New issue

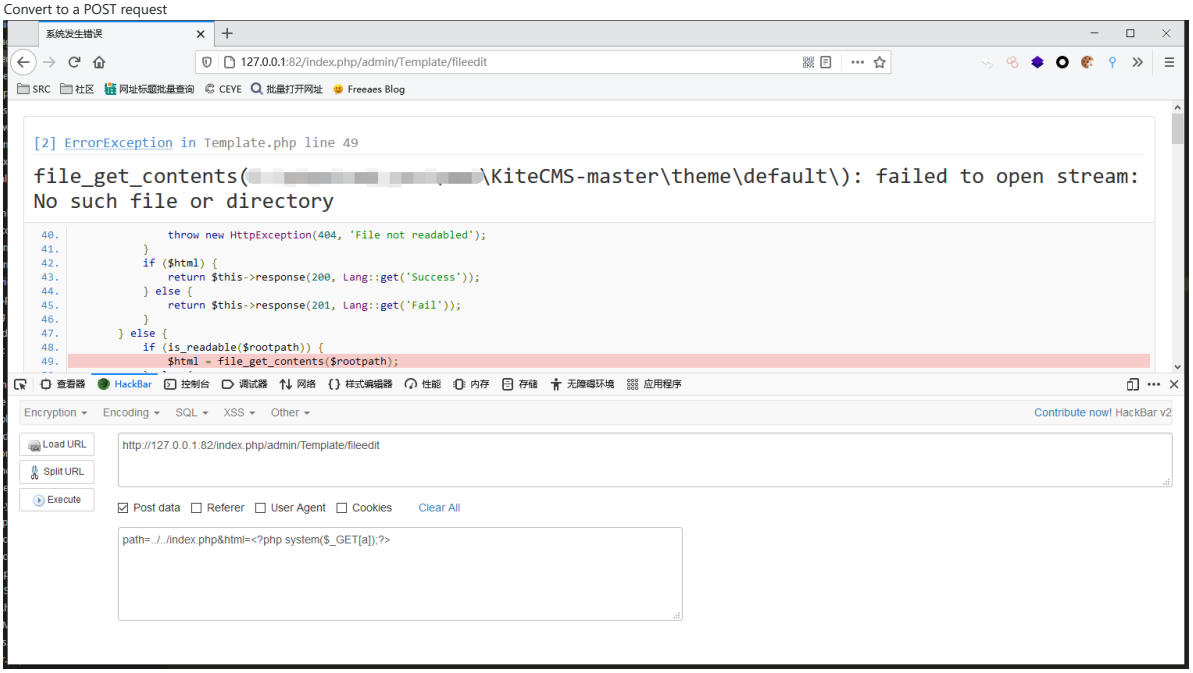
Jump to bottom

Code execution vulnerability causes RCE #9

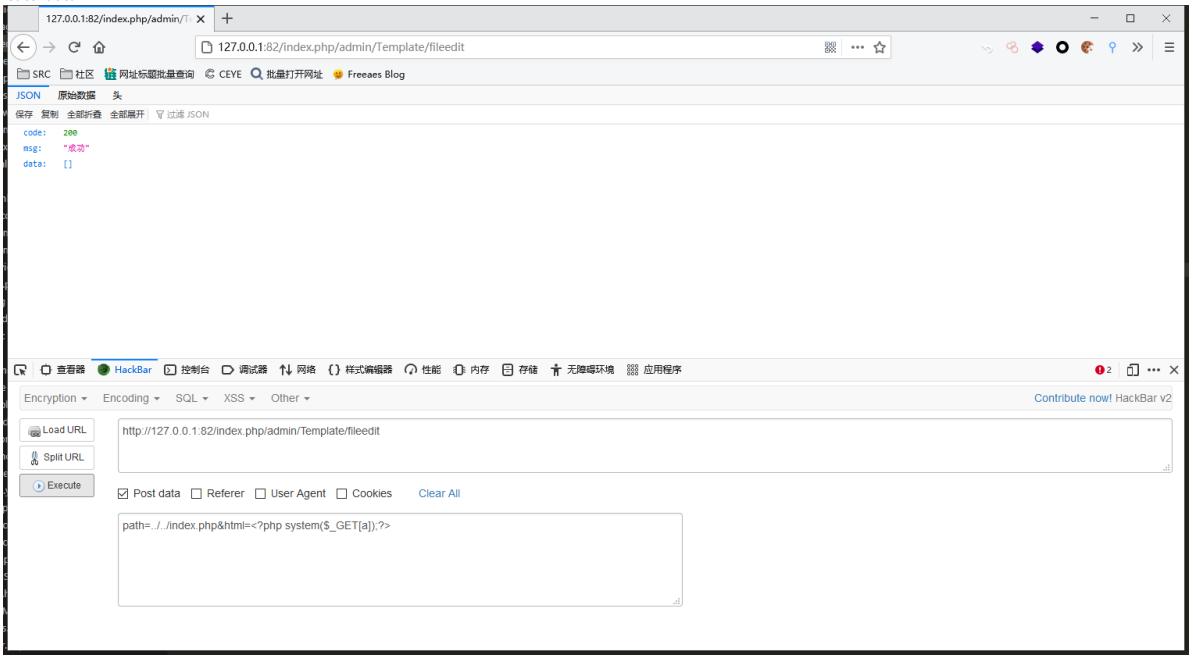
Open **catw0rld** opened this issue on Apr 21, 2021 · 0 comments

