**Pirate’s Hidden Treasure**

***Web***

**Challenge:**

A legendary treasure chest, rumored to be enchanted by Captain Jack Sparrow himself, awaits your discovery. But beware, for only those with the heart of a true pirate, much like Captain Jack, shall unlock its secrets and claim the treasure within.

https://questcon-pirate-treasure.chals.io/

**Approach:**

This was an interesting challenge, wherein there were three levels of authentication required to access the “hidden treasure” (the flag lol).

The first two were not that difficult but the last one it took me hours to solve (just because i was being dumb)

For the first level the website gives us the text:

You should have a pirate browser to access this site!

Hmmm, it’s a web challenge so something to do with the http request? We set the header:

User-Agent: pirate browser

and send the request again, boom! We see a different text now:

You should come from the ship Black Perl to access this treasure!

So the http header modification works, i guess it’ll work for this one too?

Referer: Black Perl

This worked as well, we now get the text to identify ourself? We notice there’s a cookie set:

user=barbossa

What if we have to change the user to the required use to authenticate?

According to the question it should be something similar to Captain Jack Sparrow or something.

I tried putting all combinations and wasted hours figuring out what it could possibly be, just to find it later and realize, that i wasn’t using all lowercase in the user cookie :))

We set the cookie user=captain jack

…and get our flag:

**Flag: QUESTCON{Thr33\_k33p\_a\_s3cr3t\_if\_2\_of\_th3m\_ar3\_dead}**

It can also be done by using curl with the command:

curl -H "User-Agent: pirate browser" -H "Referer: Black Perl" -H "Cookie: user=jack sparrow" https://questcon-pirate-treasure.chals.io/

Congrats!!

Happy Hacking!