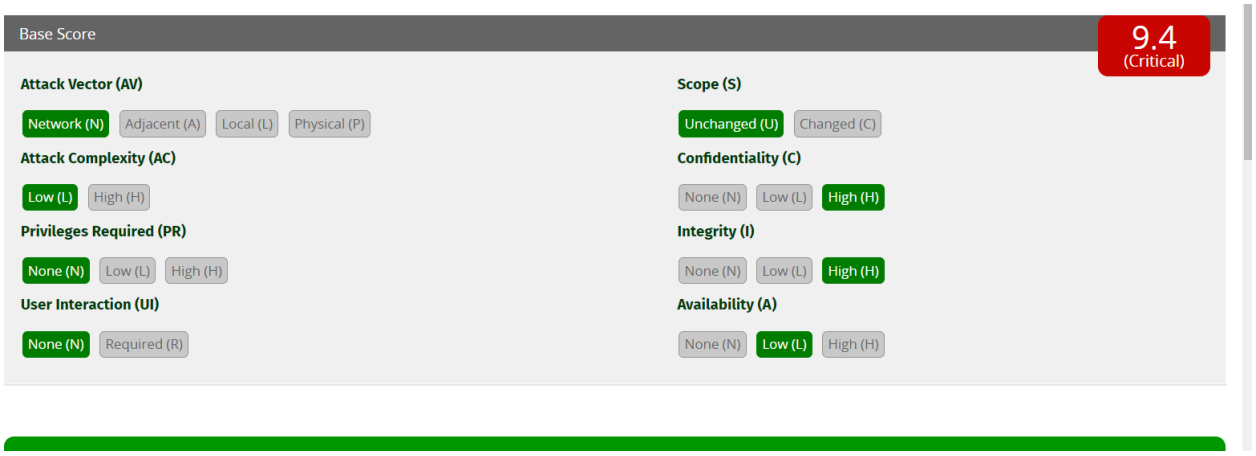
Task 10

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.

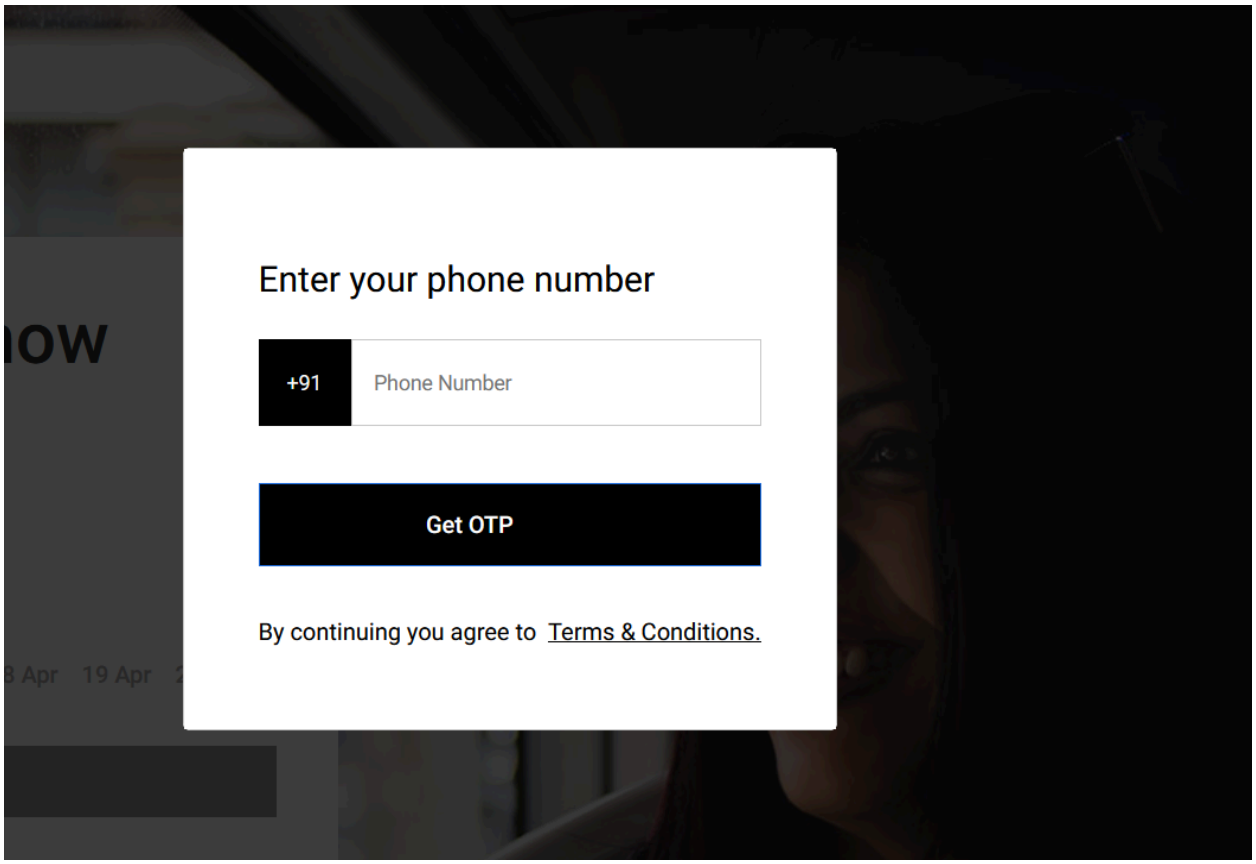
Detailed Explanation:
Upon investigation, it was discovered that yolobus does not enforce rate limiting measures on OTP generation attempts. This oversight enables attackers to repeatedly submit OTP requests, attempting to guess valid OTPs through brute-force attacks. Without rate limiting, attackers 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:

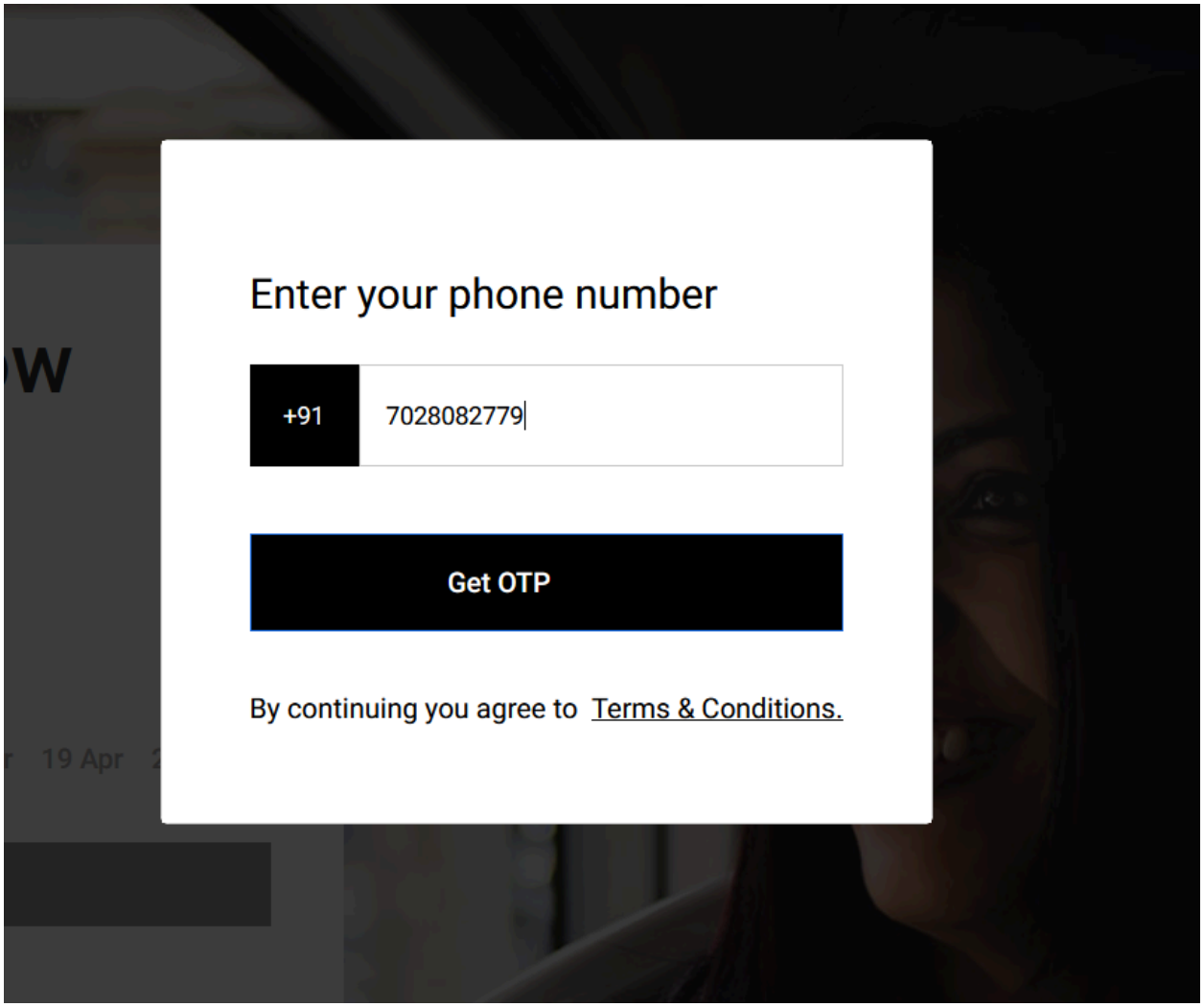
Account Takeover: Attackers can exploit the lack of rate limiting to perform brute-force attacks on OTPs, eventually gaining unauthorized access to user accounts.
Data Theft: Compromised accounts may contain sensitive information such as personal data, financial details, or confidential documents, which 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

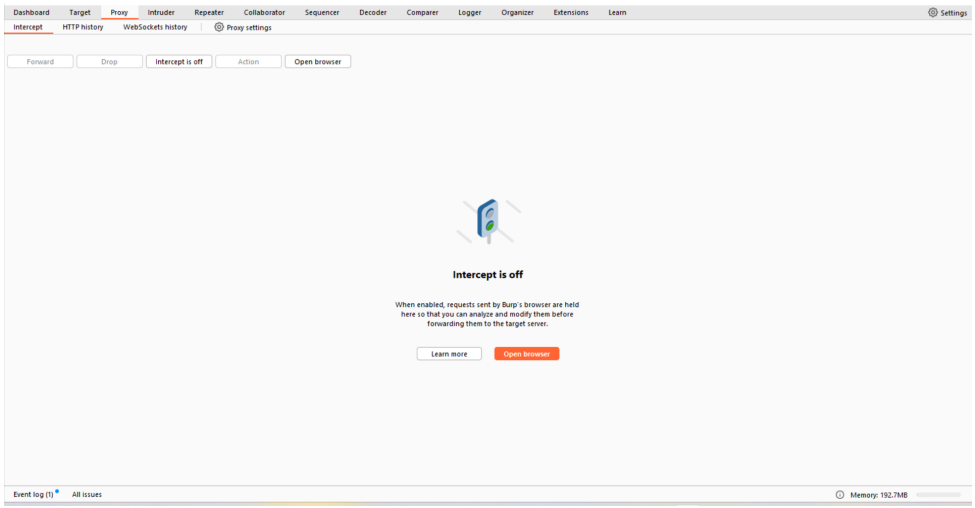
Step 1 : Go the Website and go to the login page of that website that has otp login
https://yolobus.in/



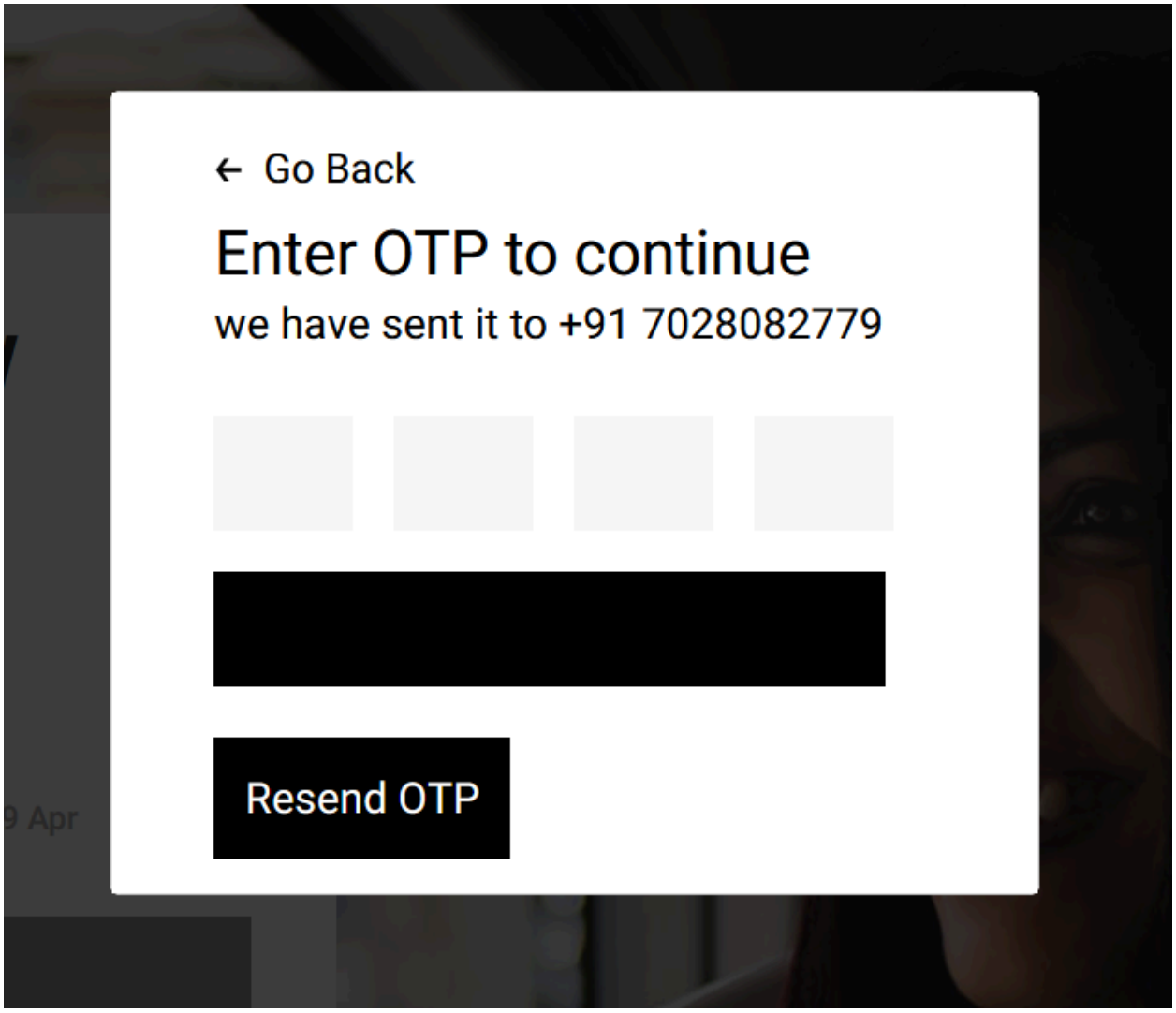
Step 2 : Enter your Number and click on send otp button



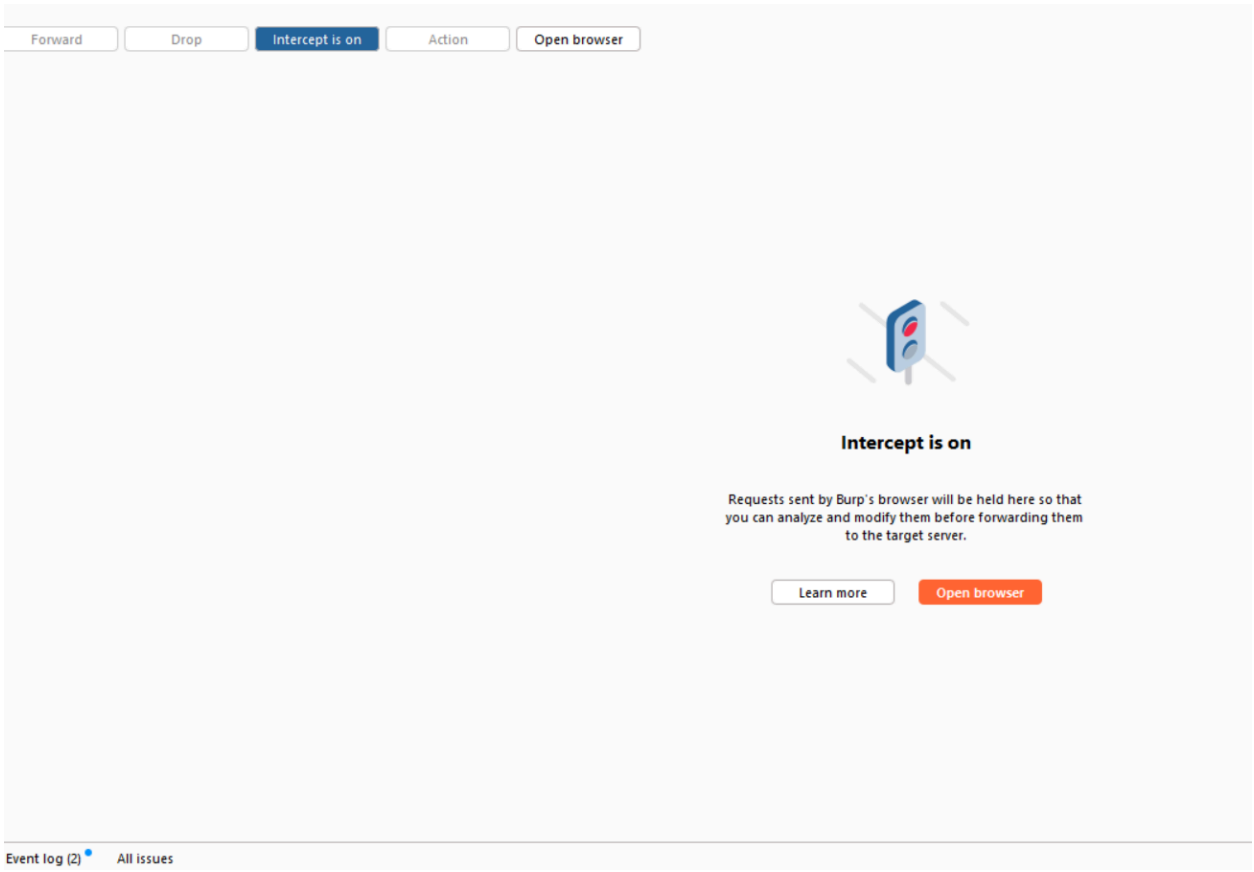
Step 3 : Open the Burp Suite Tool and go to the proxy tab in the tool



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

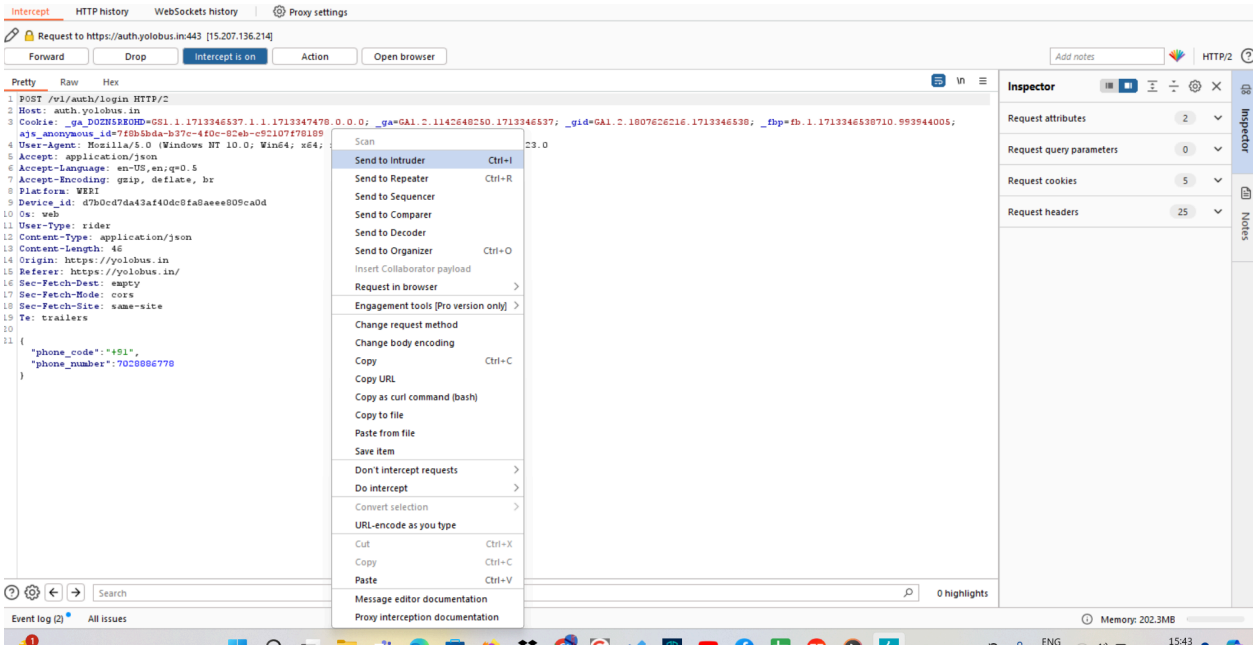


Step 5 : Now to the burp suite tool and click on the intercept, this will intercept the request

