PicoCTF Who are you? 100 points

http://mercury.picoctf.net:34588/

For reference to all Headers: https://developer.mozilla.org/fr/docs/Web/HTTP/Headers

We get a gif and a message stating: Only people who use the official PicoBrowser are allowed on this site!

Graphical user interface, application, PowerPoint

Description automatically generated

In order to tell the website we are using PicoBrowser we can simply change our browser header, in order to do this you can use a program like BurpSuite but currently I feel more comfortable using: <https://reqbin.com/>.

Inside of the browser I’ll set the User agent to PicoBrowser and press forward: Graphical user interface, application

Description automatically generated

Next up we get prompted “I don't trust users visiting from another site.” Indicating the website can see that we came from somewhere else that isn’t this site. To change this you can say that the referer is this website by simply writing: Referer: <http://mercury.picoctf.net:34588/>

Graphical user interface, application

Description automatically generated

Now we get prompted “Sorry, this site only worked in 2018.” So we can simply change the date to something like: Date: Wed, 14 Nov 2018 11:49:00 GMT

Graphical user interface, application

Description automatically generated

Almost there!: “I don't trust users who can be tracked.” For this we can use DNT, this stands for “Do Not Track”, its default value is 0 but we can put this to 1 to enable it!

Graphical user interface, application, Word

Description automatically generated

Only people in Sweeden, for this we can use X-Forwarded-For: 23.92.112.0 for this, I got the IP by basically googling:

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, application

Description automatically generated

Next we get prompted: “You're in Sweden but you don't speak Swedish?”. So we have to give our language, for sweeden we can put in the header: Accept-Language: sv

I found sv by looking up sweeden language code:

Graphical user interface, text, application, email

Description automatically generated

And so we got to the end!

Graphical user interface, application, Word

Description automatically generated

picoCTF{http\_h34d3rs\_v3ry\_c0Ol\_much\_w0w\_79e451a7}