PicoCTF Its my birthday 100 points

<http://mercury.picoctf.net:48746/>

For this one you’ll need to upload 2 identical PDF’s to the website in order to be accepted.

As instructed in another writeup I’ll use Curl in order to upload the files, I could just drag & drop them but as my main goal is learning I’ll follow his lead!

First of all we can try to just upload the same file and see if it works:

A screenshot of a computer

Description automatically generated with medium confidence

So Ofcorse it says that it is not a PDF but I also believe its important to figure out what -F does.

Using man curl and inside the man page / -F and ‘n’ to navigate I found that. -F is used to emulate a filled-in form in which a user has pressed the submit button. In the HTML a “file1”, “file2” and “Upload“ value was given which we used to send our curl command!

Lets try out sending in PDF’s now!:

Graphical user interface, text, application

Description automatically generated with medium confidence

As I send 2 identical files it noticed that, which is wrong!

In the explanation MD5 hashes where mentioned and its pretty clear is has to do with a known PHP gotcha where if you compare 2 strings of the form 0e[\d]+, when compared with == they are considered equal as they both equal to 0! Using a more nerd friendly notation:

'0e1' == '00e2' == '0'

We can check this exploit in the cmd:

Text

Description automatically generated

Php echo’s 2 different md5 hashes and when checking if both are equal to each other the bool gives back true due to it starting with 0e, when adding a 3th one too the mix you can clearly see the difference at the start!

Text

Description automatically generated

So now we can create our 2 pdf files using these 2 magic values and upload these into the website!

A screenshot of a computer

Description automatically generated

This solution has some hidden gems I really like!

First is Ofcorse once again the values used for the MD5 which we went over. -n behind echo is used to not create a trailing new line.

Md5sum is used to simply display the md5 hashes

And the last command the curl command is also fairly simple.  
We already know about -F and -s | egrep -o "picoCTF{[^}]+}" is new.

-s is used to not show a progress meter when executing a curl command.

When you do this command you get the entire html from the website which we do not want! Knowing this we could actually just cast the html in a txt file and look it up like this:

Text

Description automatically generated

But that’s not cool or professional enough!

Instead we will take the output: The whole bunch of html above and execute egrep on it, what egrep does is: it searches for patterns in each file or whatever you put in and prints each line that has this pattern. -o stands for only matching, which will only print back the things matching what you put in! In this case it is looking for something that starts with PicoCTF{ and ends with }.

To clarify I made another version, this time where it starts with PicoCTF but ends with ‘u’

