

It is my Birthday picoCTF

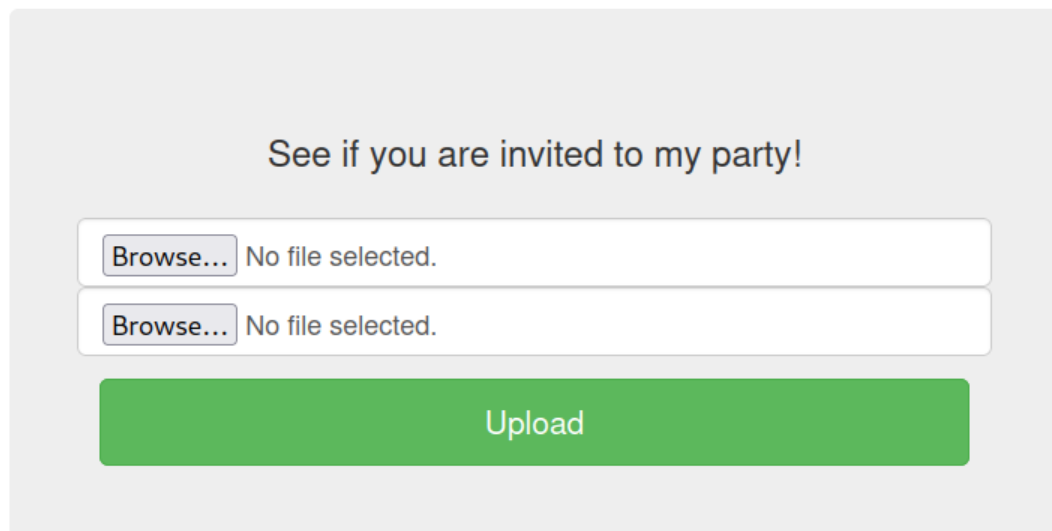
AUTHOR: MADSTACKS

Description

I sent out 2 invitations to all of my friends for my birthday! I'll know if they get stolen because the two invites look similar, and they even have the same md5 hash, but they are slightly different! You wouldn't believe how long it took me to find a collision. Anyway, see if you're invited by submitting 2 PDFs to my website. <http://mercury.picoctf.net:50970/>

To start I read through the description and saw the mentioning of md5 hash and mentioning of 2 PDFs. As I continued to the website I saw that there are just options to upload 2 PDFs and nothing else.

It is my Birthday



See if you are invited to my party!

No file selected.

No file selected.

From the instructions we can see that we need to create a collision using the pdfs to break the md5 collision. To get the pdf executables I found a website <https://www.mscs.dal.ca/~selinger/md5collision/> which gave me a pair of executables that I can change to pdfs to insert into the website.

After downloading the .exe files I converted them into PDFs and inserted them into the website.

See if you are invited to my party!

Browse... hello.pdf

Browse... erase.pdf

Upload

This gave me the flag `picoCTF{c0ngr4ts_u_r_1nv1t3d_73b0c8ad}`