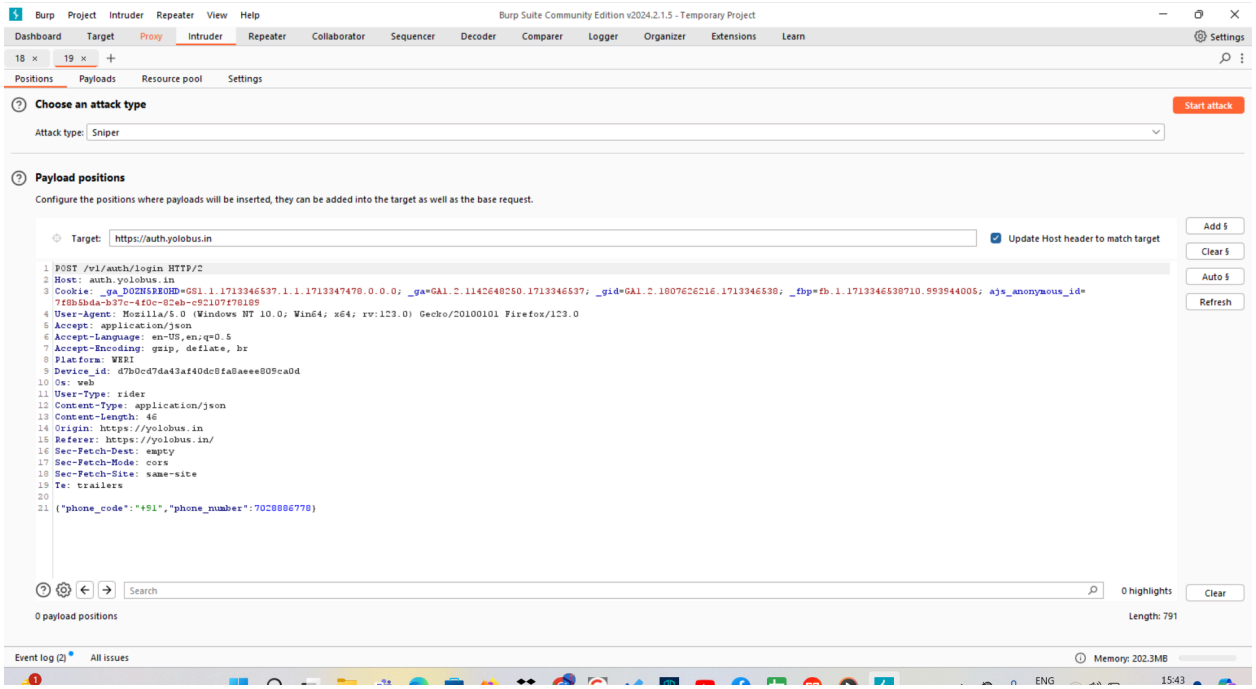


Step 6 : Now in the Website go and click on resend otp button

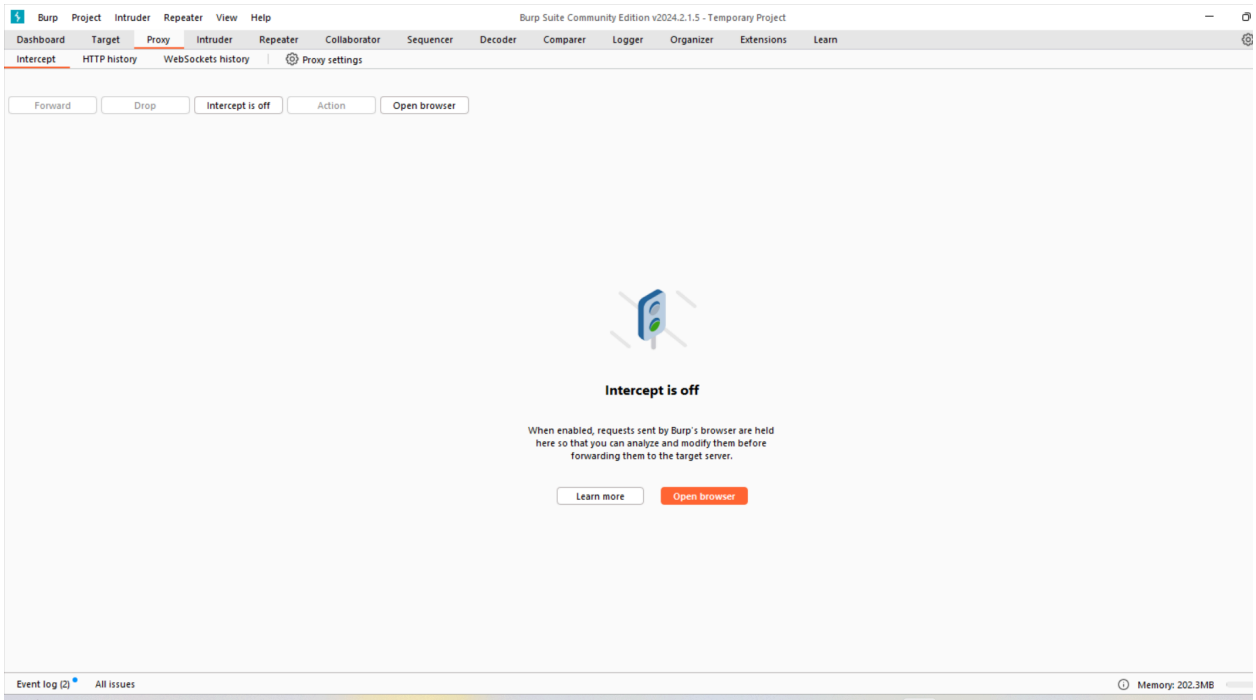
Step 7 : Now in the burp Suite tool you can see the request in the proxy tab , right click in that tab and send that request to the intruder



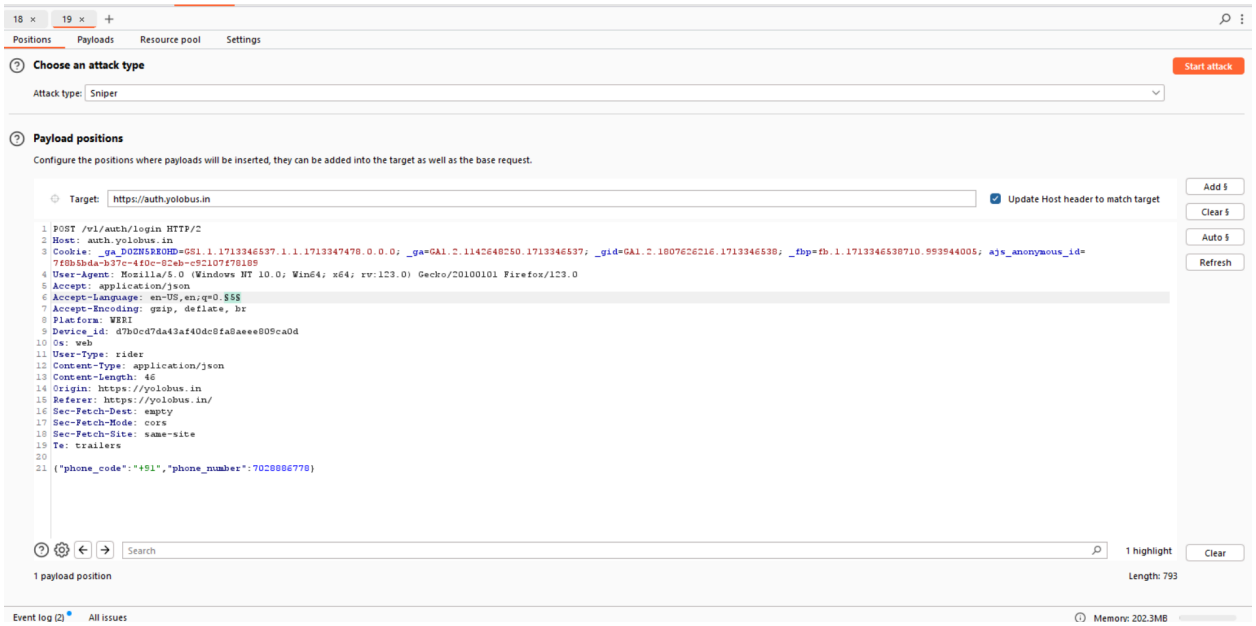
Step 8 : In the Intruder Tab we can see the entire reuqest thst is been sent , click on the clear button on the right side



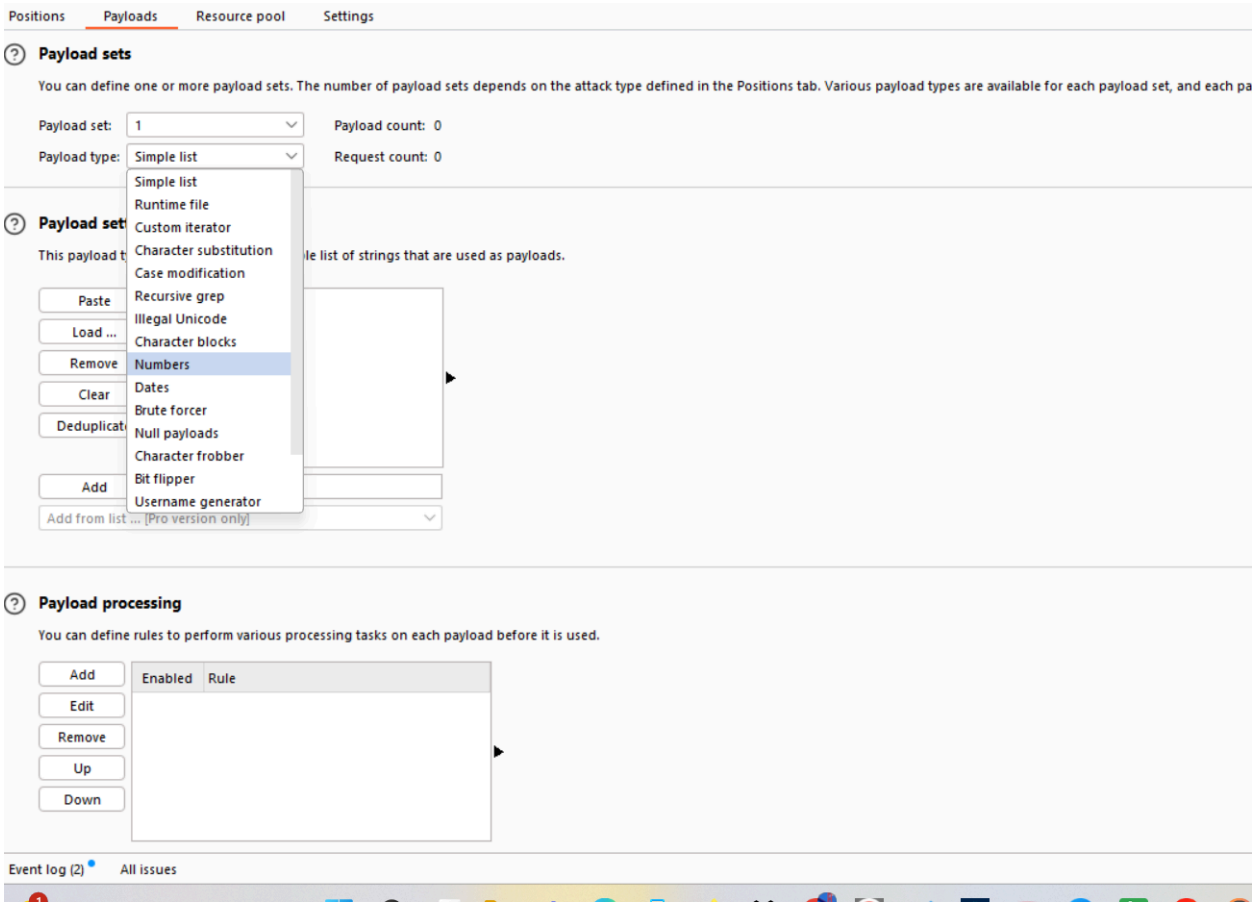
Step 9 : Again go to the Proxy tab and off the intercept by click on intercept off button



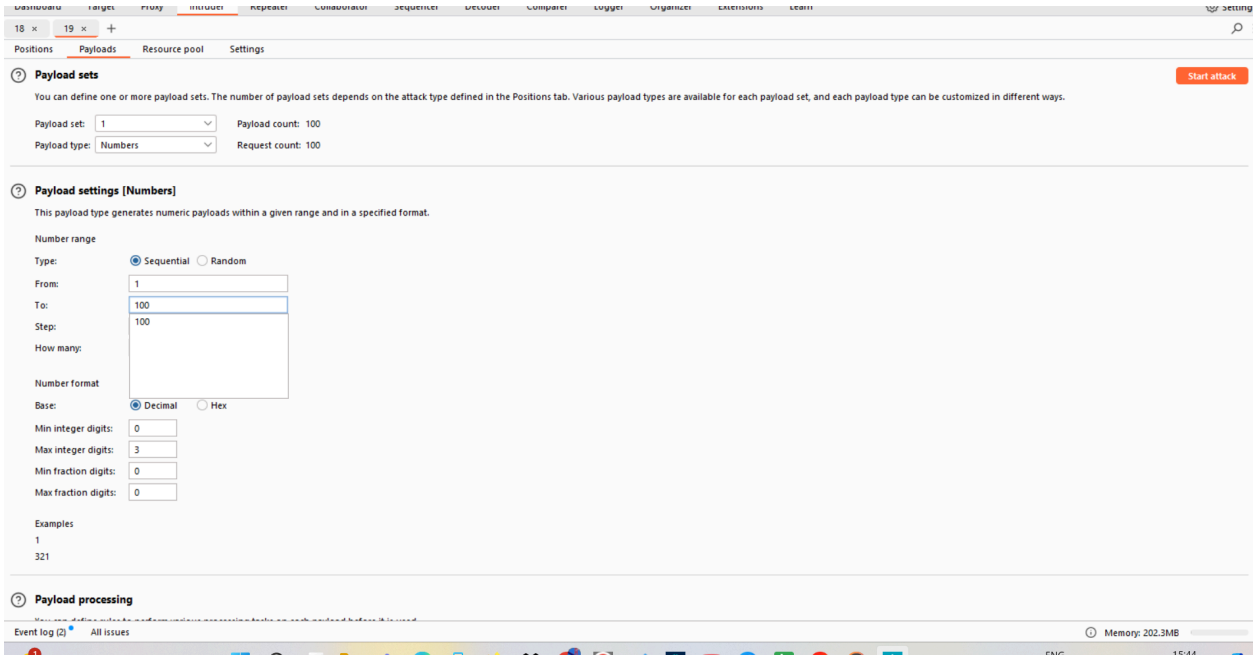
Step 10 : Now go to the Intruder tab and in the request we can see the accept-language text in that accept language we can see a number like q=0.5 , in this select the 5 number and click on the add button on right side



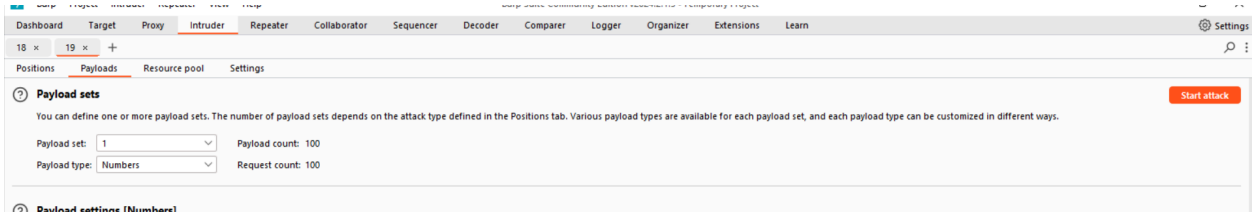
Step 11 : Now in the intruder tab only select the payload tab and in the payload type select the option has numbers



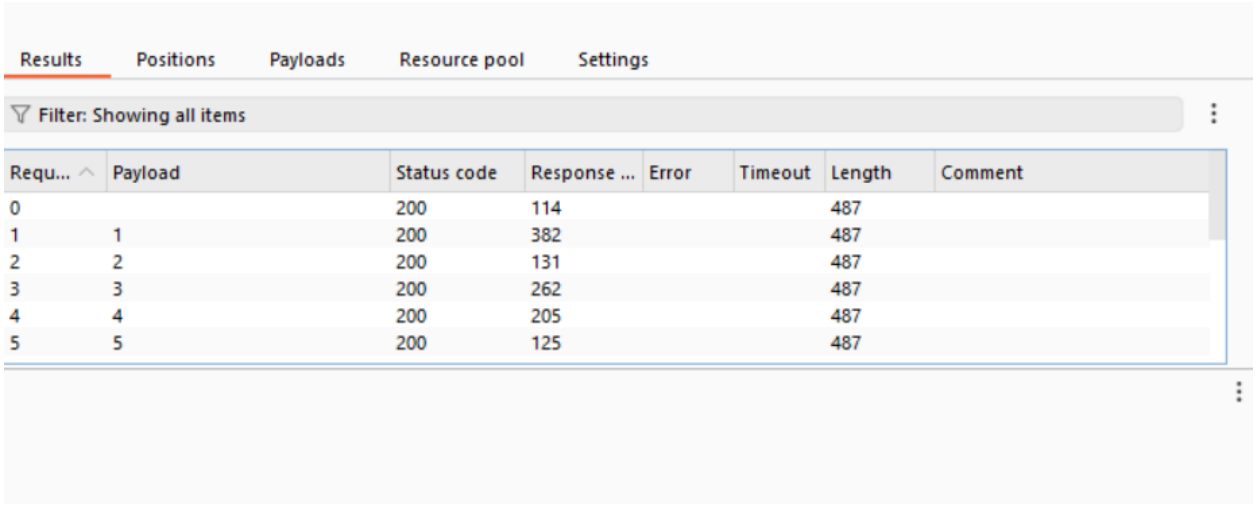
Step 12 : In the Payload setting set the payload by setting the FROM as 1 and TO HAS 100



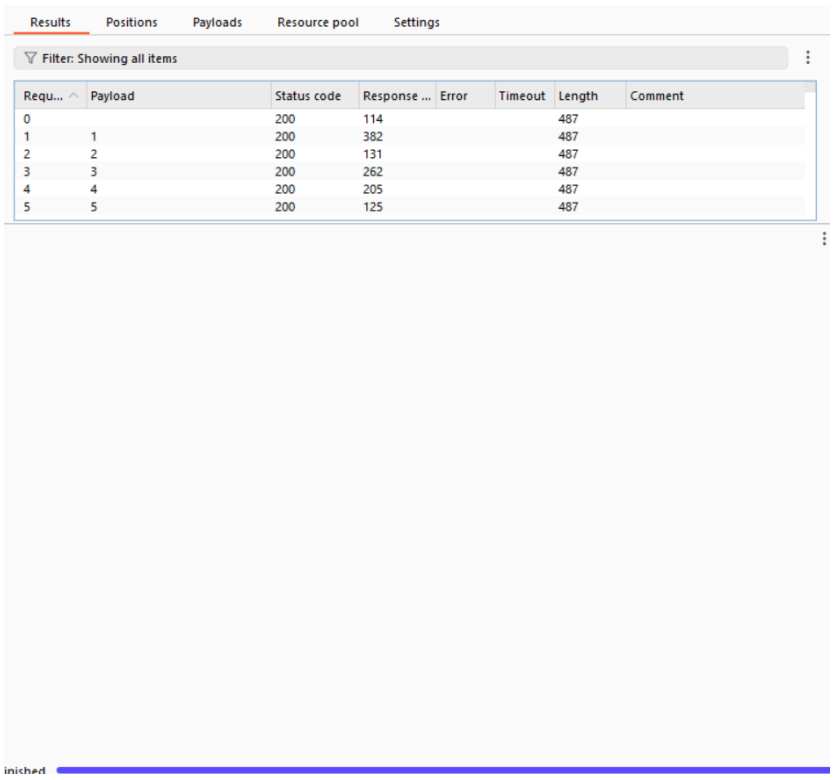
Step 13 : Lastly click on the attack button in orange on the Top right corner



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 vulnerbale to No rate limiting attack

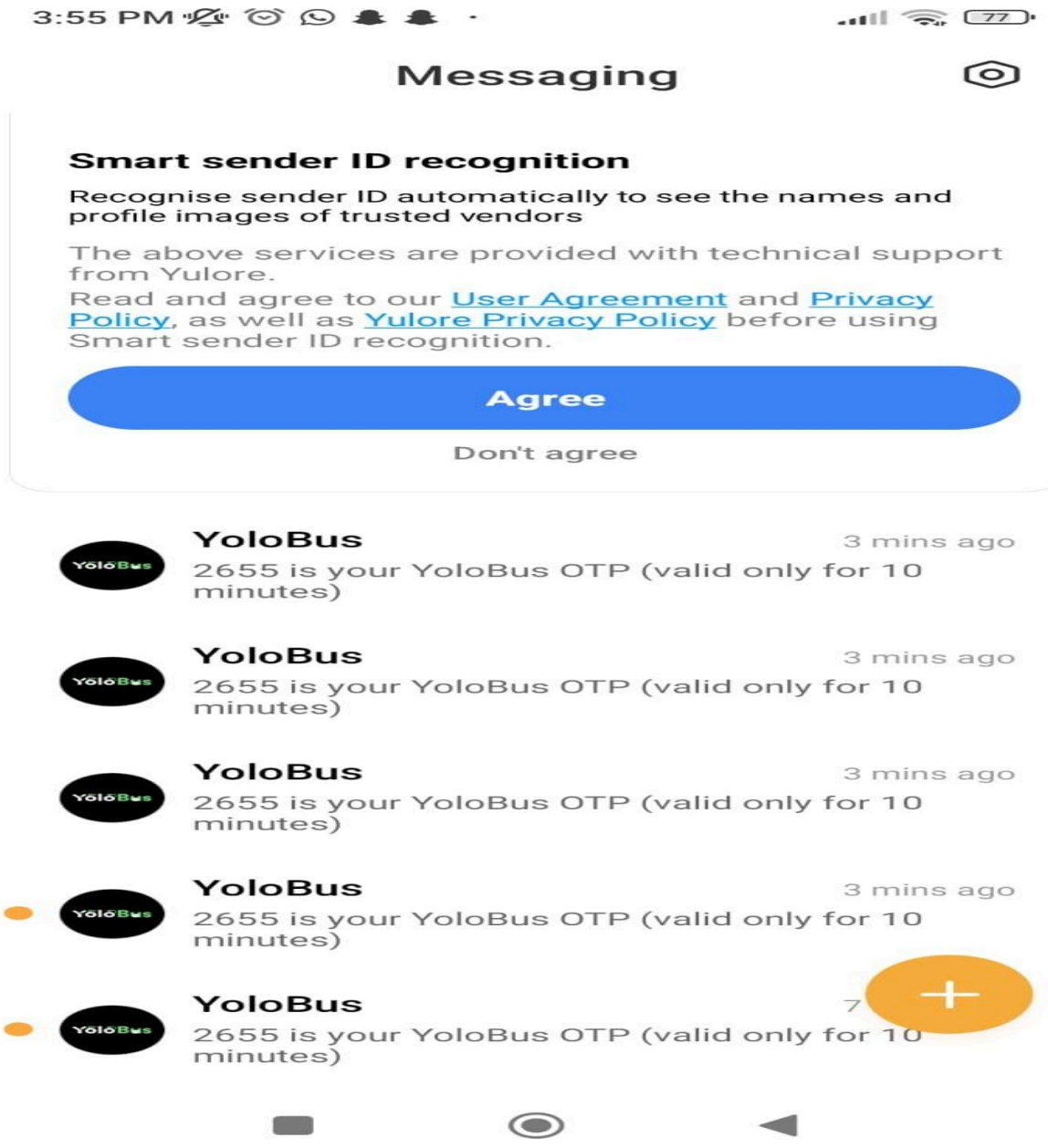


Requ...	Payload	Status code	Response ...	Error	Timeout	Length	Comment
0		200	114			487	
1	1	200	382			487	
2	2	200	131			487	
3	3	200	262			487	
4	4	200	205			487	
5	5	200	125			487	



