Crypto : Cookie Monster

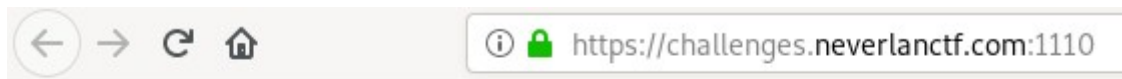Value : 10 pts

Difficulty : Easy

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

Attachment : This website is hiding the flag. You'll need to use your browser's tools to solve the challenge.
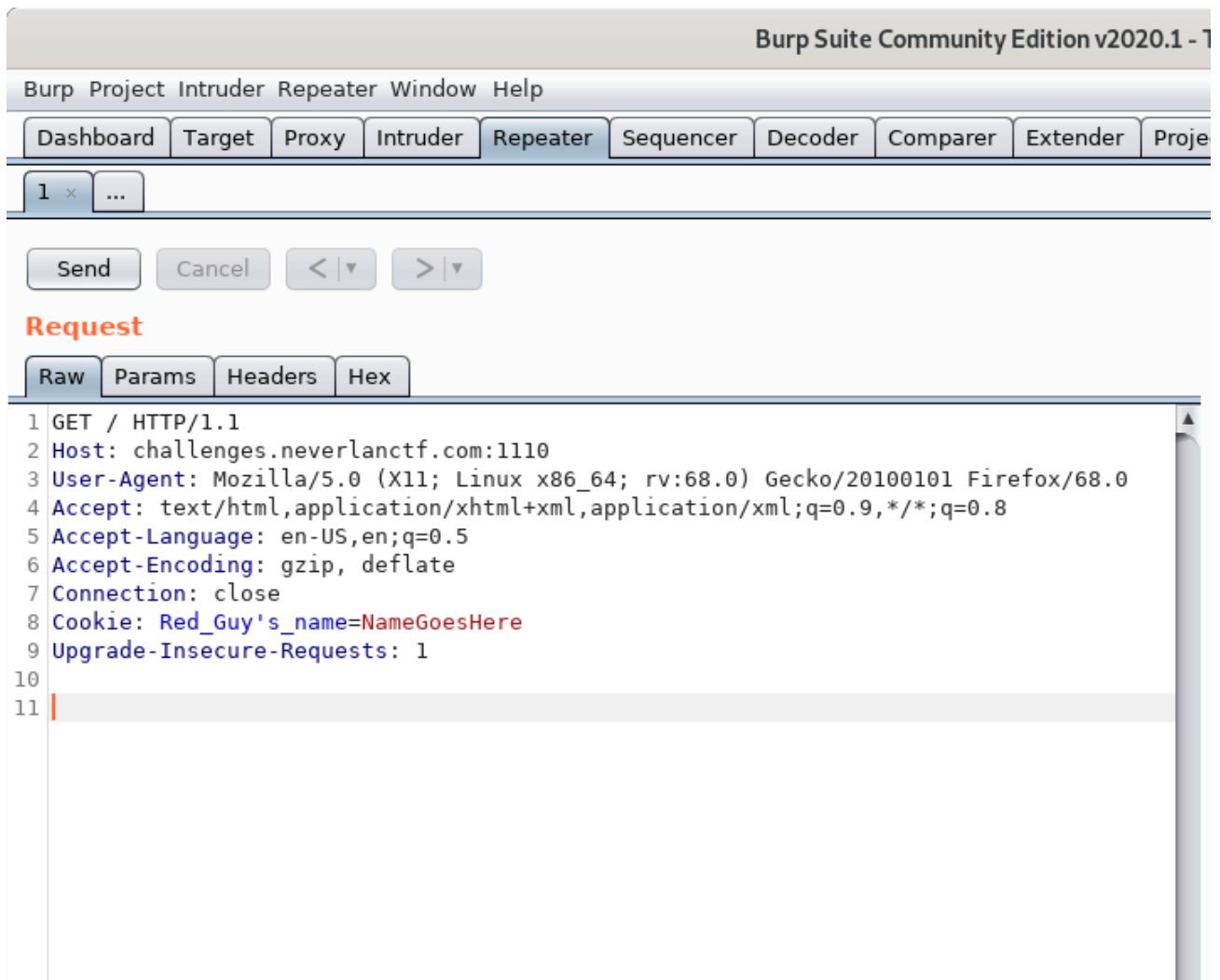
https://challenges.neverlanctf.com:1110

Solution :

When visiting the website for the first time, we can see this sentence and nothing else :

He's my favorite Red guy

With the tool Burp Suite, we can see an other hint :

So it seems that we need to guess this cookie's value, and that it's the name of a red guy. The name of the challenge is 'Cookie Monster'.

By searching 'Cookie monster' and 'red guy' on Google, we can find a name : Elmo, a red guy of the Muppets show.

With the value of 'Elmo' for this cookie, we get the flag!

Burp Project Intruder Repeater Window Help

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

1 × ...

Send   Cancel   < |▼   > |▼   Target: https://challenges.neverlanctf.com:1110 ✎

Request

Raw | Params | Headers | Hex

```
1 GET / HTTP/1.1
2 Host: challenges.neverlanctf.com:1110
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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: Red_Guy's_name=Elmo
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 19:26:26 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>Cookie_monster</title>
13   </head>
14   <body>
15    <p>You got it! flag{YummyC00k13s}</p></body>
16 </html>
17
```