

NeverLAN CTF

Web : Browser Bias

Value : 150 pts

Difficulty : Easy

Description : Your flag will be in the normal flag{flagGoesHere} syntax.

Attachment : <https://challenges.neverlanctf.com:1130>

Solution :

Going to the website, we see only one message.



Sorry, this site is only optimized for browsers that run on commodore 64

The website expects us to be on Commodore 64. We can't really find a Commodore 64 to obtain the flag, so we'll have to trick the challenge to think we're really on Commodore.

This is what the User-Agent header is for. After searching for 'user-agent' and 'commodore 64', I found that useful github page:

<https://gist.github.com/dstufft/2502524>

The User-Agent we need is 'Contiki/1.0'.

We replace the header, and the website gives us the flag!

Burp Suite Community Edition v2020.1 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 x 2 x 3 x ...

Send Cancel <|>

Target: https://challenges.neverlanctf.com:1130

Request

Raw Params Headers Hex

```
1 GET / HTTP/1.1
2 Host: challenges.neverlanctf.com:1130
3 User-Agent: Contiki/1.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=ia82rhdrehplut1lvv95eo7krn
9 Upgrade-Insecure-Requests: 1
10
11
```

Response

Raw Headers Hex HTML Render

```
1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=UTF-8
3 Date: Mon, 10 Feb 2020 19:34:17 GMT
4 Server: nginx
5 X-Powered-By: PHP/7.2.10
6 Content-Length: 152
7 Connection: close
8
9 <!DOCTYPE html>
10 <html>
11 <head>
12 <title>Browser Bias</title>
13 </head>
14 <body>
15 Welcome fellow c64 user. flag{8b1t_w3b}</body>
16 </html>
17
```

0 matches 0 matches

Done 329 bytes | 375 millis

flag{8b1t_w3b}