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	

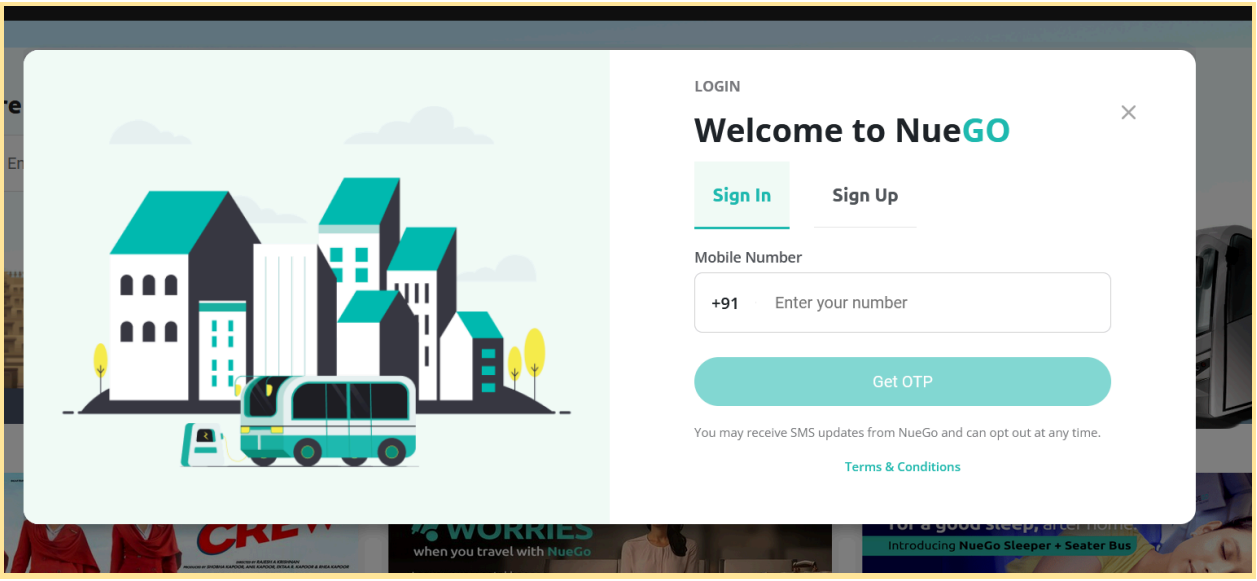
Step 15: Since i am getting 100 otps it is vulnerable to no rate limiting attack


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

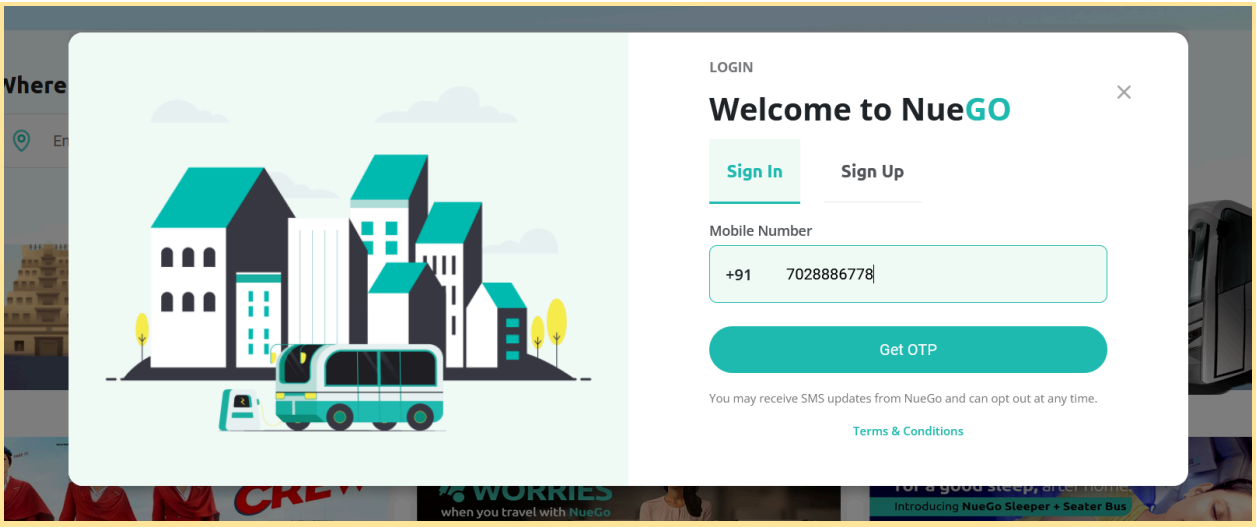
b) https://nuego.in/

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

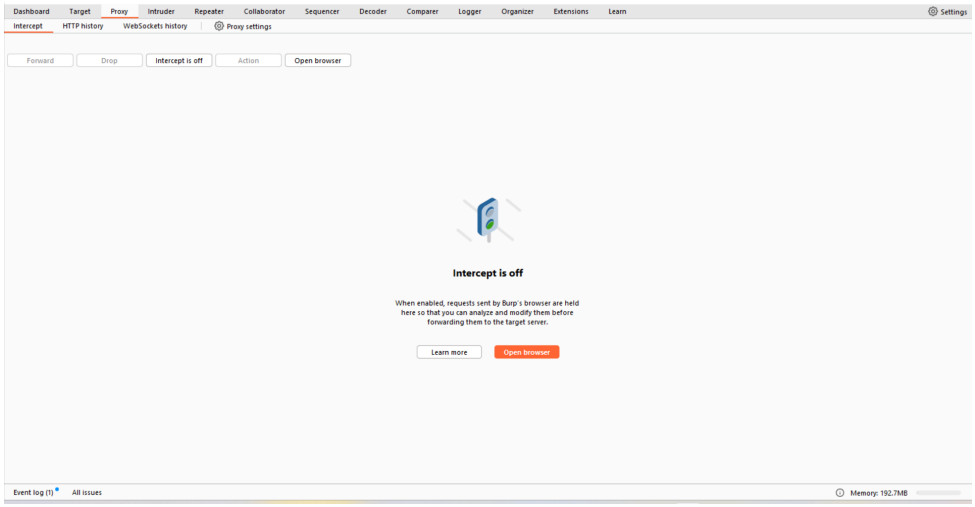
Step 1 : Go the Website and go to the login page of that website that has otp login



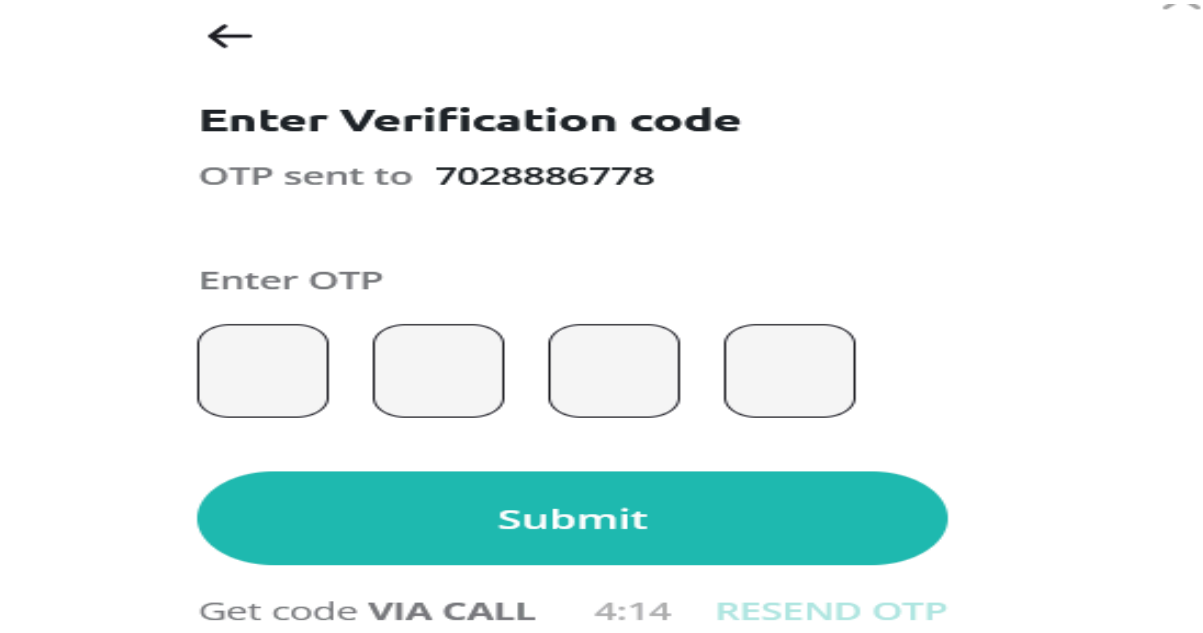
Step 2 : Enter your Number and click on send otp button



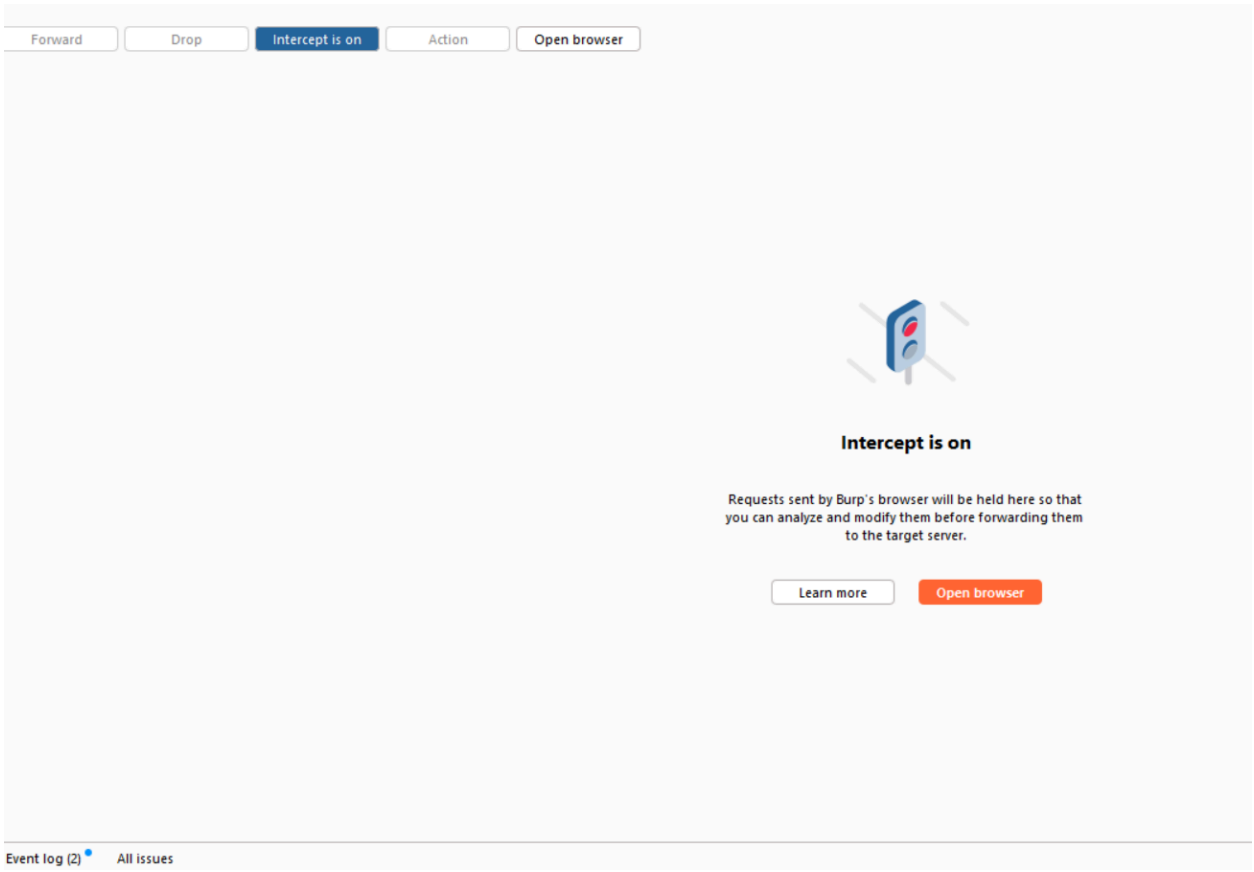
Step 3 : Open the Burp Suite Tool and go to the proxy tab in the tool



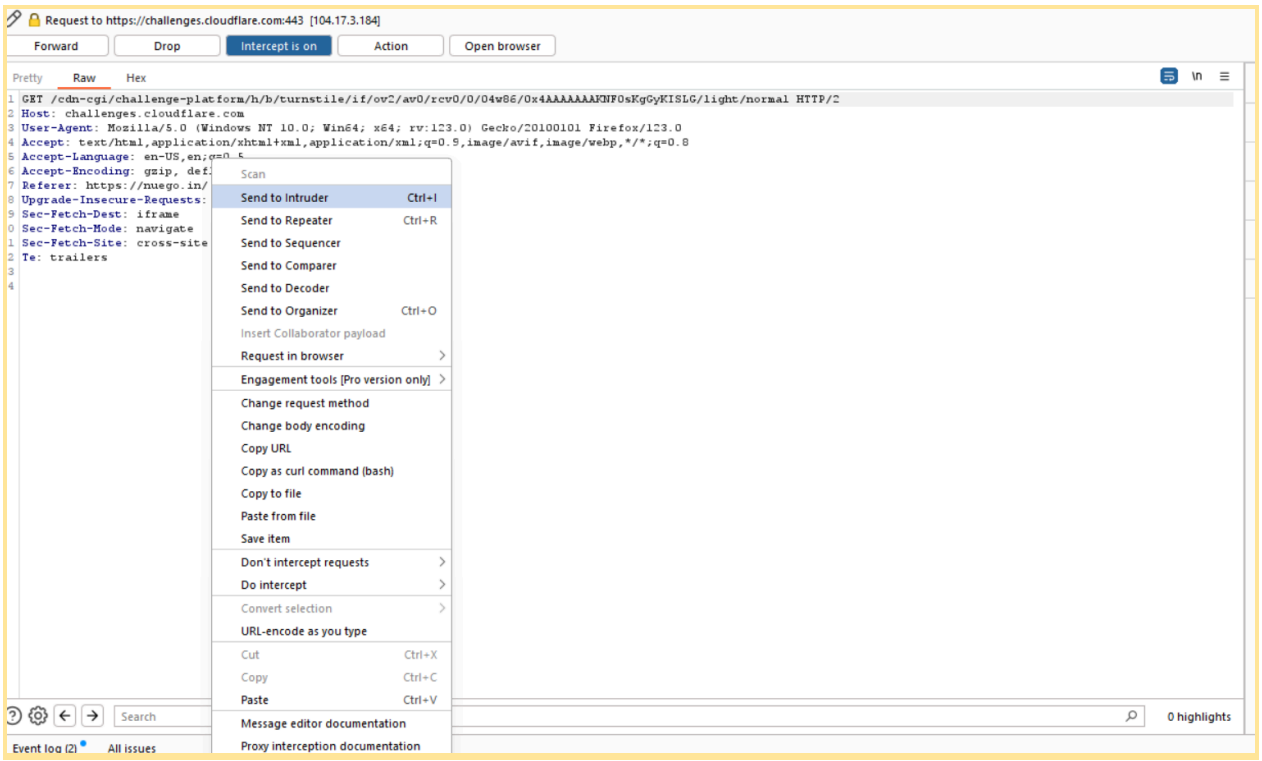
Step 4 : Now on your Website, there must be a resend otp button , don't just yet click on that button



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

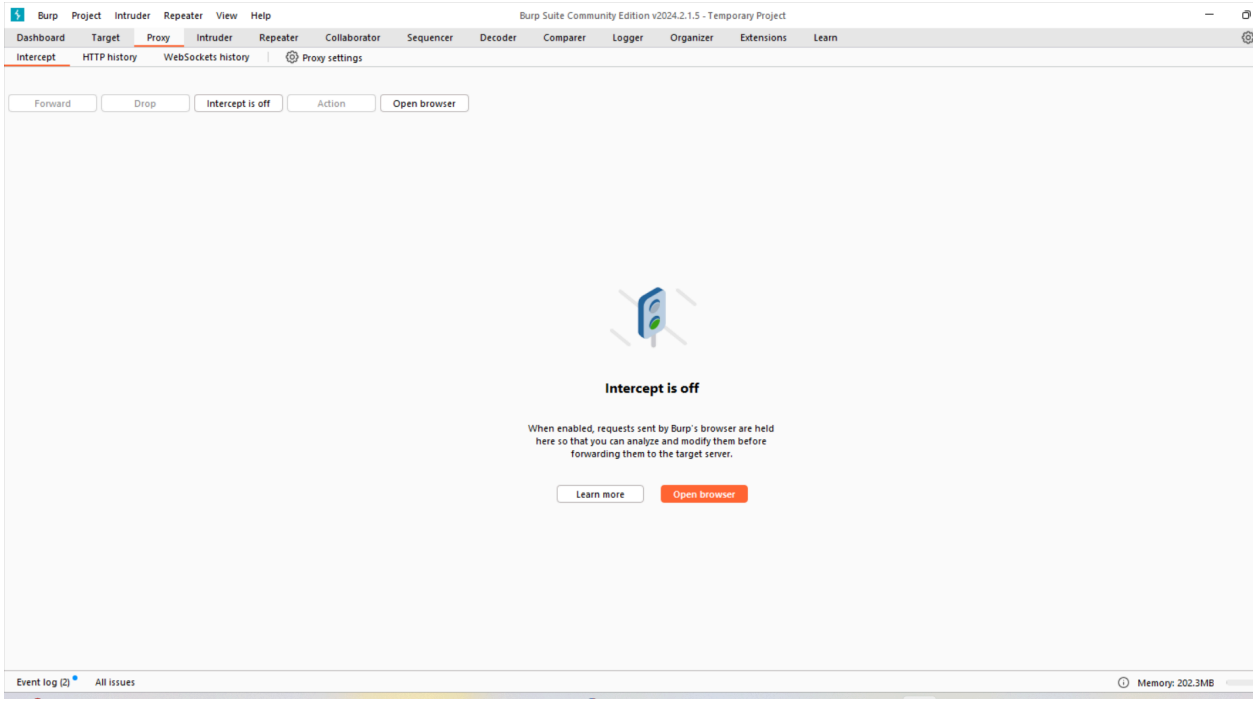


Step 6 : Now in the Website go and click on resend otp button
Step 7 : Now in the burp Suite tool you can see the request in the proxy tab , right click in that tab and send that request to the intruder

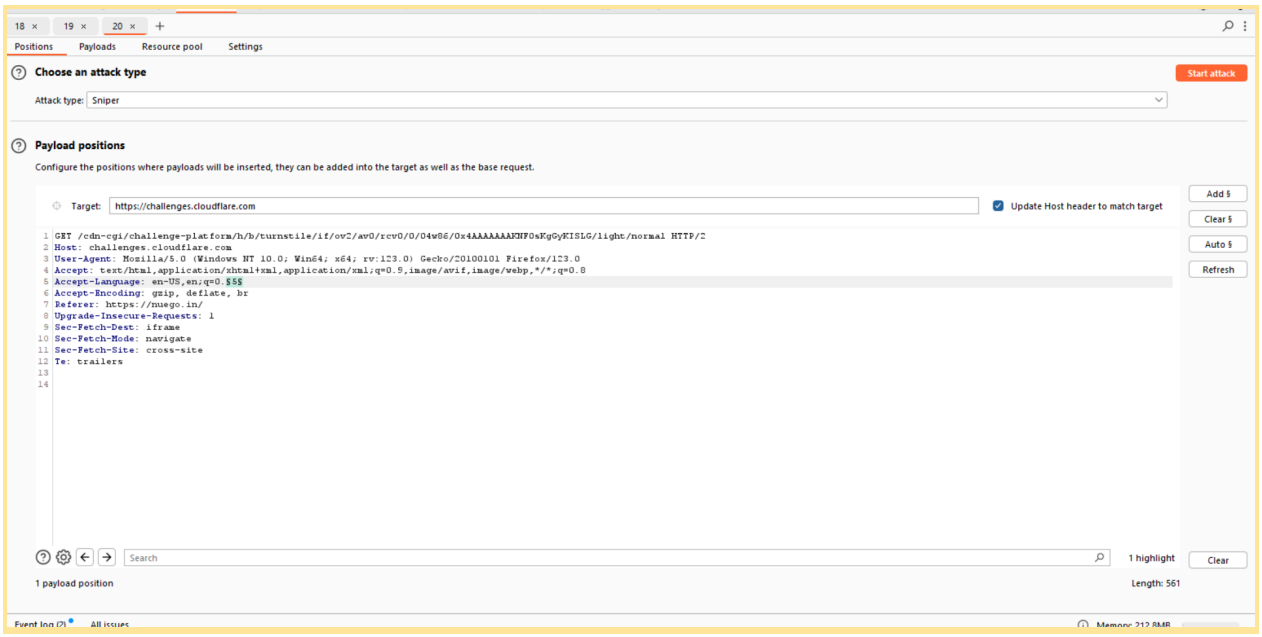


Step 8 : In the Intruder Tab we can see the entire request that is been sent , click on the clear button on the right side

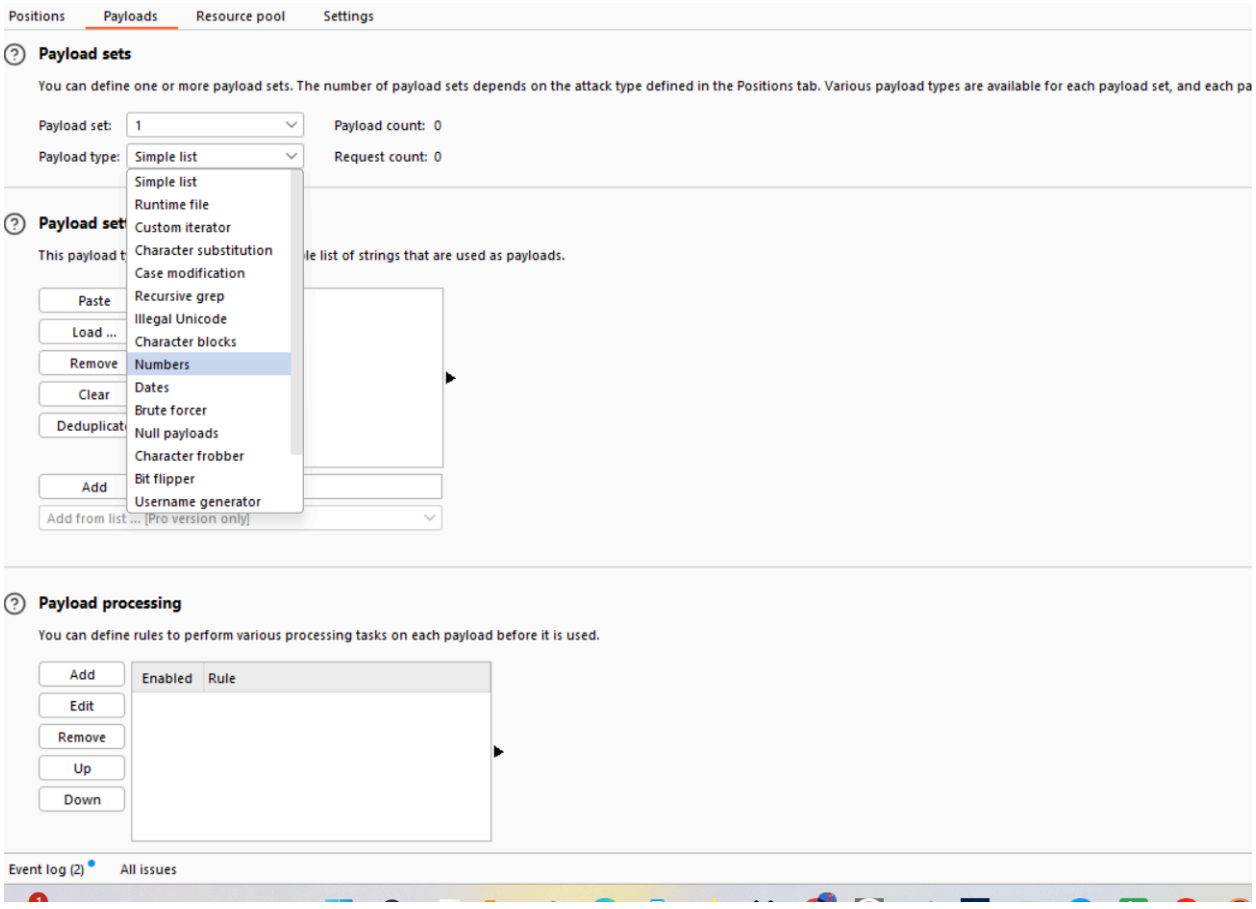
Step 9 : Again go to the Proxy tab and off the intercept by click on intercept off button



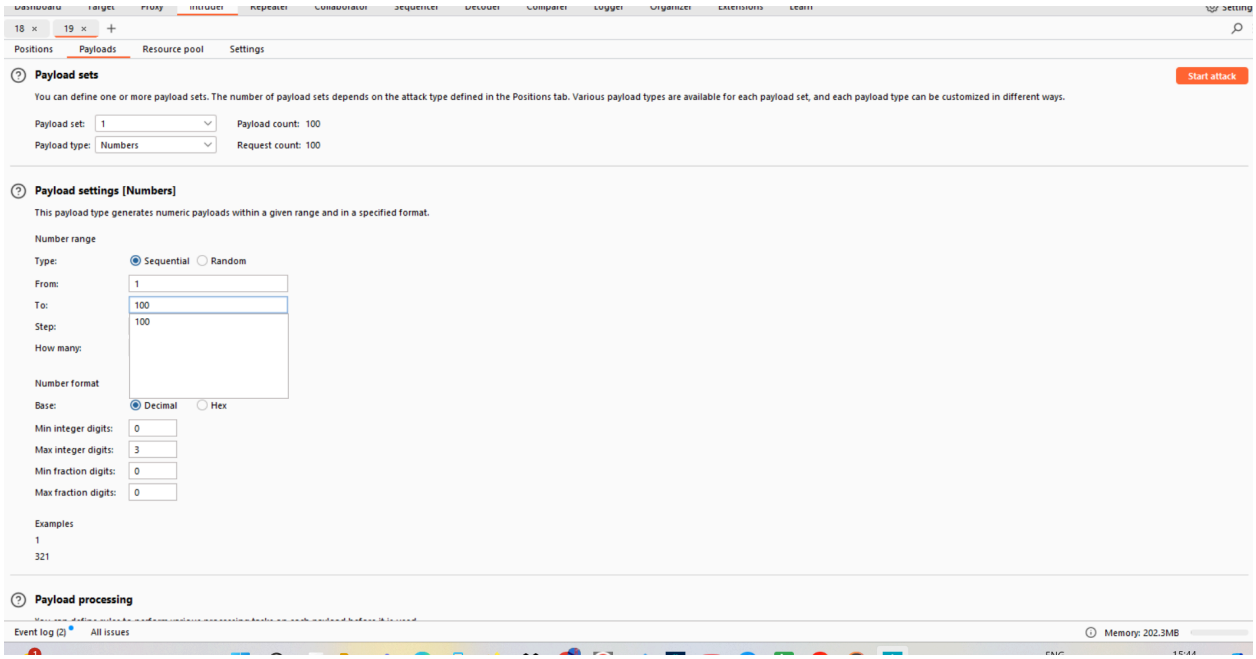
Step 10 : Now go to the Intruder tab and in the request we can see the accept-language text in that accept language we can see a number like q=0.5 , in this select the 5 number and click on the add button on right side



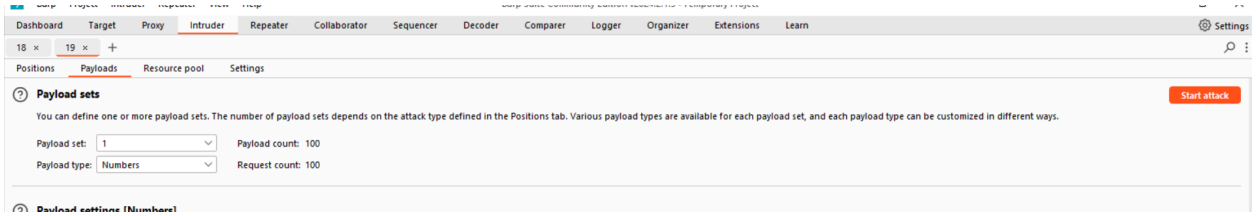
Step 11 : Now in the intruder tab only select the payload tab and in the payload type select the option has numbers



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

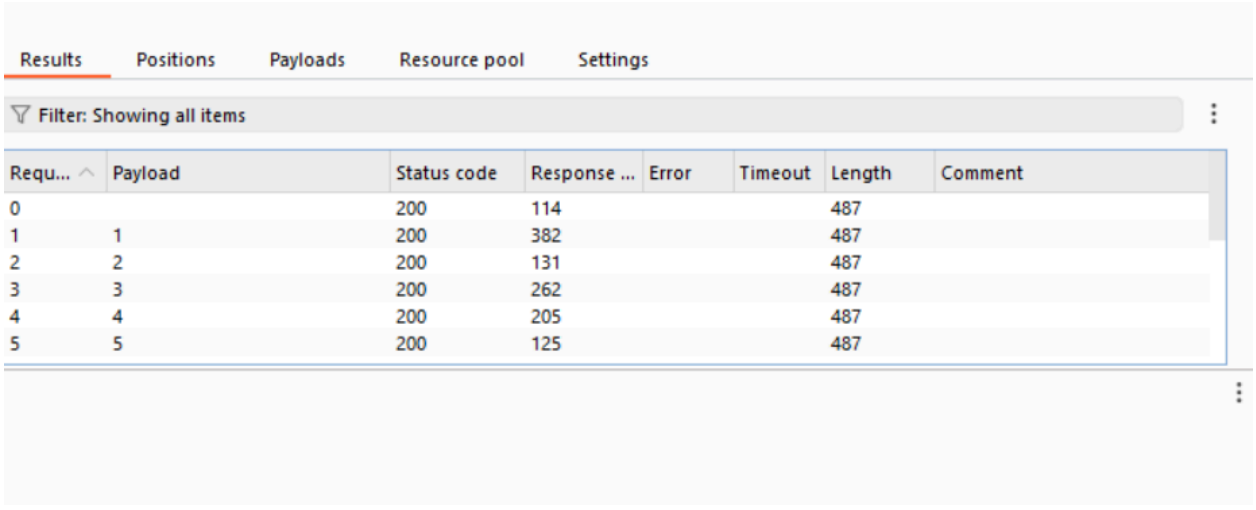


Step 13 : Lastly click on the attack button in orange on the Top right corner



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 vulnerbale to No rate limiting attack

\

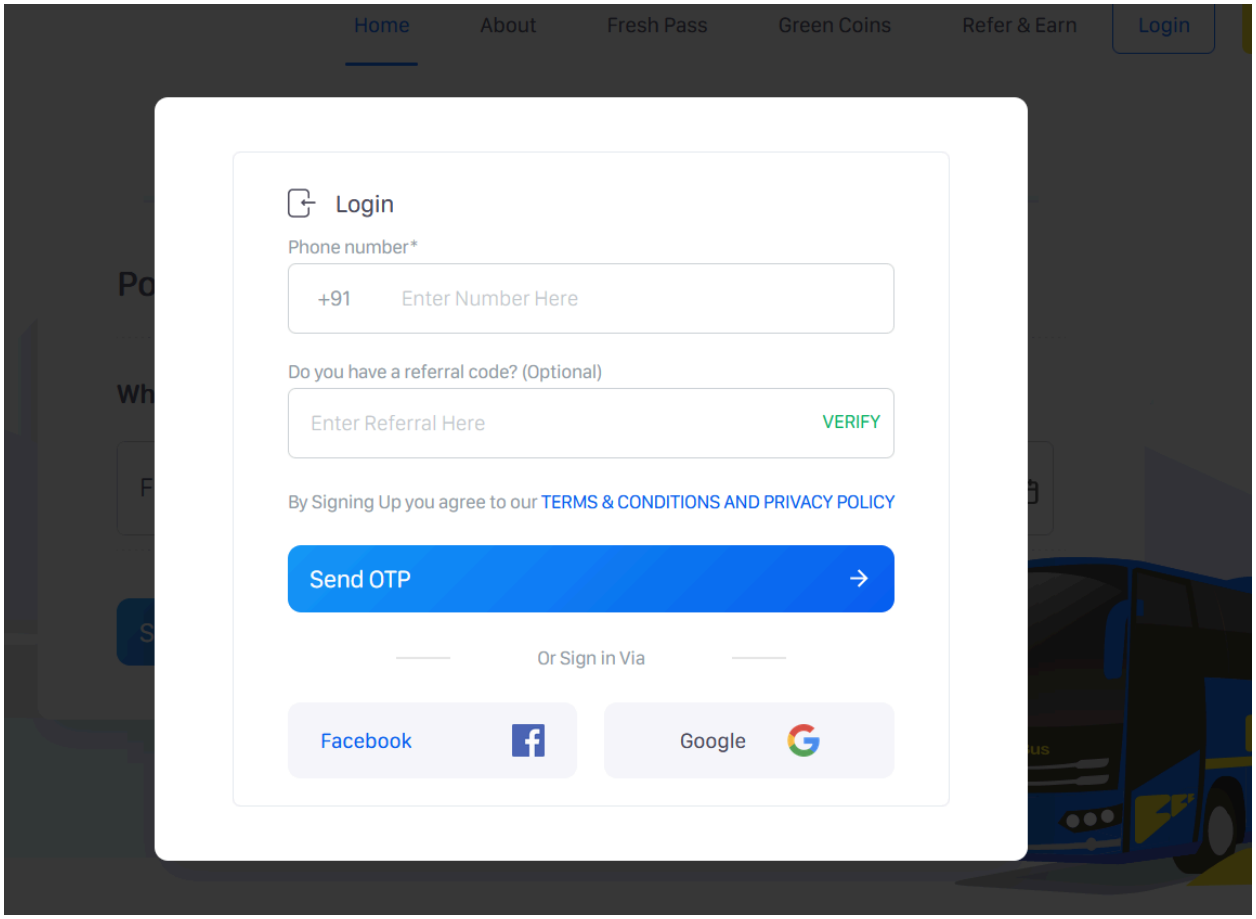


Requ...	Payload	Status code	Response ...	Error	Timeout	Length	Comment
0		200	114			487	
1	1	200	382			487	
2	2	200	131			487	
3	3	200	262			487	
4	4	200	205			487	
5	5	200	125			487	

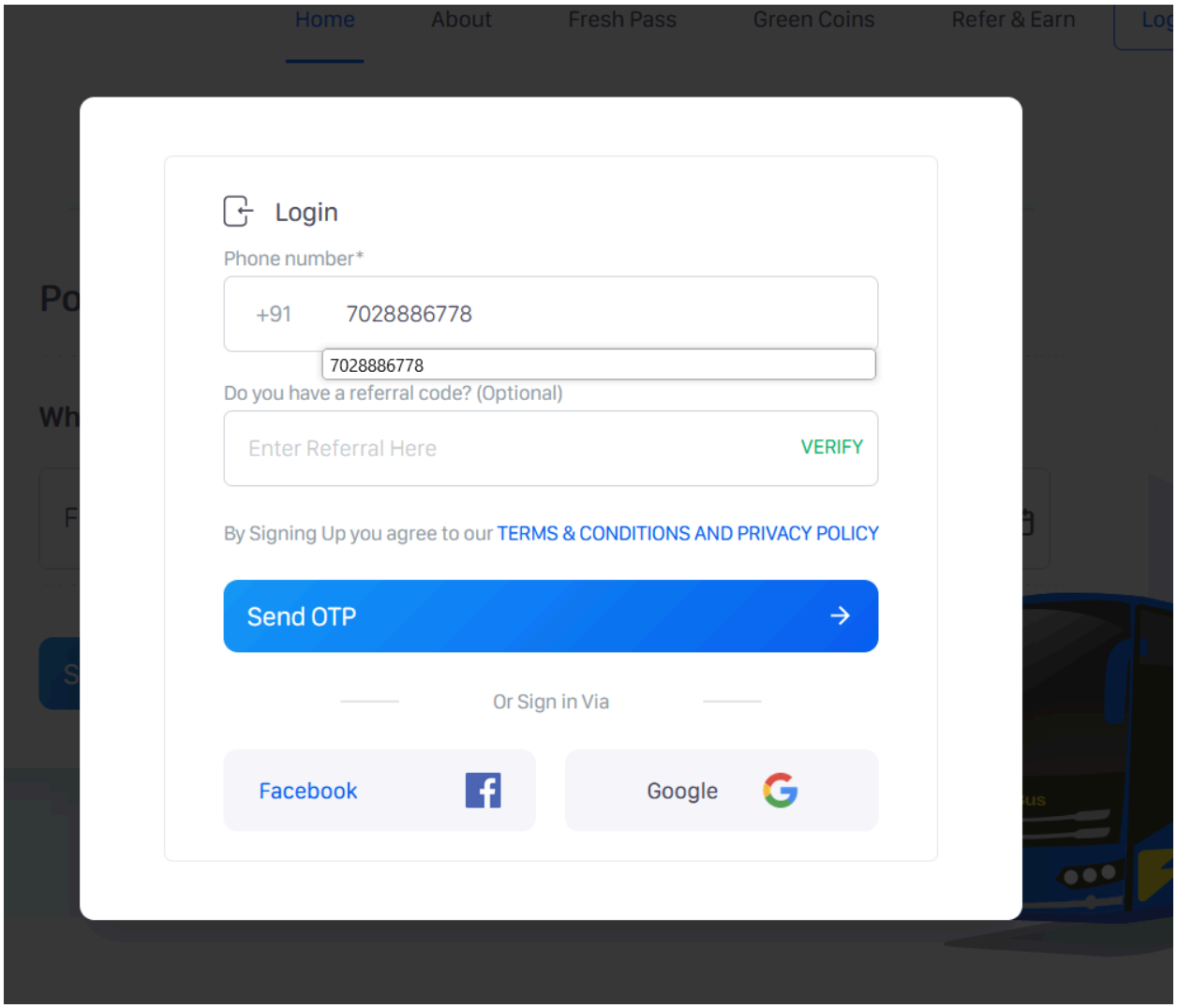
Step 15: Since I am not getting any otp it is not vulnerable to the no rate limiting attack

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

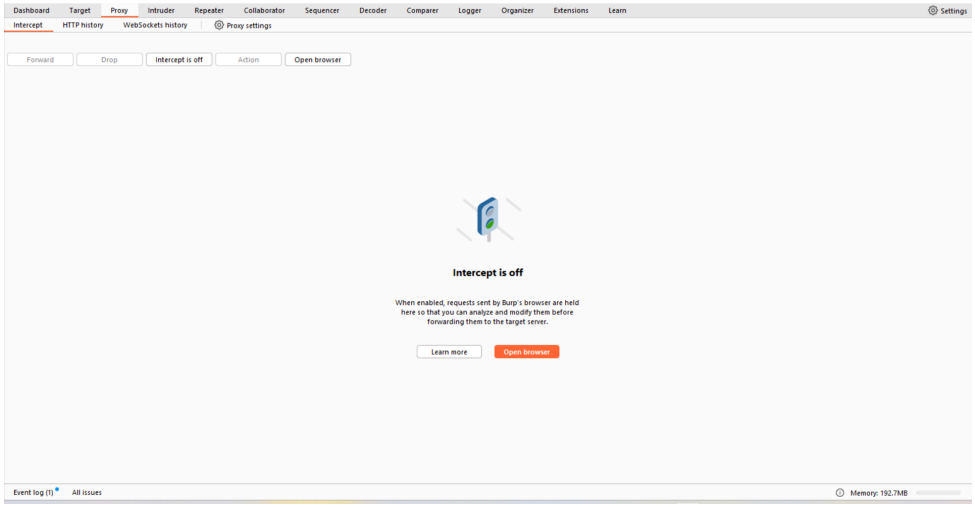
Step 1 : Go the Website and go to the login page of that website that has otp login



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

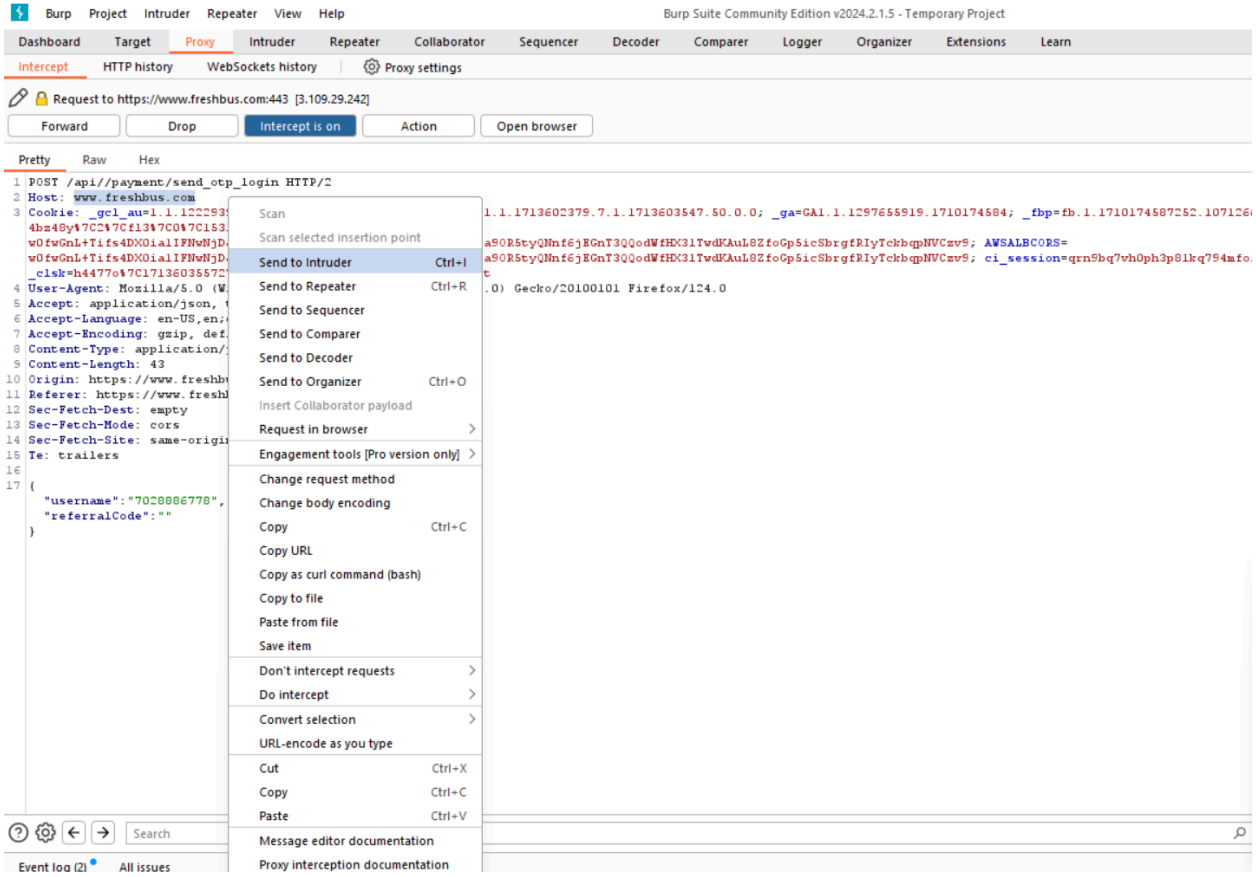


Step 3 : Open the Burp Suite Tool and go to the proxy tab in the tool and on the intercept

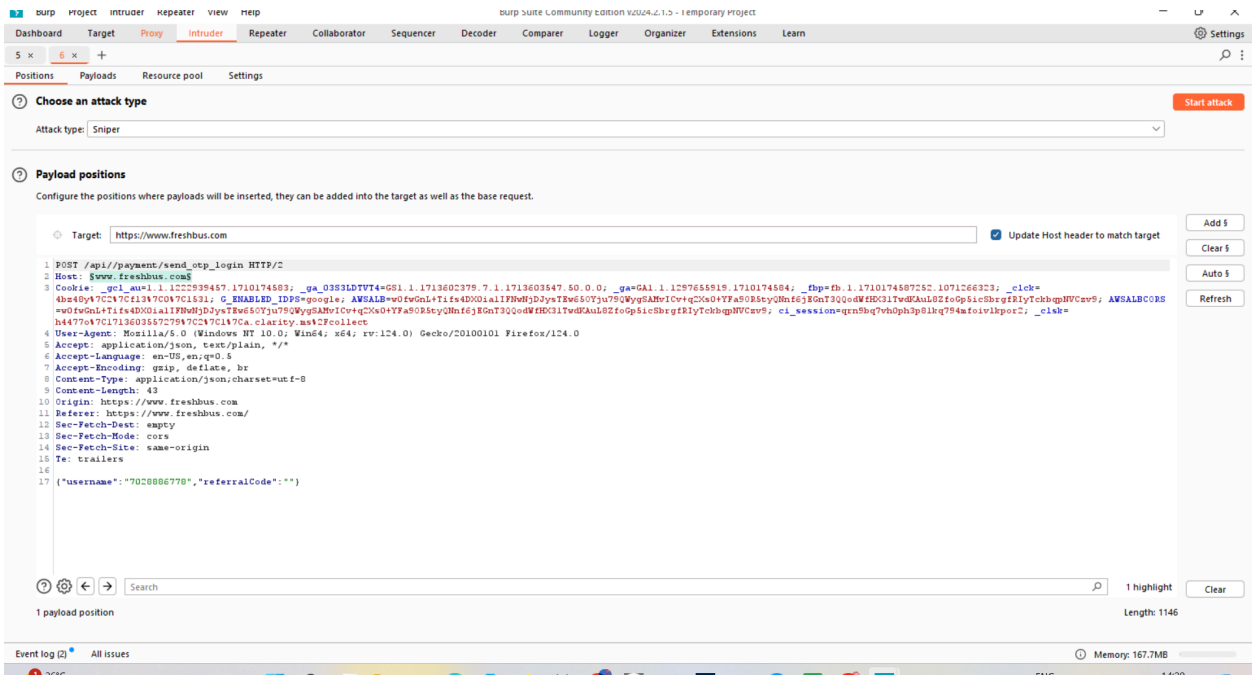


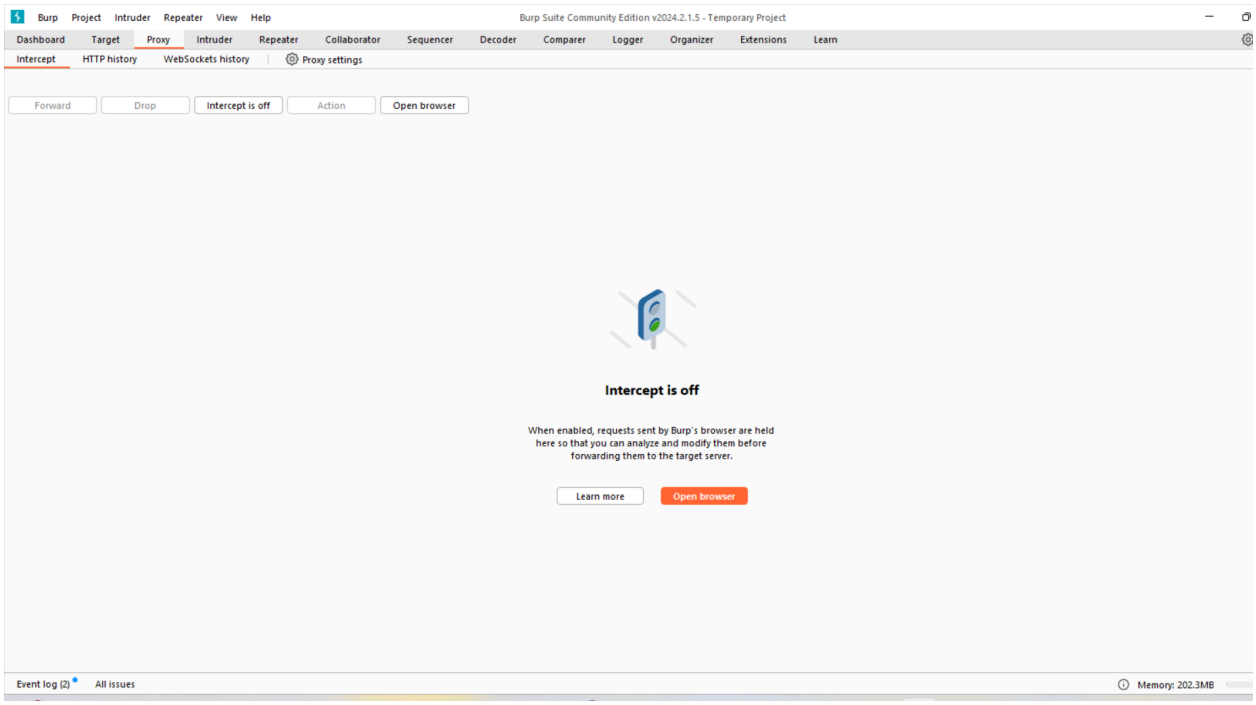
Step 4 : Now on your Website, click on the send otp button

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

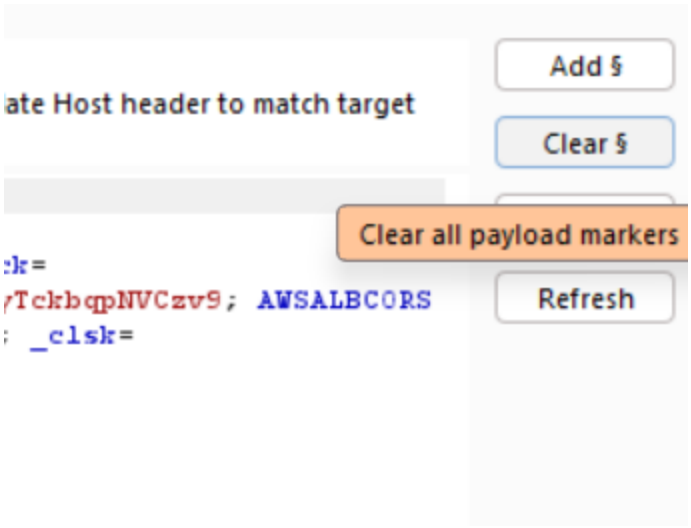


Step 6 : Then go to intruder and check if your receive the request and then just go to proxy tab and off the intercept

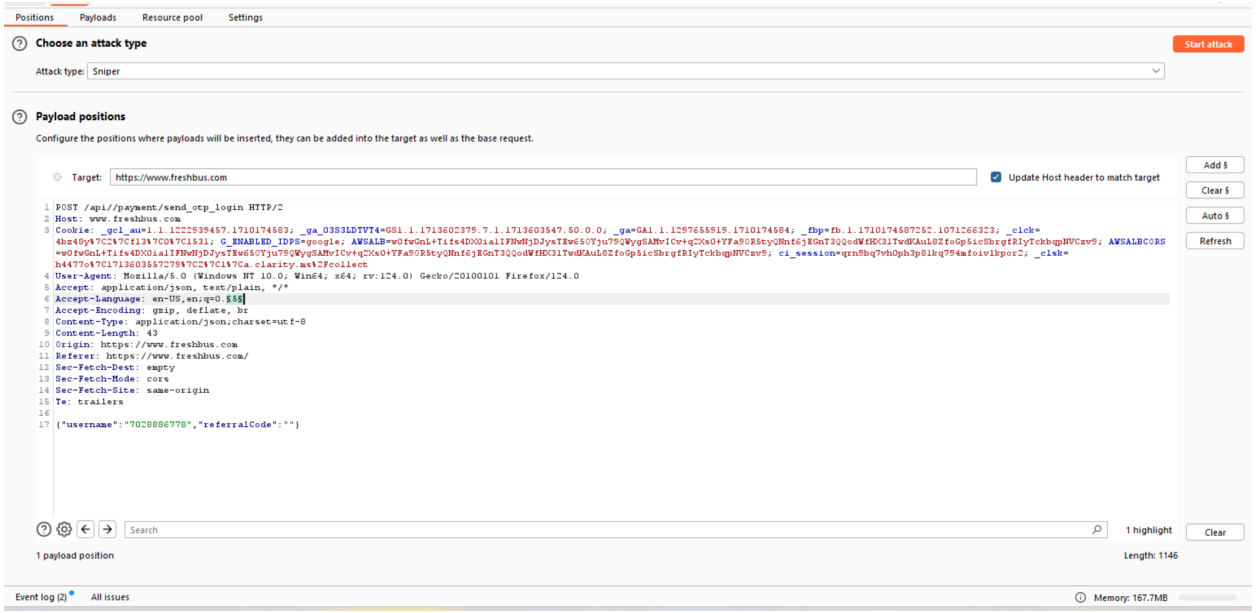




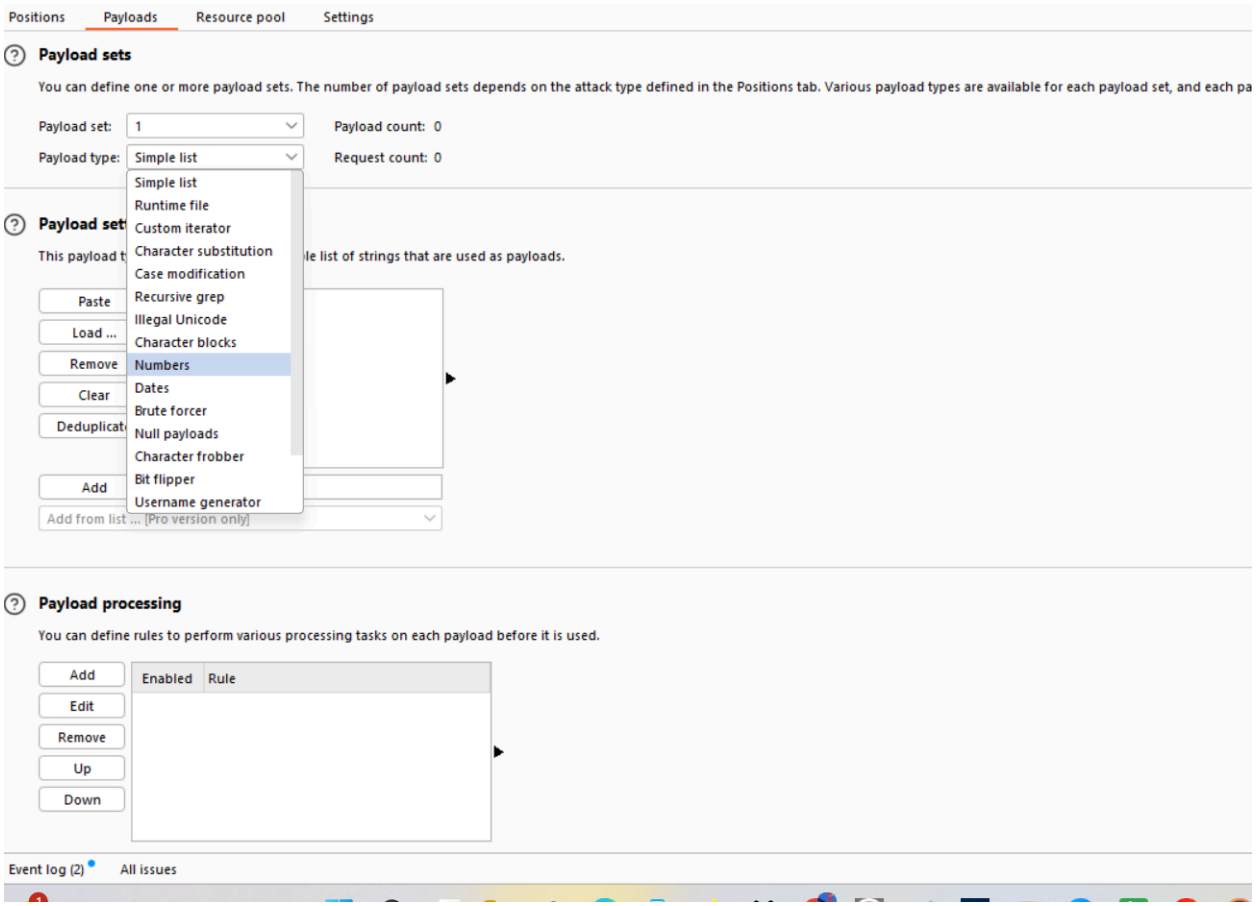
Step 7 : In the Intruder Tab we can see the entire request that is been sent , click on the clear button on the right side



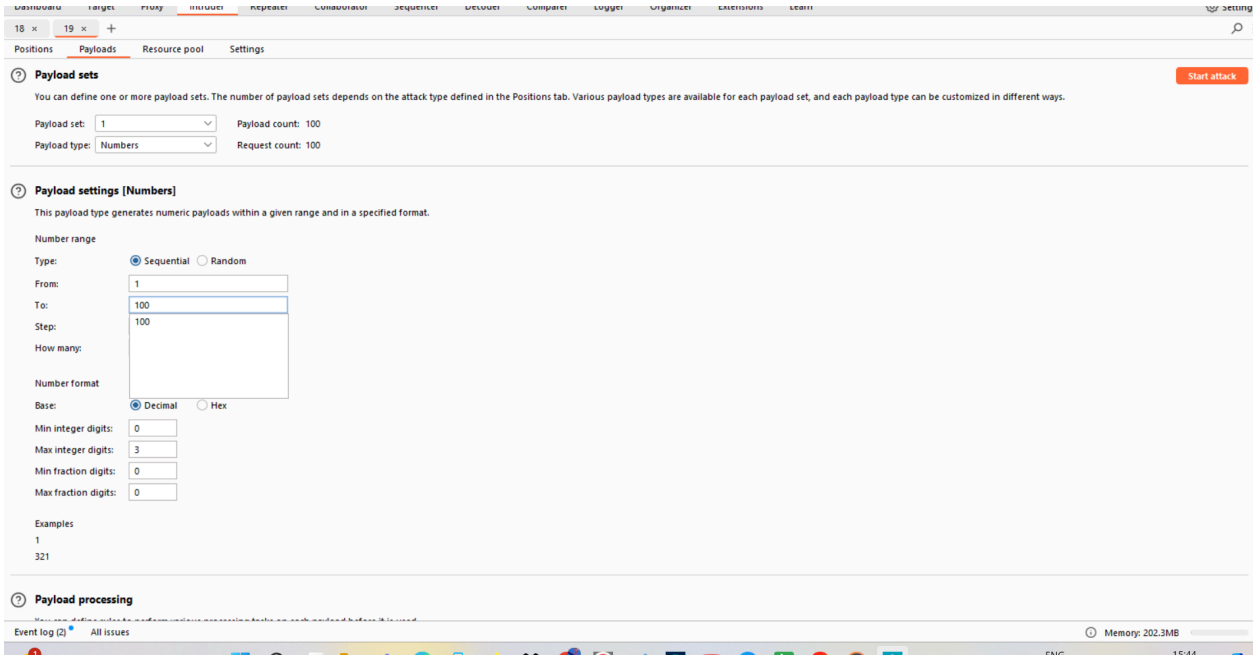
Step 8 : Now go to the Intruder tab and in the request we can see the accept-language text in that accept language we can see a number like q=0.5 , in this select the 5 number and click on the add button on right side



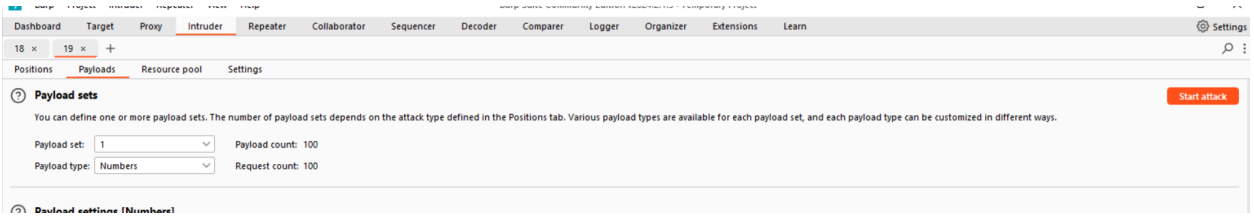
Step 11 : Now in the intruder tab only select the payload tab and in the payload type select the option has numbers



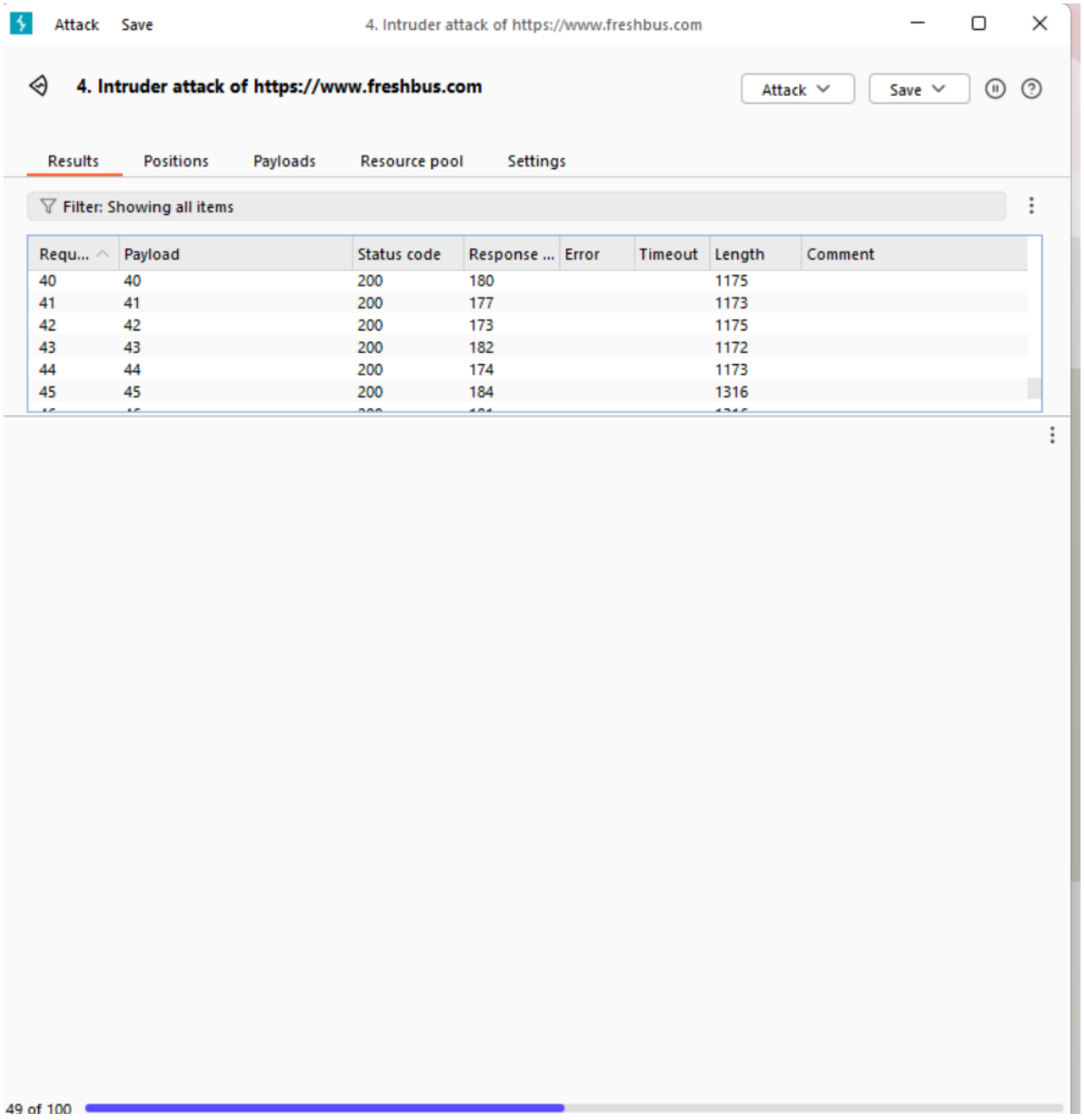
Step 12 : In the Payload setting set the payload by setting the FROM as 1 and TO HAS 100



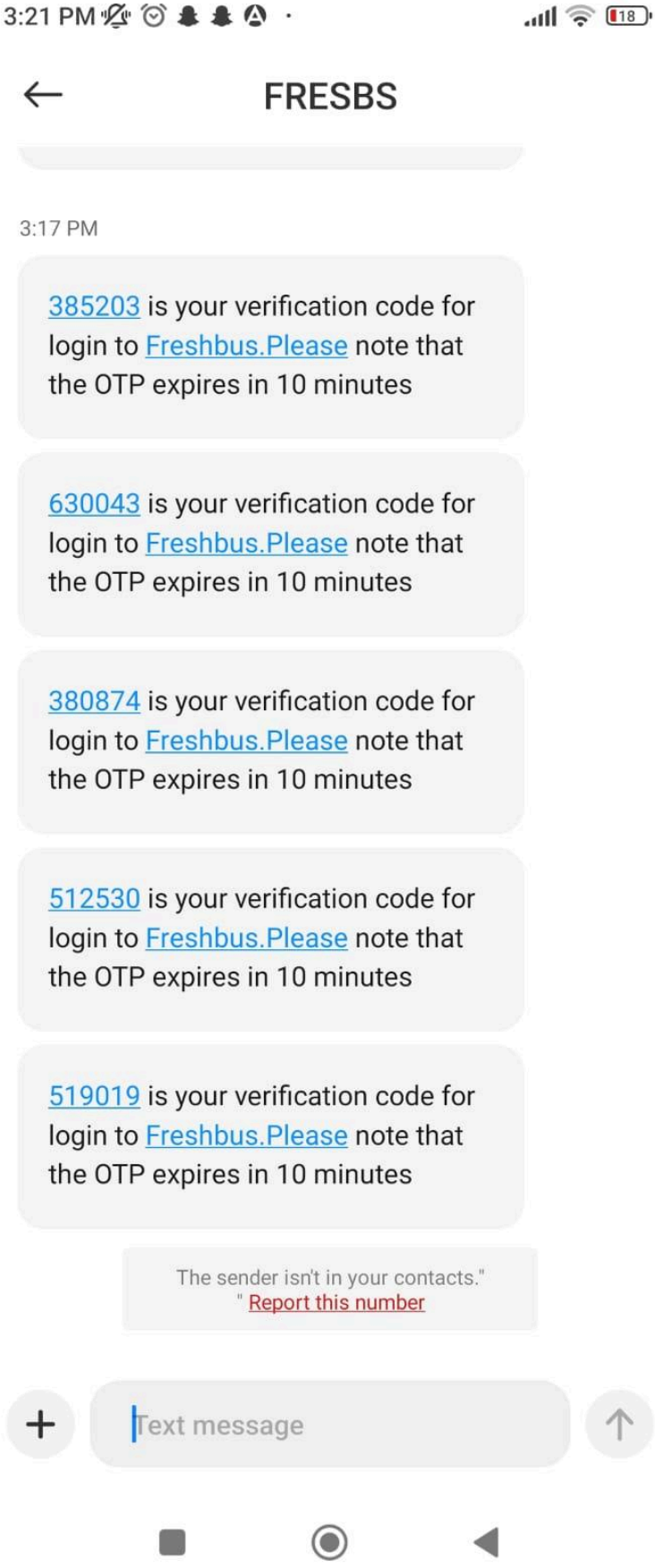
Step 13 : Lastly click on the attack button in orange on the Top right corner



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 vulnerbale to No rate limiting attack



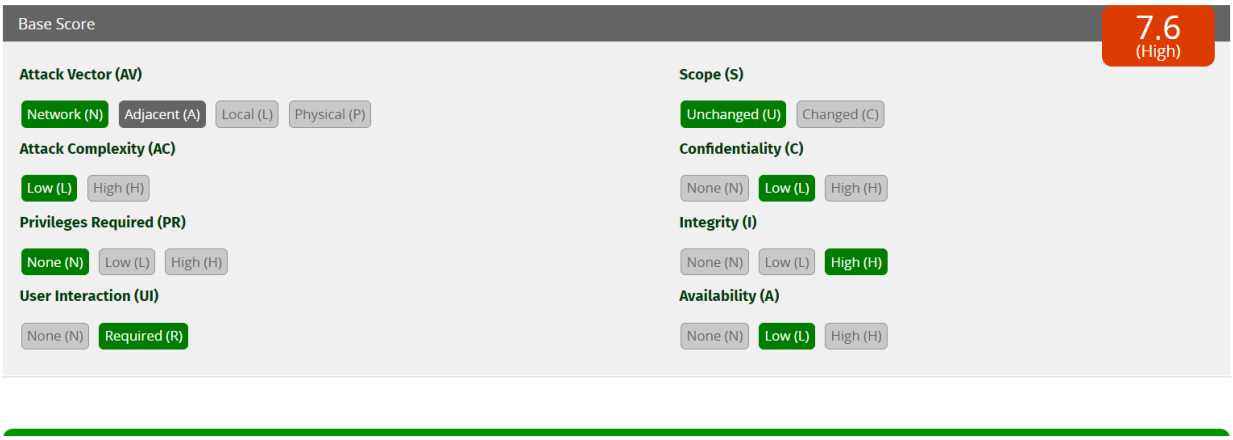
Step 15 : Since i am getting only few OTPs it is not vulnerable to no rate limiting


3:21 PM
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:

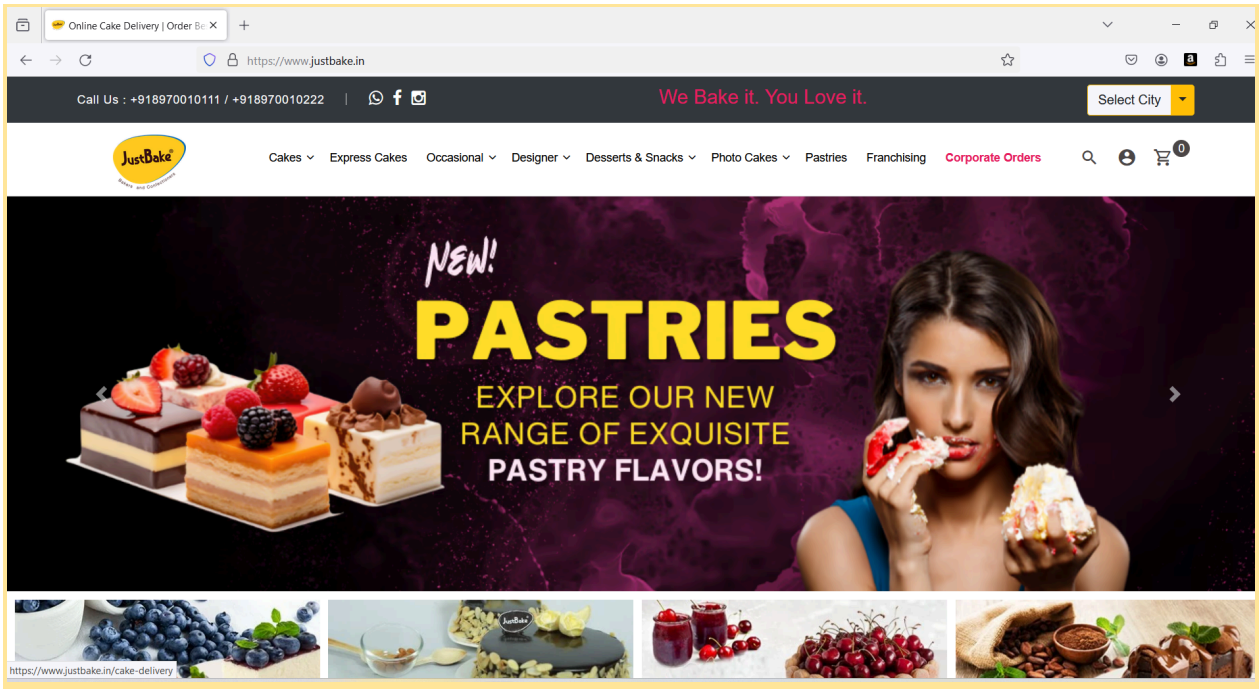
Financial Losses: Attackers can manipulate price parameters to lower the cost of items during transactions, leading to revenue losses for the organization.