catw0rld commented on Apr 21, 2021 • edited

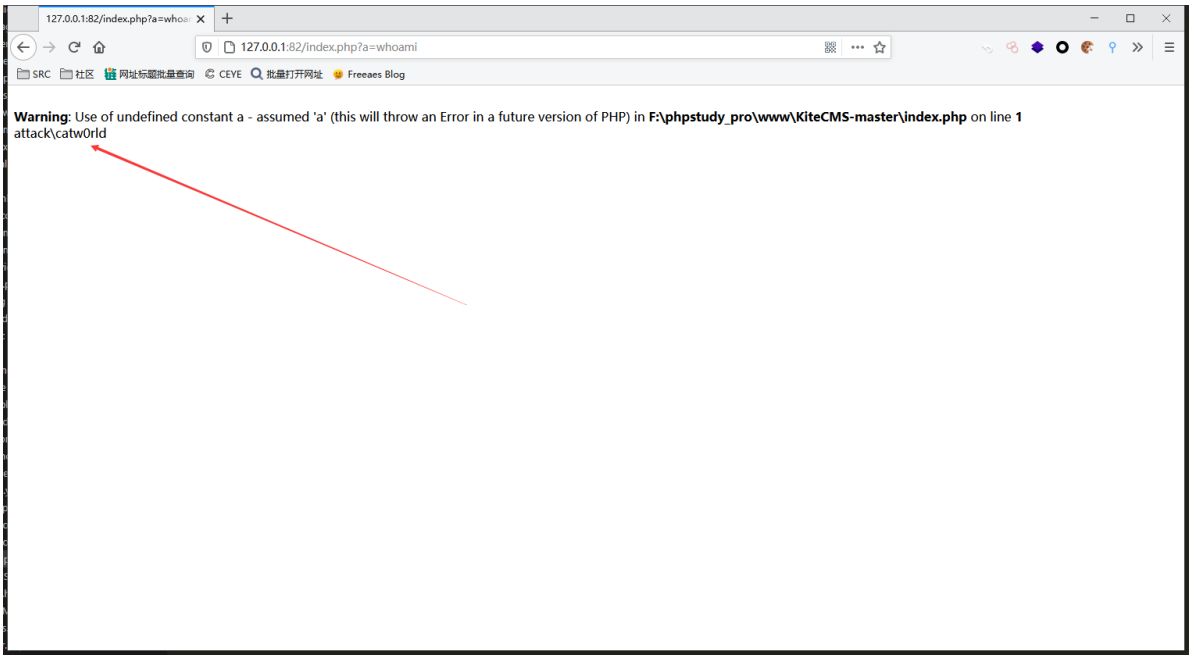
1. log into the background of the site
   url: /index.php/admin/passport/login.html
2. Add vulnerability URL
   url: /index.php/admin/Template/fileedit
   Convert to a POST request



let contract



3. Access index.php generated in the root directory
   url: /index.php?a=whoami



Code audit

The vulnerability file is located at: /application/admin/controller/Template.php -> fileedit()

Template.php

application > admin > controller > Template.php > Template > fileedit

```
20          ];
21
22          return $this->fetch('filelist', $data);
23      }
24
25      public function fileedit()
26      {
27          $path = Request::param('path');
28          $siteObj = new Site;
29          $template = $siteObj->where('id', $this->site_id)->value('theme');
30          $rootpath = Env::get('root_path') . 'theme' . DIRECTORY_SEPARATOR . $template . DIRECTORY_SEPARATOR . $path;
31          // 判断文件是否存在
32          if (!file_exists($rootpath) && !preg_match("/theme/", $rootpath)) {
33              throw new HttpException(404, 'This is not file');
34          }
35
36          if (Request::isPost()) {
37              if (is_writable($rootpath)) {
38                  $html = file_put_contents($rootpath, htmlspecialchars_decode(Request::param('html')));
39              } else {
40                  throw new HttpException(404, 'File not readabled');
41              }
42              if ($html) {
43                  return $this->response(200, Lang::get('Success'));
44              } else {
45                  return $this->response(201, Lang::get('Fail'));
46              }
47          } else {
48              if (is_readable($rootpath)) {
49                  $html = file_get_contents($rootpath);
50              } else {
51                  throw new HttpException(404, 'File not readabled');
52              }
53              $data = [
54                  'html' => htmlspecialchars($html),
55                  'path' => $path,
56                  'name' => base64_decode(Request::param('name')),
57              ];
58
59              return $this->fetch('fileedit', $data);
60          }
61      }
62  }
63
```

$path and $html We controlled,$rootpath Path splicing
And the PATH variable can be passed through .. / directory
The variable HTML is written to our PHP code
The HTML is decoded, but it has no effect on the PHP code
So we can find an existing file to overwrite the writing.
POST payload is:
path=../../index.php&html=(you php code)
Finally, the command is executed at index.PHP

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant