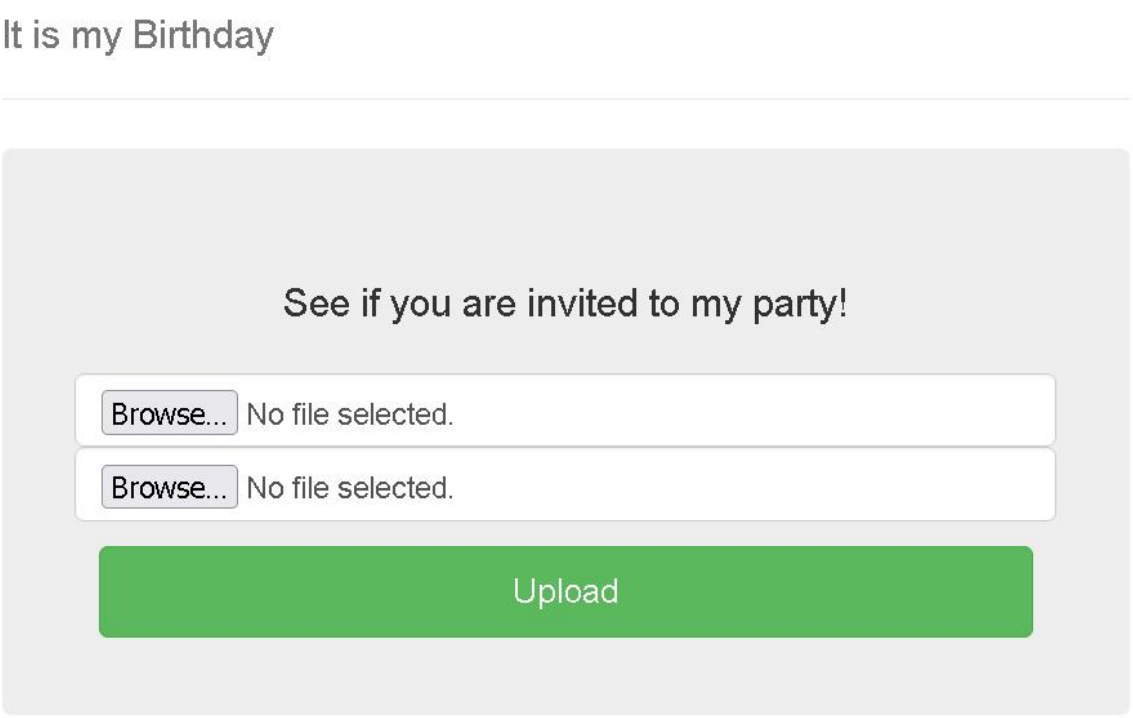
PicoCTF - dont-use-client-side Writeup

Open (http://mercury.picoctf.net:57247) in Firefox.



Since the problem mentioned something about MD5 collision. So I searched it on Google.
I found a website discussed about MD5 collision.
(https://www.mathstat.dal.ca/~selinger/md5collision/)

- **Windows version:**
  - hello.exe. MD5 Sum: cdc47d670159eef60916ca03a9d4a007
  - erase.exe. MD5 Sum: cdc47d670159eef60916ca03a9d4a007
- **Linux version (i386):**
  - hello. MD5 Sum: da5c61e1edc0f18337e46418e48c1290
  - erase. MD5 Sum: da5c61e1edc0f18337e46418e48c1290

Downloaded both files in Windows version (if you are using Linux, then download the matching version). Rename the extension into PDF. Submit both files into the page.

Instead of complains about file too large or MD5 hash do not match. We got the PHP script exposed instead.

```php
<?php

if (isset($_POST["submit"])) {
    $type1 = $_FILES["file1"]["type"];
    $type2 = $_FILES["file2"]["type"];
    $size1 = $_FILES["file1"]["size"];
    $size2 = $_FILES["file2"]["size"];
    $SIZE_LIMIT = 18 * 1024;

    if (($size1 < $SIZE_LIMIT) && ($size2 < $SIZE_LIMIT)) {
        if (($type1 == "application/pdf") && ($type2 == "application/pdf")) {
            $contents1 = file_get_contents($_FILES["file1"]["tmp_name"]);
            $contents2 = file_get_contents($_FILES["file2"]["tmp_name"]);

            if ($contents1 != $contents2) {
                if (md5_file($_FILES["file1"]["tmp_name"]) == md5_file($_FILES[
                    highlight_file("index.php");
                    die();
                } else {
                    echo "MD5 hashes do not match!";
                    die();
                }
            } else {
                echo "Files are not different!";
                die();
            }
        } else {
            echo "Not a PDF!";
            die();
        }
    } else {
        echo "File too large!";
        die();
    }
}

// FLAG: picoCTF{c0ngr4ts_u_r_1nv1t3d_40d81ca2}
```

The flag is revealed in the PHP script. Hurray!
Flag: picoCTF{c0ngr4ts_u_r_1nv1t3d_40d81ca2}