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.

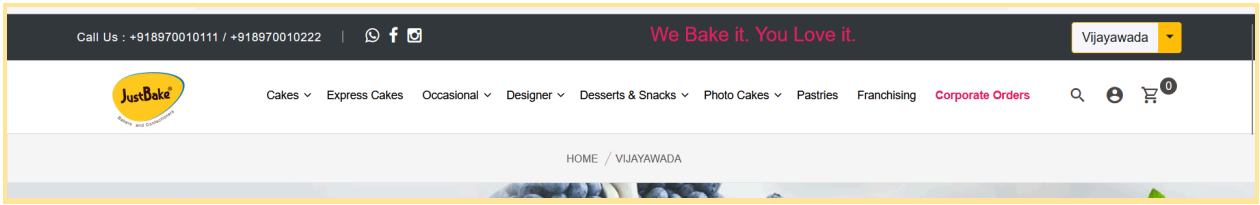
Steps to recreate

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

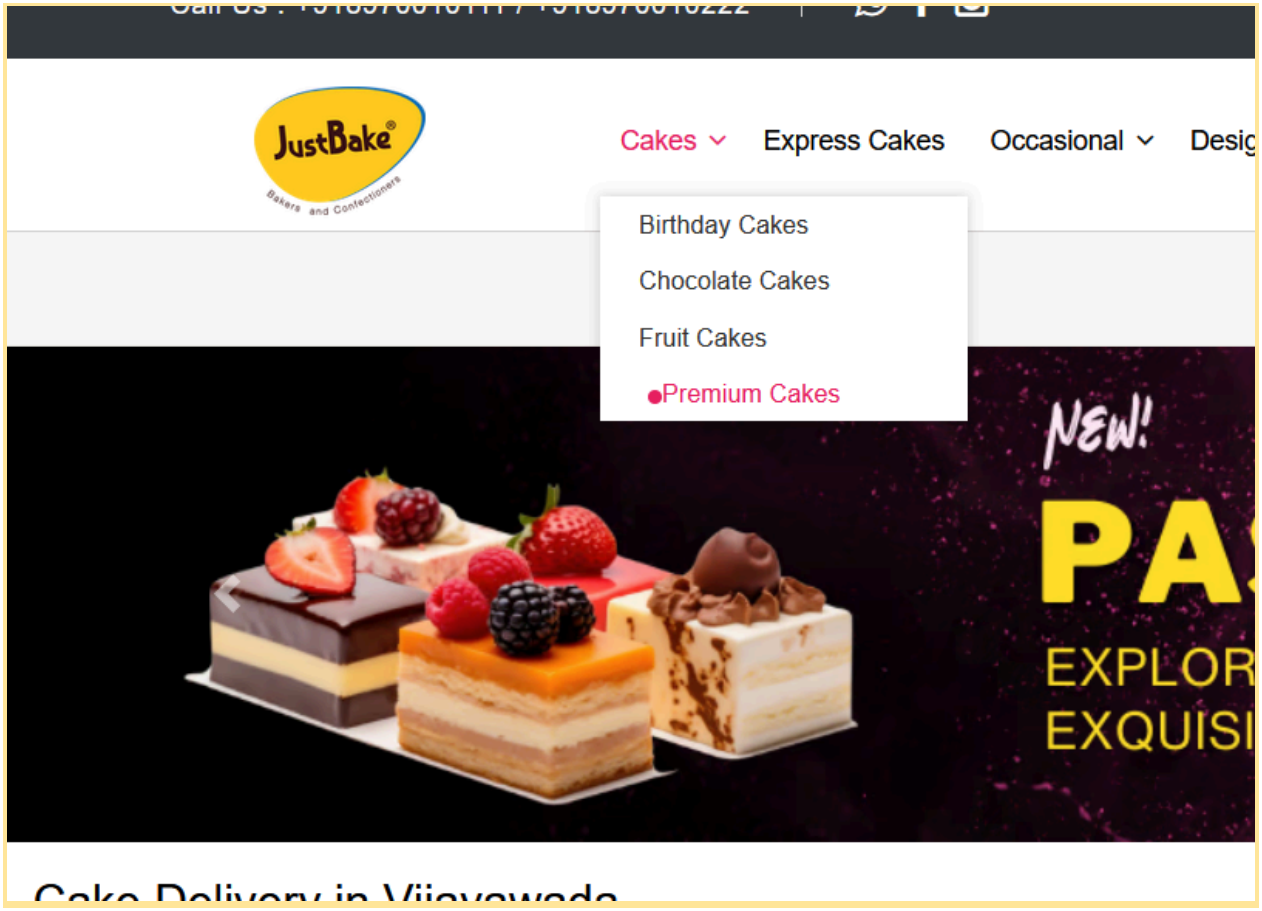
Step 1 : Open the website you want to perform parameter price tampering on

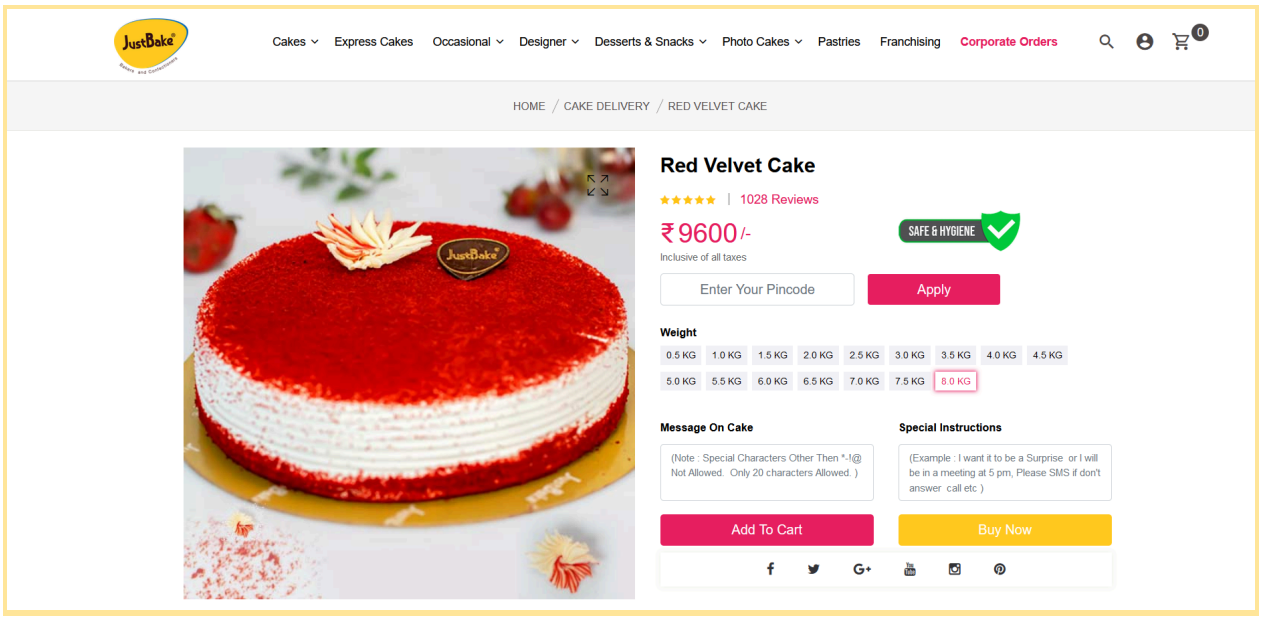


Step 2 : Click on the Select city in the tab select city and select the city you want

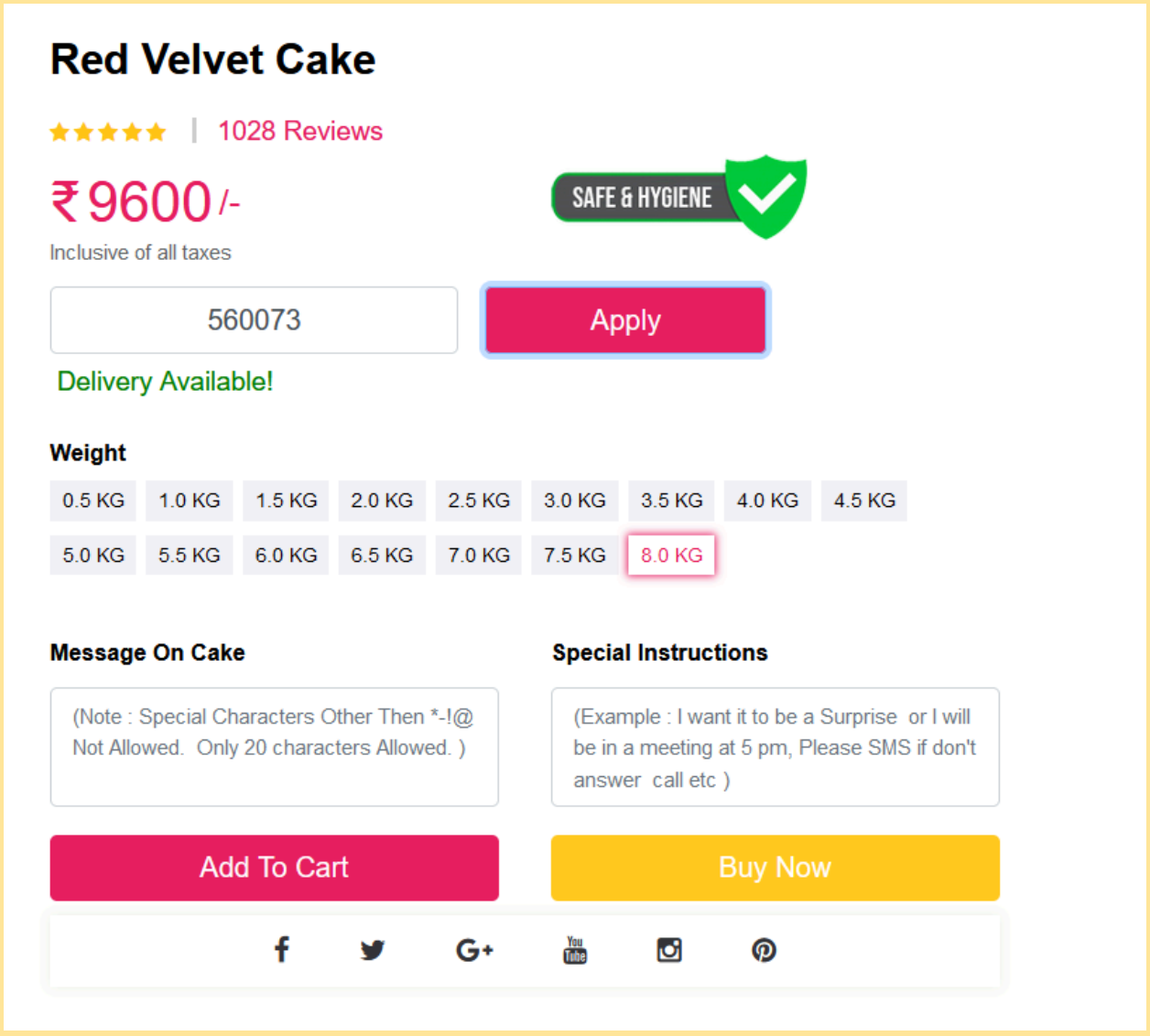


Step 3 : In the Cakes tab we want the expensive cake so go to the premium cake section and select the premium red velvet cake

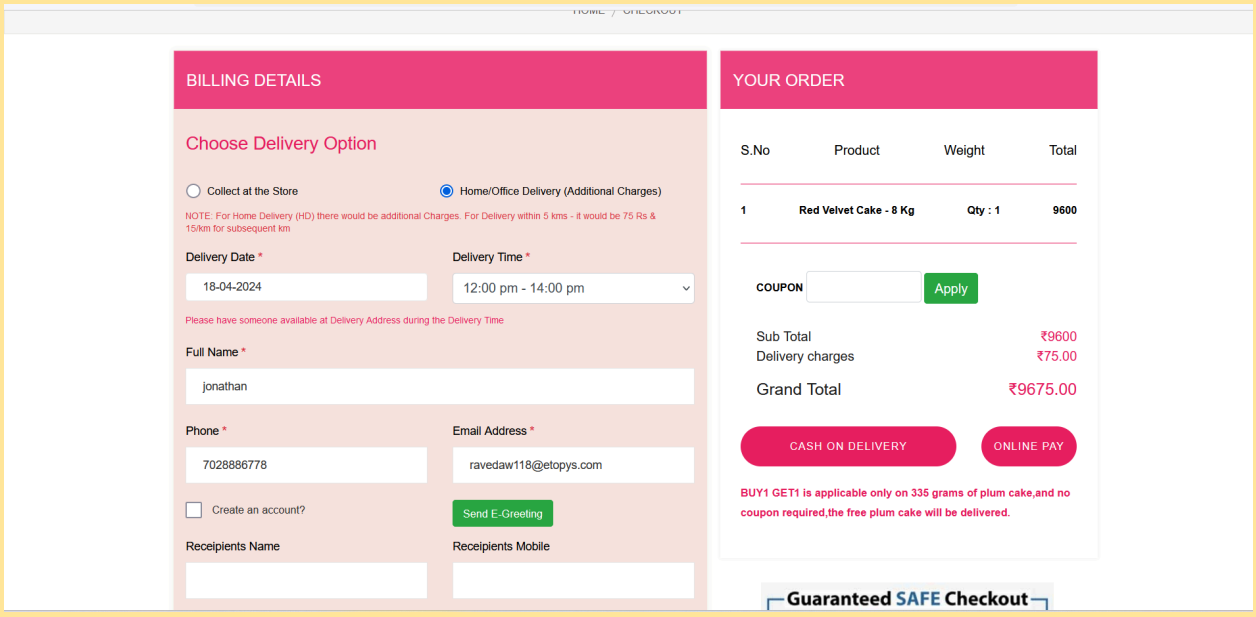




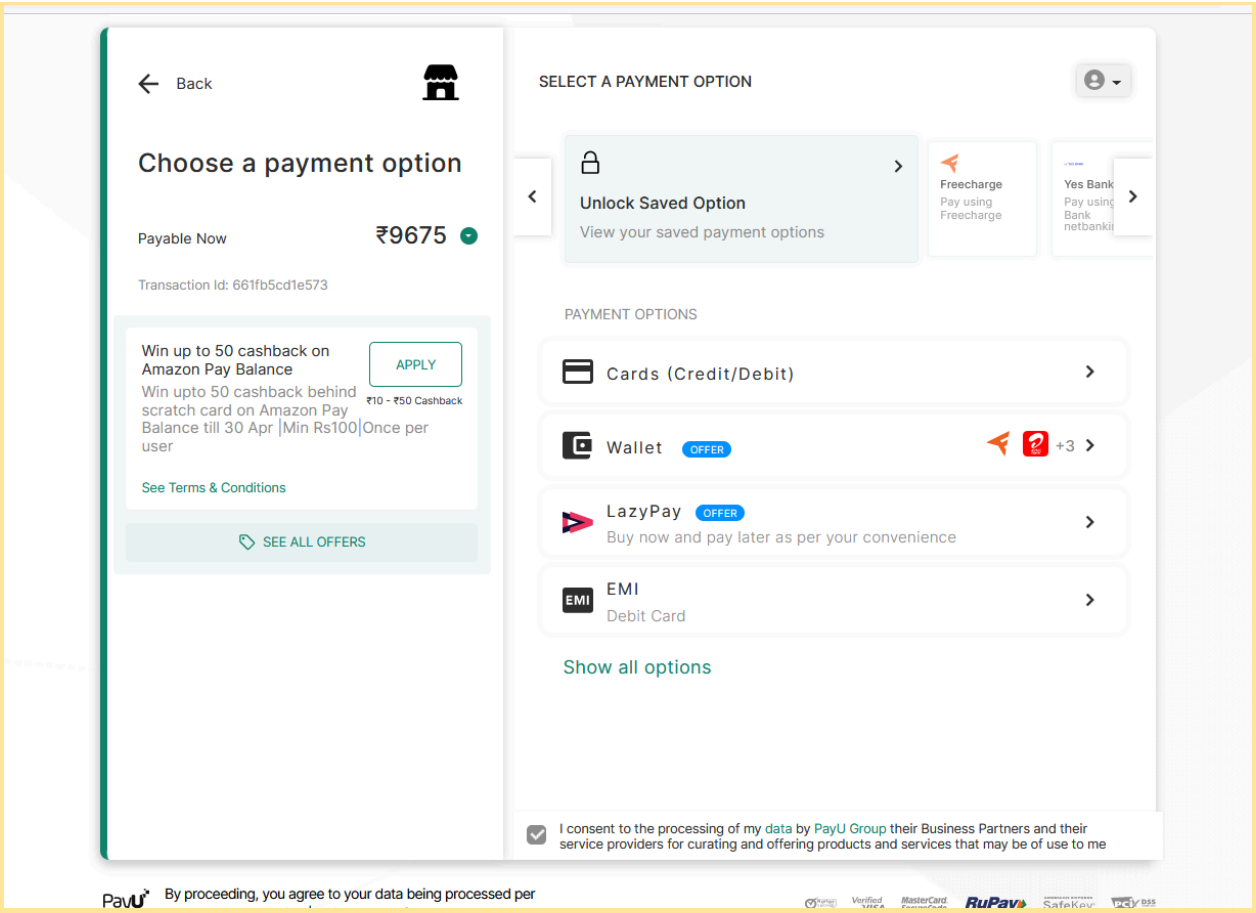
Step 4 : Enter the pincode 560073 for vijayawada in pincode tab and click on apply



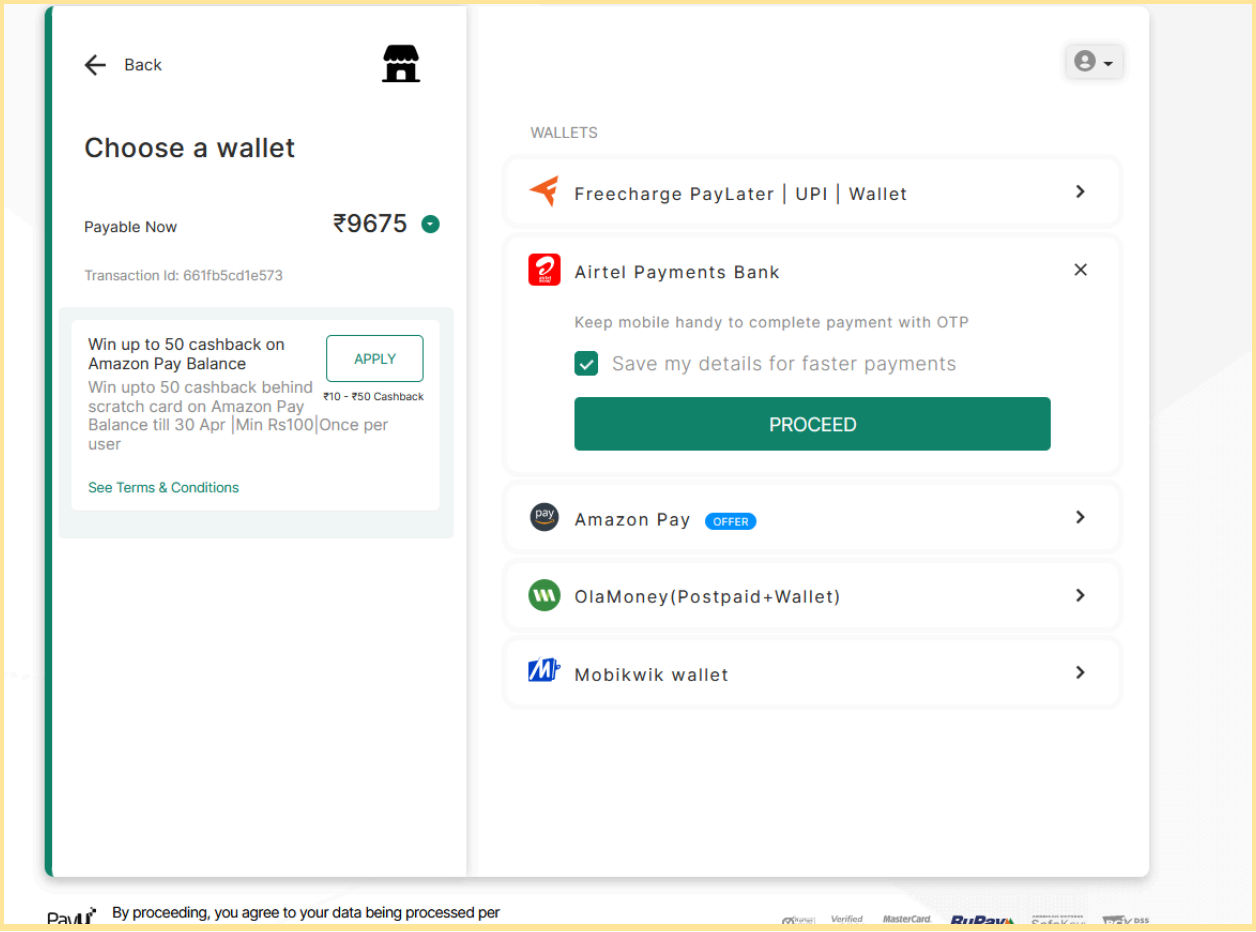
Step 5 : Then click on buy now and give random details about yourself , just put the mobile number real rest everything can be fake



