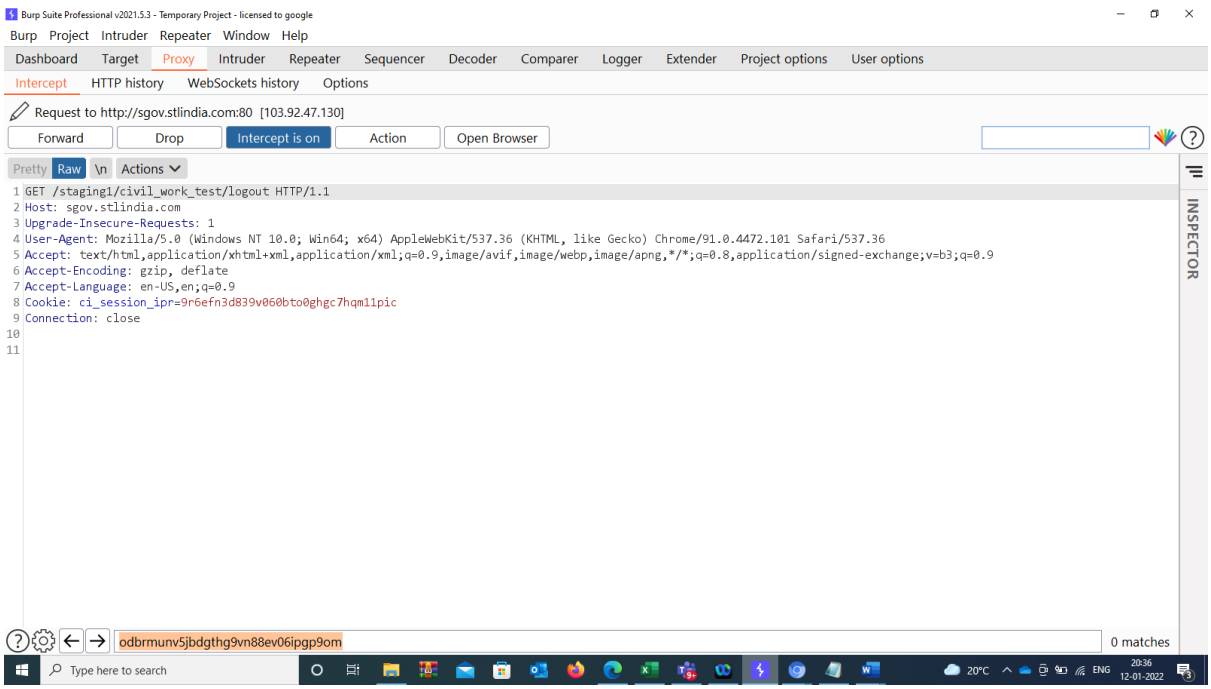


At the same time, the attacker navigates to the application login page from incognito browser as shown below.

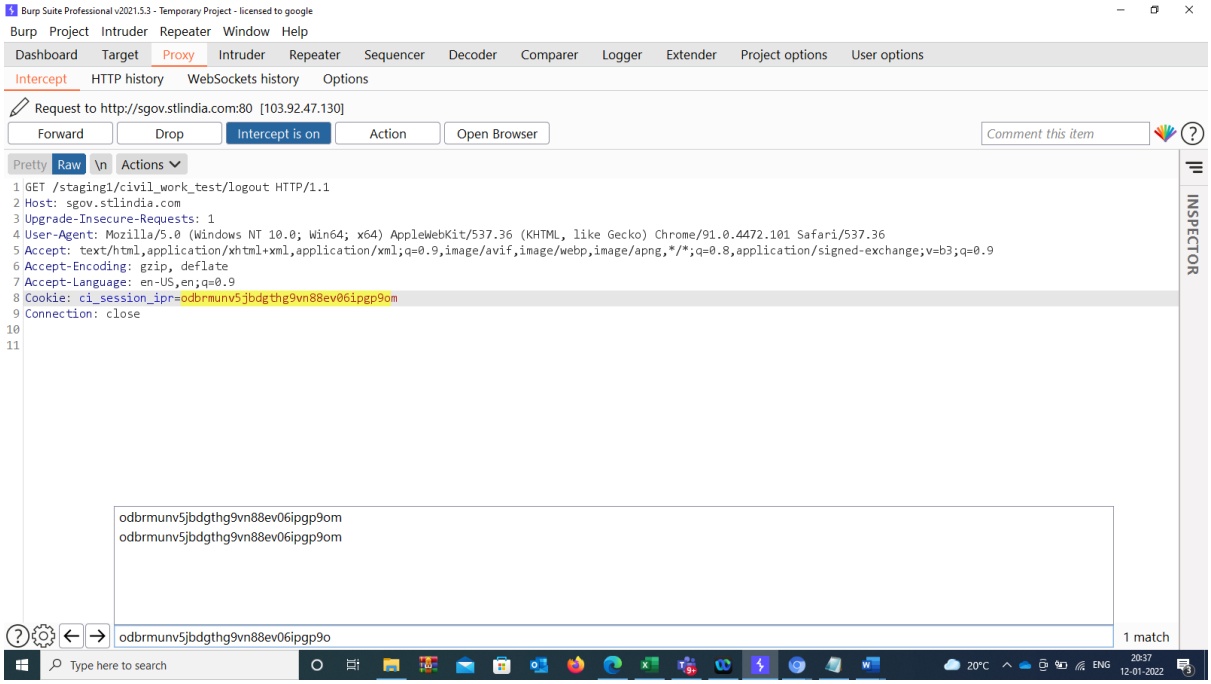


The login page is refreshed, and the request is captured in an HTTP interceptor.

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


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
Intercept HTTP history WebSockets history Options
Request to http://sgov.stlindia.com:80 [103.92.47.130]
Forward Drop Intercept is on Action Open Browser
Comment this item
Pretty Raw \n Actions
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
INSPECTOR
odbrmunv5jbdgthg9vn88ev06ipgp9om
odbrmunv5jbdgthg9vn88ev06ipgp9om
odbrmunv5jbdgthg9vn88ev06ipgp9o
1 match
Type here to search
20°C
ENG
20:37
12-01-2022