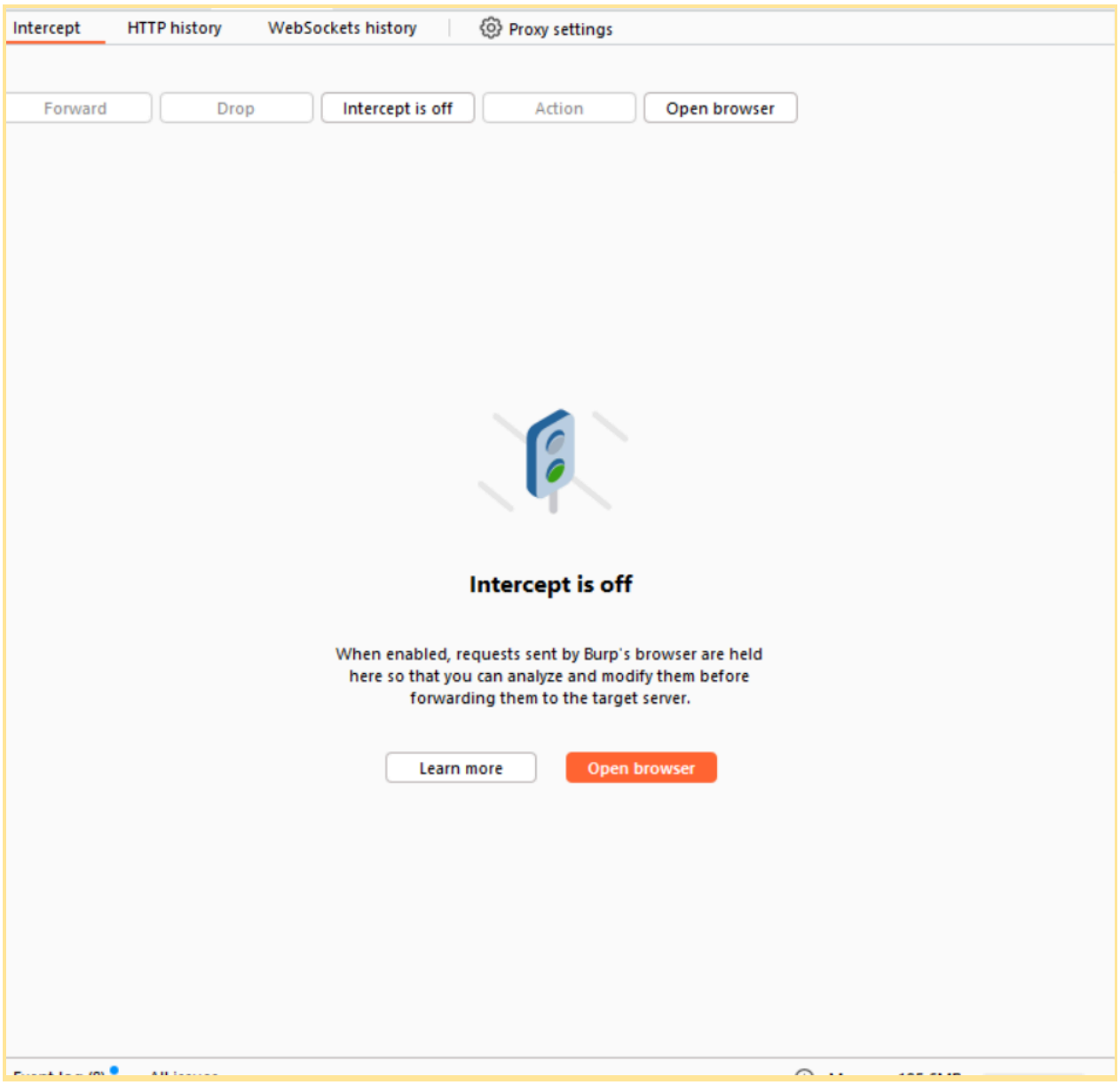
Step 6 : Then click on online pay button and proceed to checkout



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

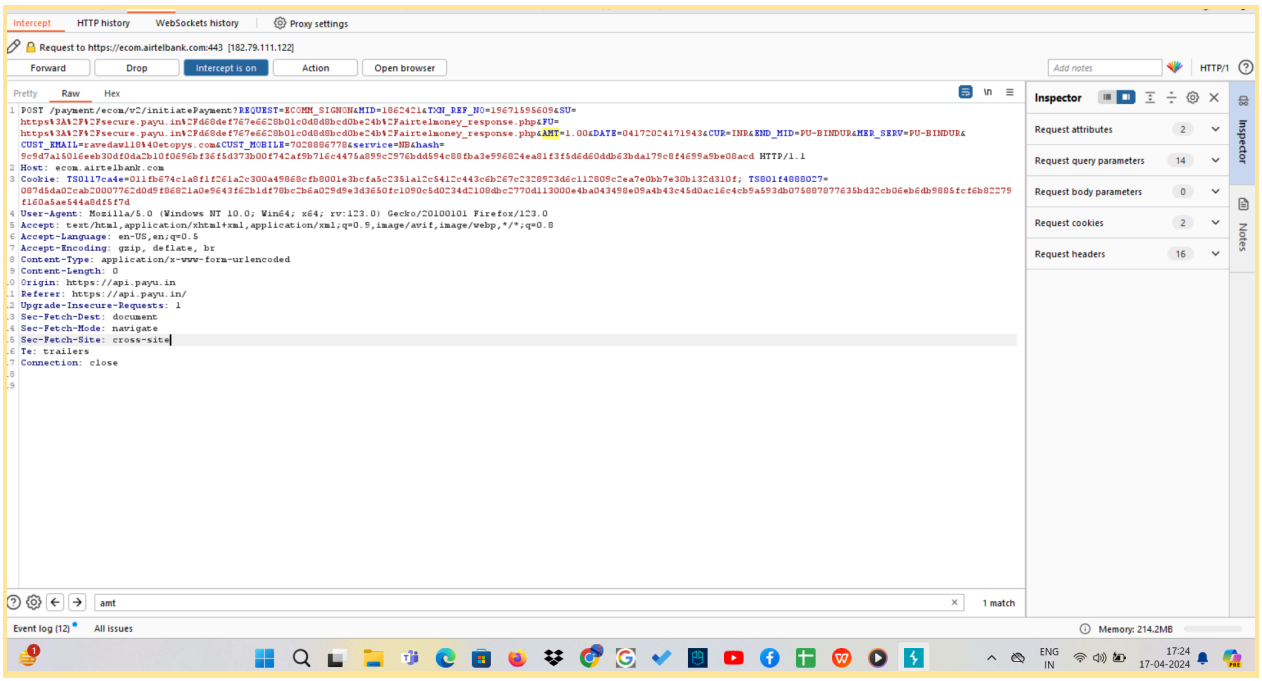


Step 8 : Before clicking on the proceed button , open the burp suite tool and go in the proxy tab and on the intercept and then click on the proceed button

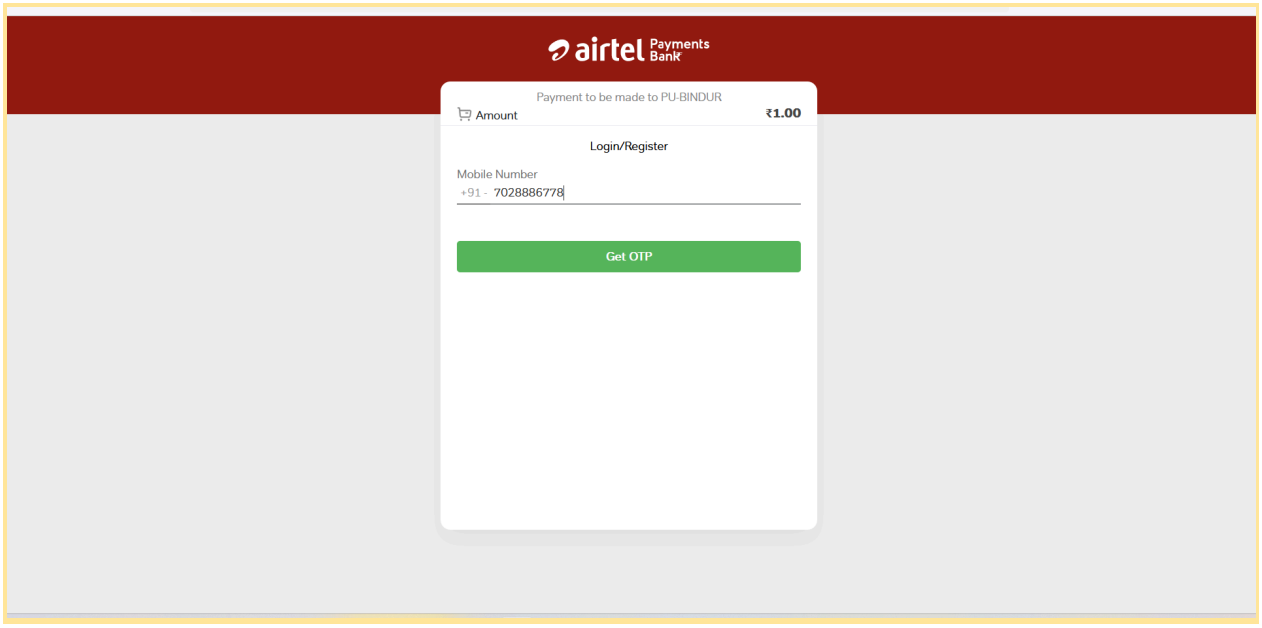


Step 9 : Now in the burp suite tab check for the parameter price or total price or amount or anything that has the value of the item added in the cart, if you dont find keep on forwarding the request

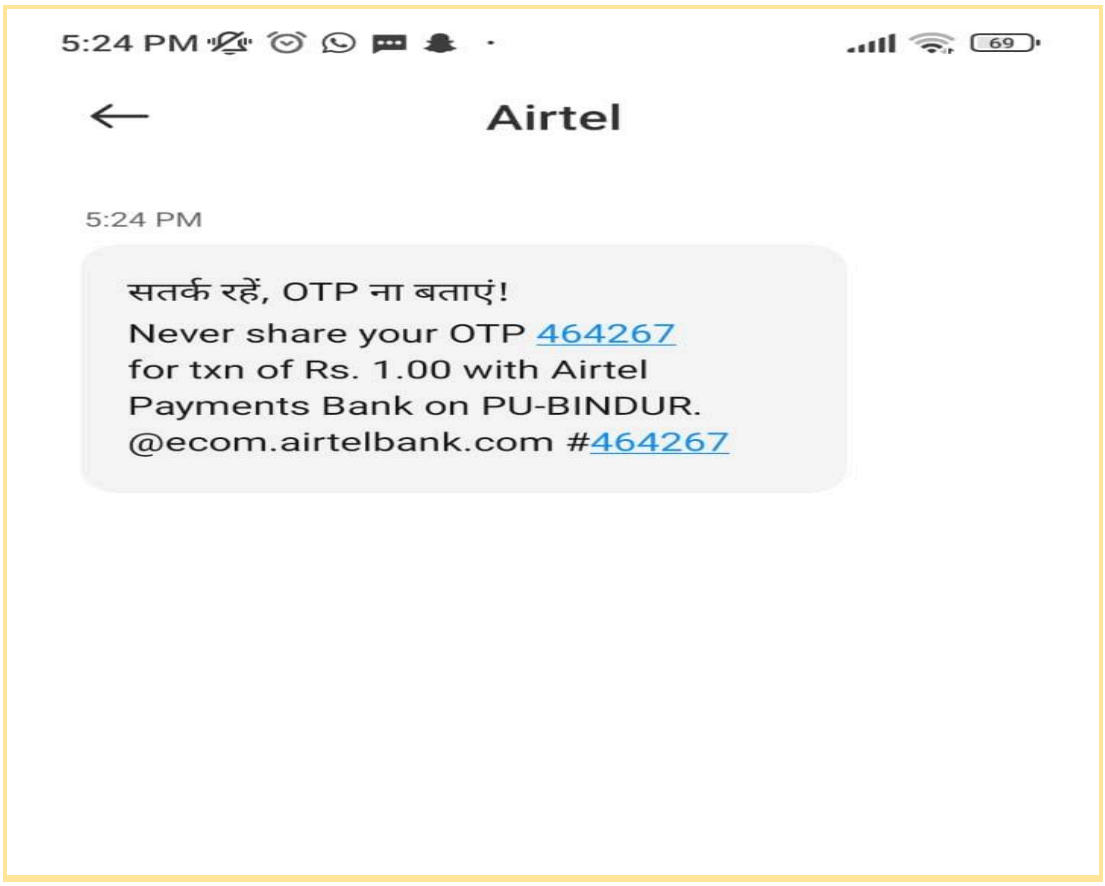
Step 10: Once you find it just click on the price and change it to 1rs and turn off the intercept



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



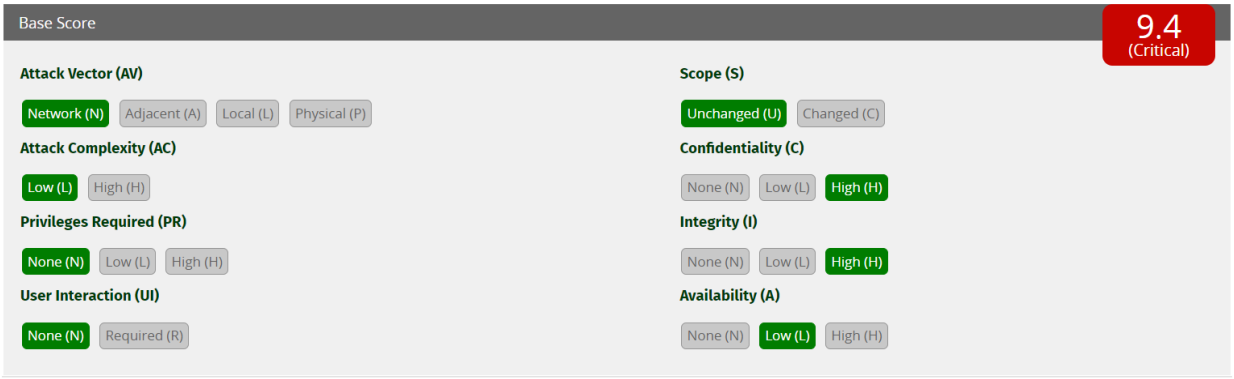
Step 12 : Enter the otp but don’t proceed as it is illegal


5:24 PM
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.

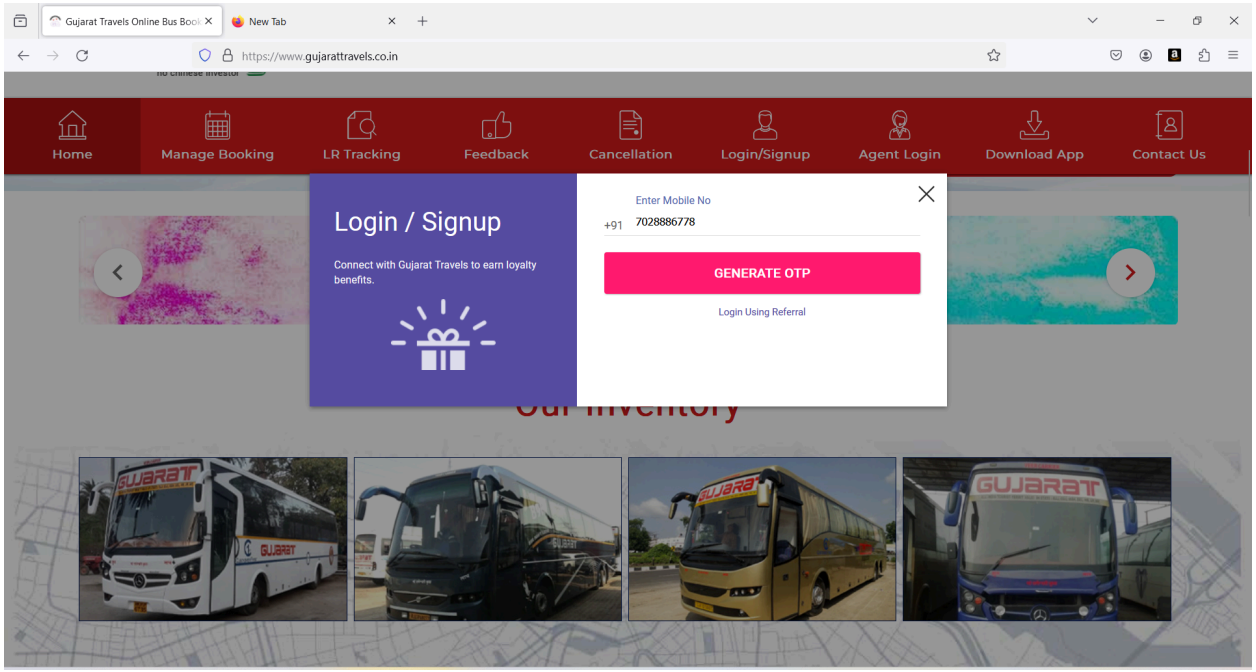
Detailed Explanation:
Upon investigation, it was discovered that relies solely on OTP parameters for authentication without implementing additional security controls. Attackers can exploit this vulnerability by intercepting or modifying requests containing OTP parameters, then replaying or manipulating 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.

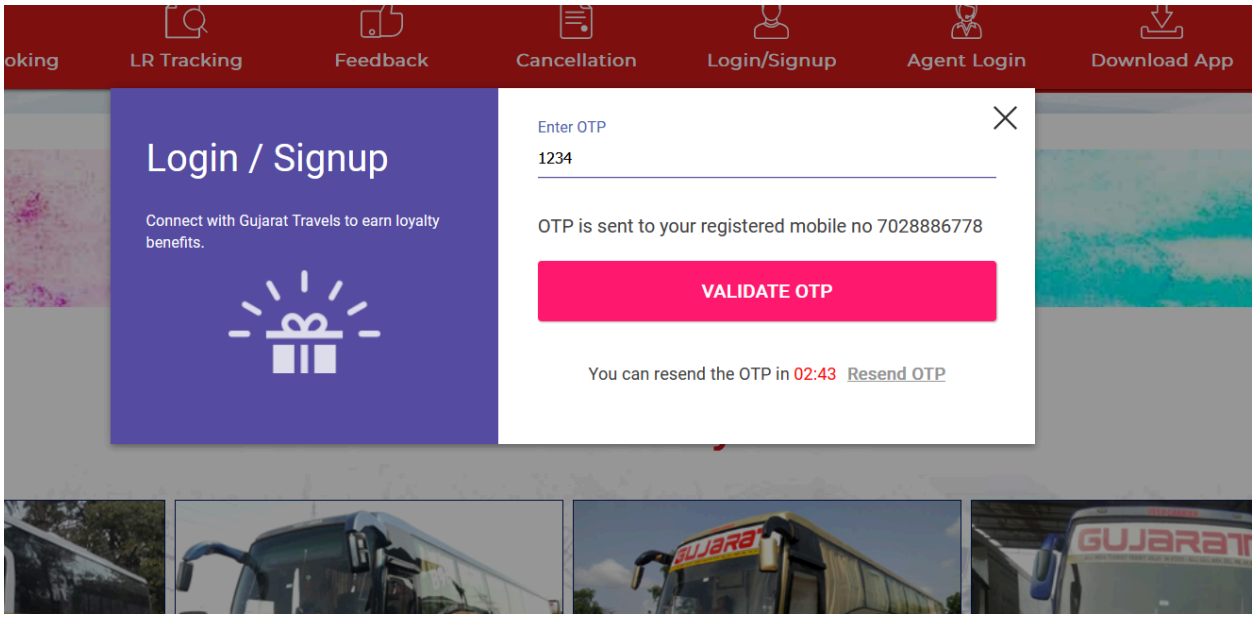
Data Theft: Compromised accounts may contain sensitive data such as personal information, financial details, or confidential documents, which can be stolen or manipulated by attackers.
Identity Theft: Attackers can impersonate legitimate users by accessing their accounts through OTP bypass, leading to 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

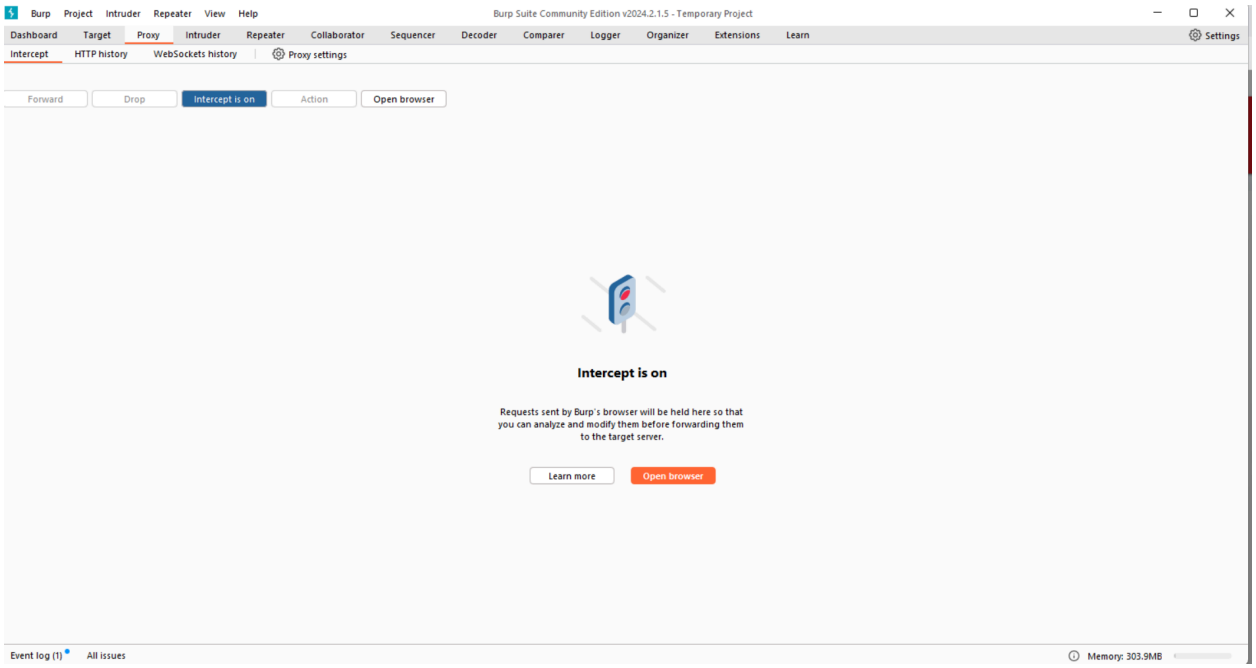
Step 1 : Find a website that has a OTP Login Authentication
Step 2 : Enter your phone number and click on the send otp button



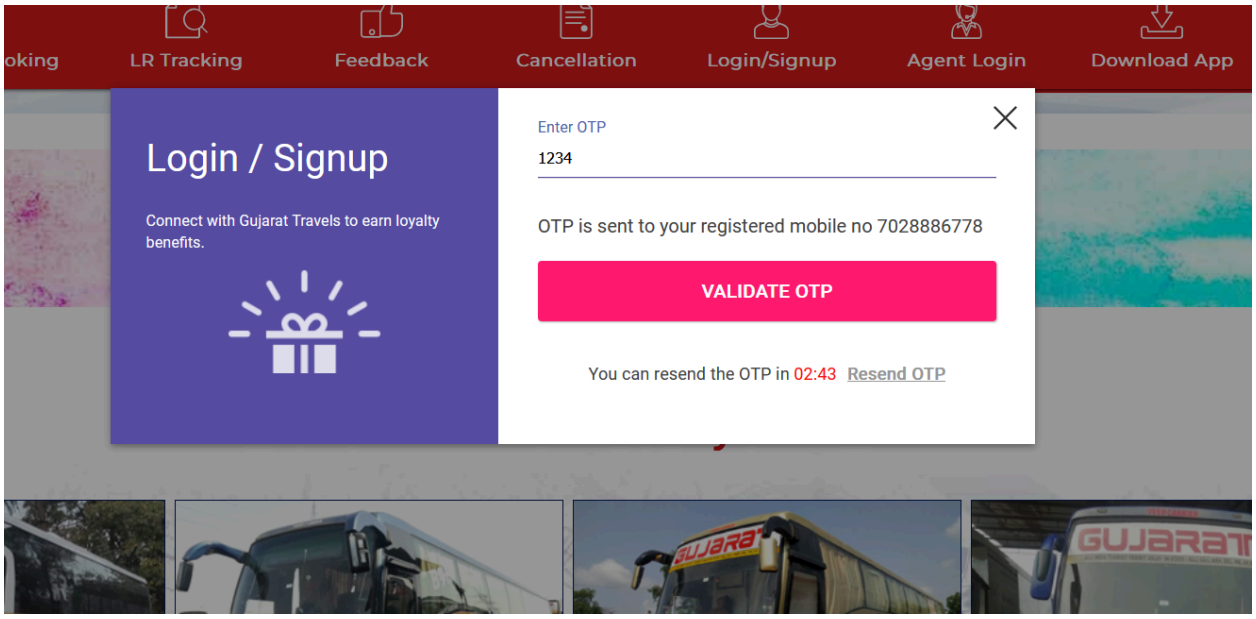
Step 3: Once you have got the otp enter any wrong otp but don't click on validate otp



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

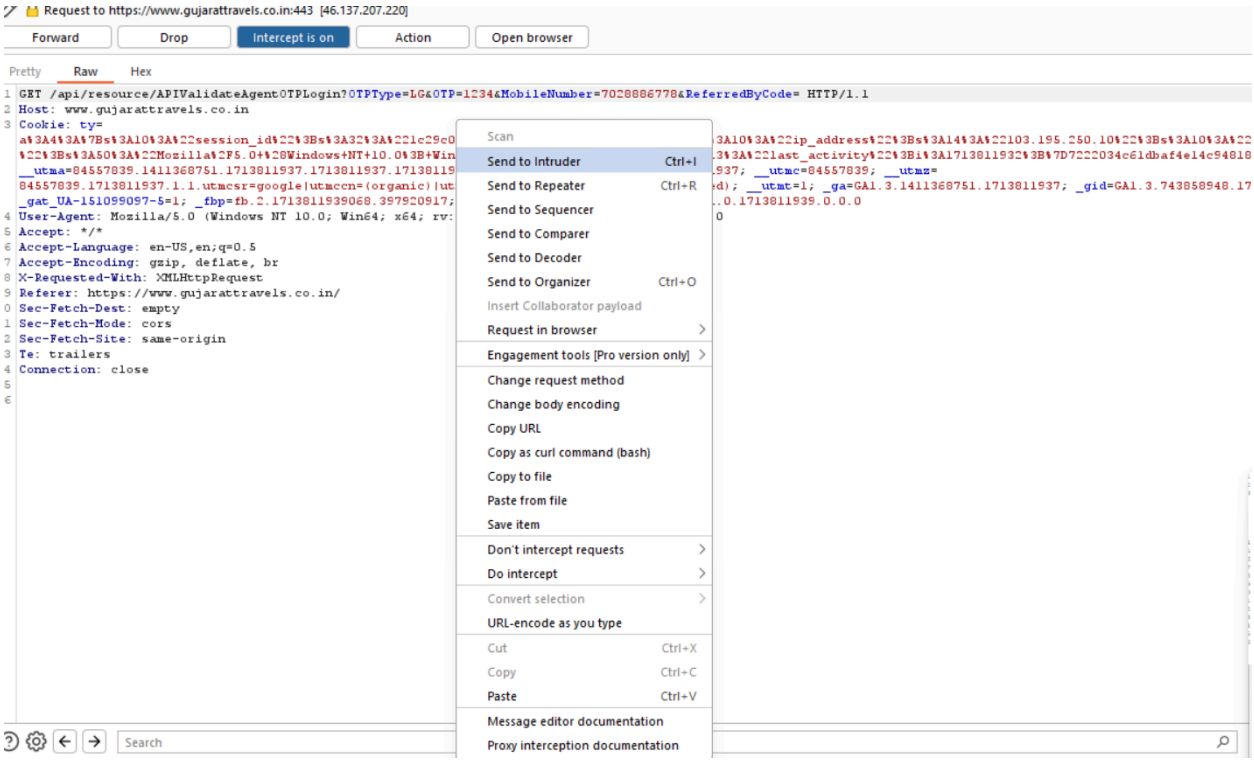


Step 5: Then come back to your website and click on validate otp button, now the request will be captured



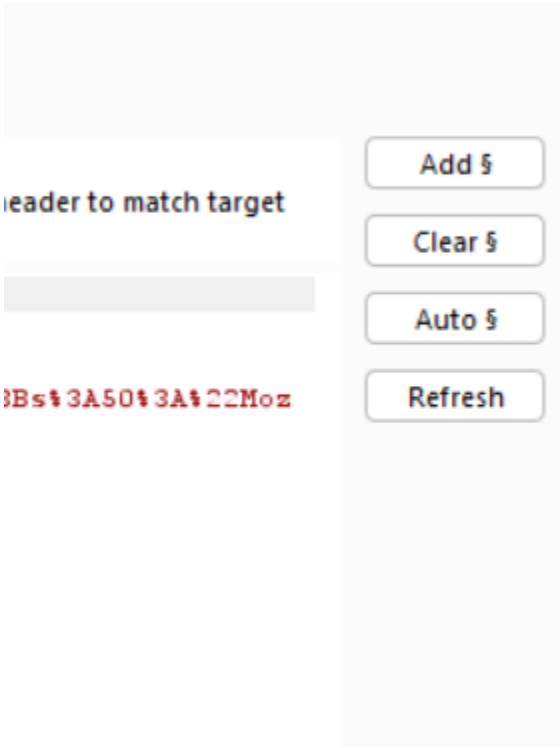
```
GET /api/resource/APIValidateAgentOTPLogin?OTPType=LG&OTP=1234&MobileNumber=7028886778&ReferredByCode= HTTP/1.1
Host: www.gujarattravels.co.in
Cookie: ty=
a%3A4%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%221c29c076de6ecf60dddbf8cb169d67db%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A14%3A%22103.195.250.10%22%3Bs%3A10%3A%22user_agent
%22%3Bs%3A50%3A%22Mozilla%2F5.0+%28Windows+NT+10.0%3B+Win64%3B+x64%3B+rv%3A124.0%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1713811932%3B%7D7222034c61dbaf4e14c9481893e5eaad;
__utma=84557839.1411368751.1713811937.1713811937.1713811937.1; __utmb=84557839.1.10.1713811937; __utmc=84557839; __utmz=
84557839.1713811937.1.1.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided); __utmt=1; _ga=GA1.3.1411368751.1713811937; _gid=GA1.3.743858948.1713811939;
_gat_UA-151099097-5=1; _fbp=fb.2.1713811939068.397920917; _ga_TBSR47F1TS=GS1.3.1713811939.1.0.1713811939.0.0.0
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

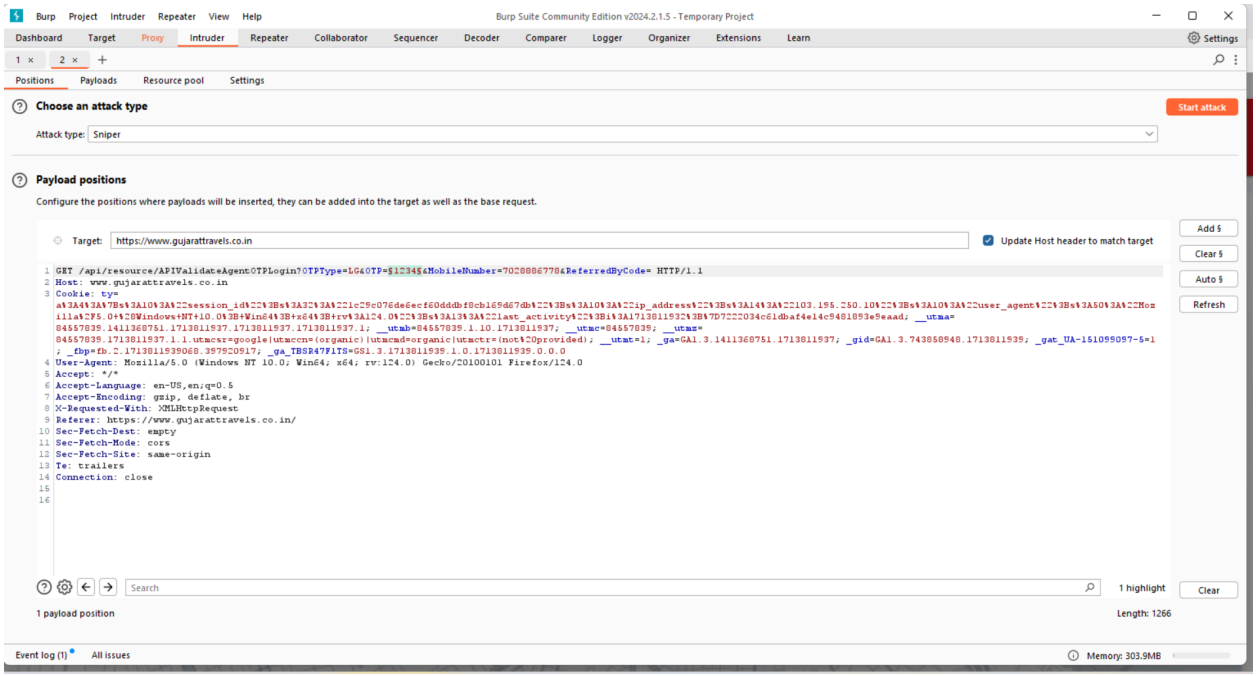


Step 7 : In intruder tab see the request and in proxy tab turn off the intercept

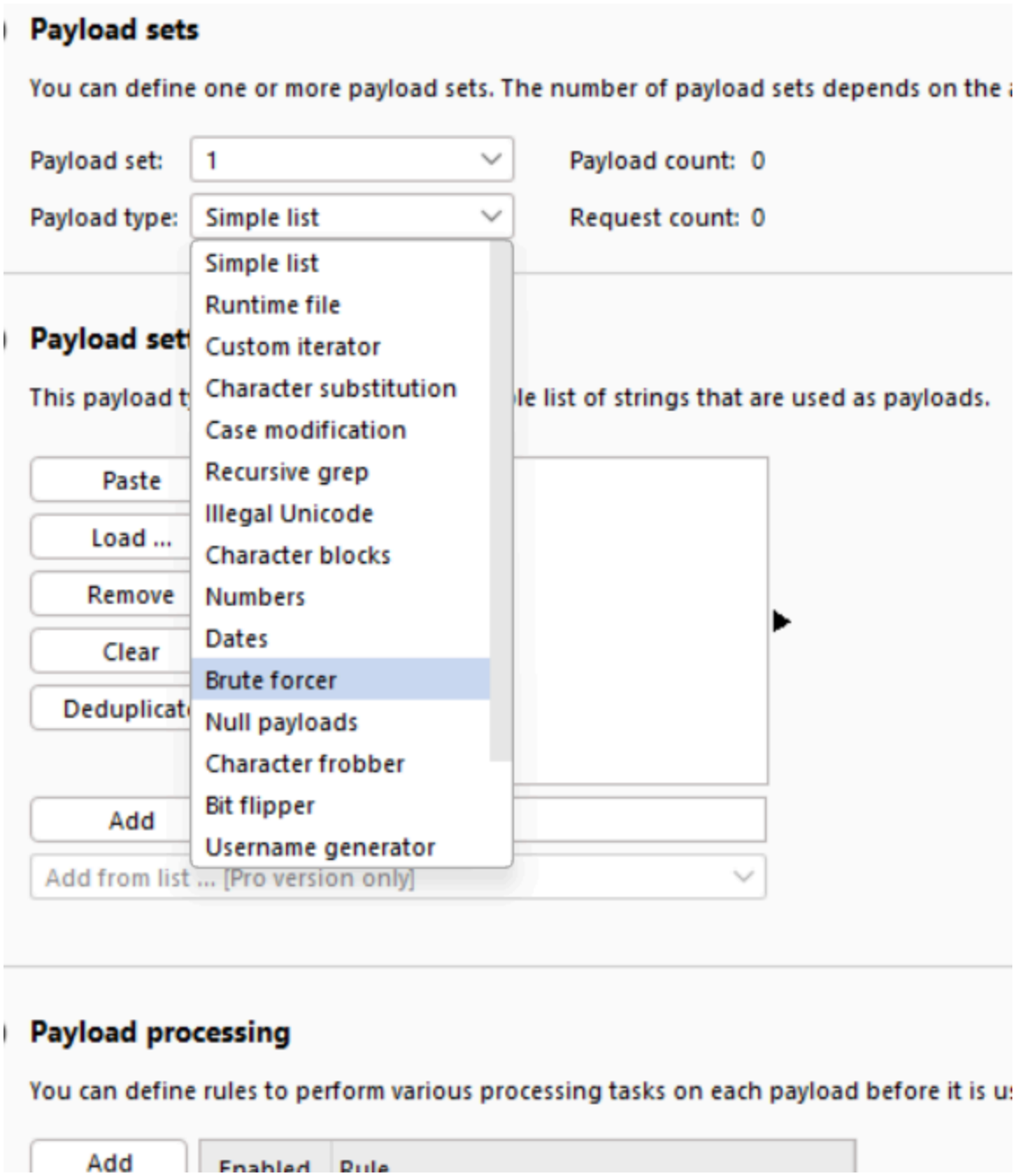
Step 8 : In the intruder tab , on the right hand side there is clear button click on that



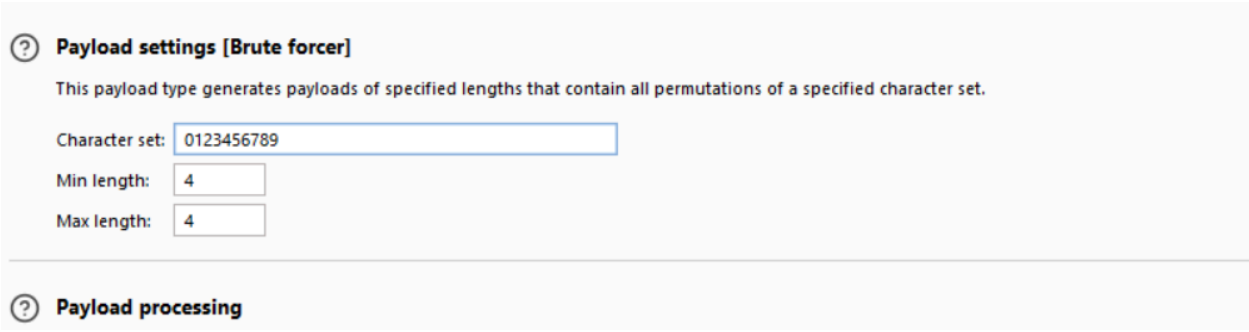
Step 9 : In the intruder tab again , select the otp value (only the value) and on the right hand side there is add button click on that button



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



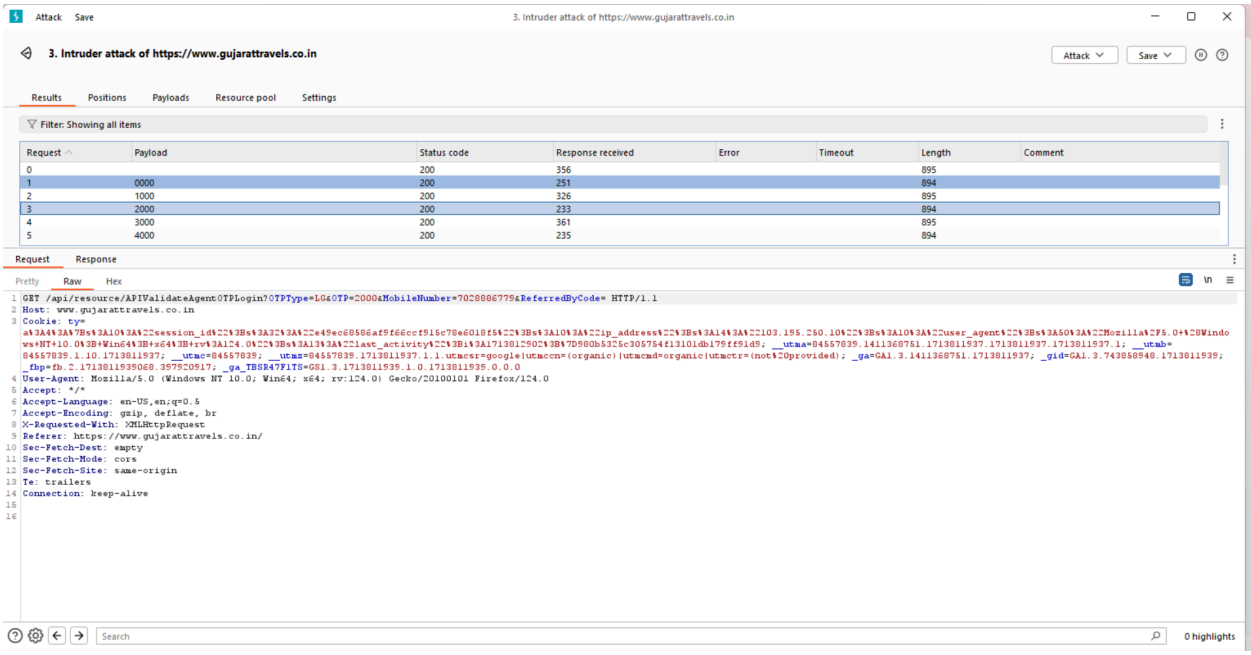
Step 11: Then in the payload setting , we have a character set since the otp value are only numeric we will remove the alphabets and keep the numeric values only



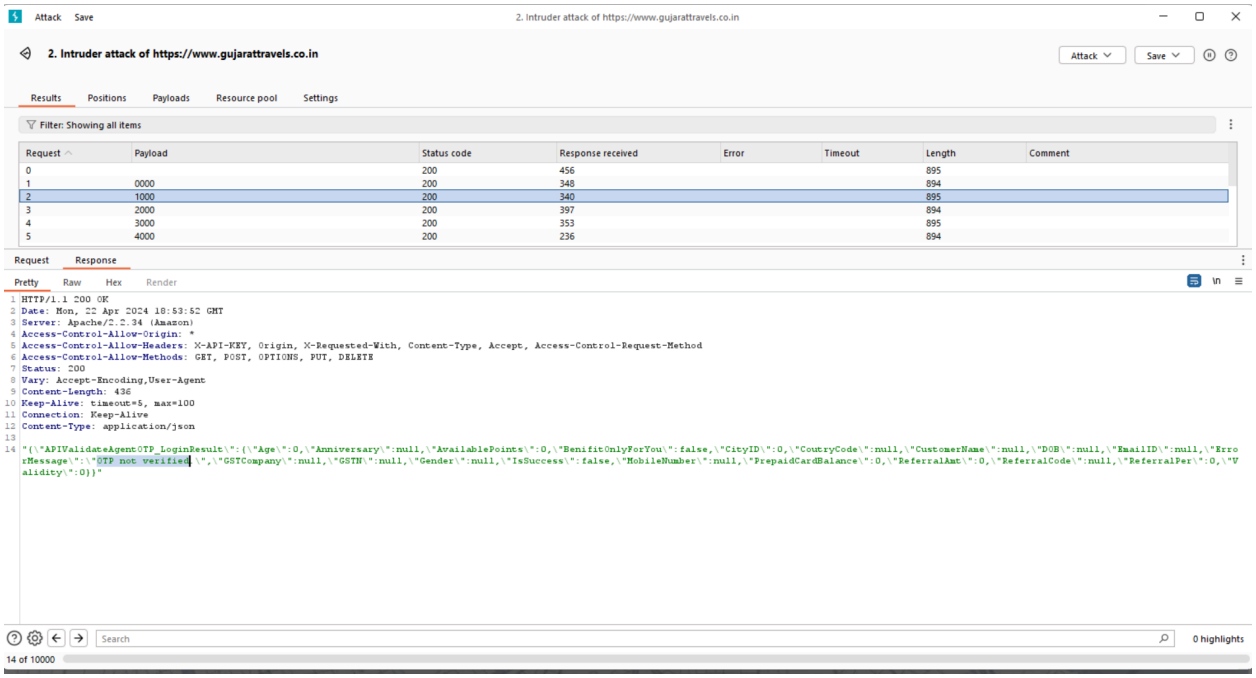
Step 12 : Now once this is done , in the top right corner just click on start attack

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



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
2. Intruder attack of https://www.gujarattravels.co.in
Attack
Save
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
HTTP/1.1 200 OK
Date: Mon, 22 Apr 2024 18:53:52 GMT
Server: Apache/2.2.34 (Amazon)
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-API-KEY, Origin, X-Requested-With, Content-Type, Accept, Access-Control-Request-Method
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE
Status: 200
Vary: Accept-Encoding,User-Agent
Content-Length: 436
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json
"{\"APIValidateAgentOTP_LoginResult\":{\"Age\":0,\"Anniversary\":null,\"AvailablePoints\":0,\"BenifitOnlyForYou\":false,\"CityID\":0,\"CoutryCode\":null,\"CustomerName\":null,\"DOB\":null,\"EmailID\":null,\"ErrorMessage\":\"OTP not verified\",\"GSTCompany\":null,\"GSTN\":null,\"Gender\":null,\"IsSuccess\":false,\"MobileNumber\":null,\"PrepaidCardBalance\":0,\"ReferralAmt\":0,\"ReferralCode\":null,\"ReferralPer\":0,\"Validity\":0}}"
Search
0 highlights
14 of 10000