2020.4.6 xctf(shrine)②

转载

藏蓝色的达达 于 2020-04-06 22:29:10 发布 665 收藏 2

分类专栏： web安全

原文链接：https://blog.csdn.net/chuxuezheerer/article/details/104219527

首先打开网站，看到网站的源码：

```
import flask
import os

app = flask.Flask(__name__)

app.config['FLAG'] = os.environ.pop('FLAG')


@app.route('/')
def index():
    return open(__file__).read()


@app.route('/shrine/<path:shrine>')
def shrine(shrine):

    def safe_jinja(s):
        s = s.replace('(', '').replace(')', '')
        blacklist = ['config', 'self']
        return ''.join(['{{% set {}=None%}}'.format(c) for c in blacklist]) + s

    return flask.render_template_string(safe_jinja(shrine))


if __name__ == '__main__':
    app.run(debug=True)
```

里面有些关键词:jinja什么的，判断这应该是一道模版注入的题吧。

（1）通过分析上面的源码，可以看待这段代码有一下几个内容：

A.路径在/shrine/下
B.将所有的(,) 都替换成了空格。
C.有黑名单:config, self。
(2)进行分析，常规的jinja注入，参见三分题第一题。因为这里的（）都已经被替换，所以那道题中的解题方面不适用了。
这里的方式是适用内置函数：get_flashed_messages(), url_for()

url_for()

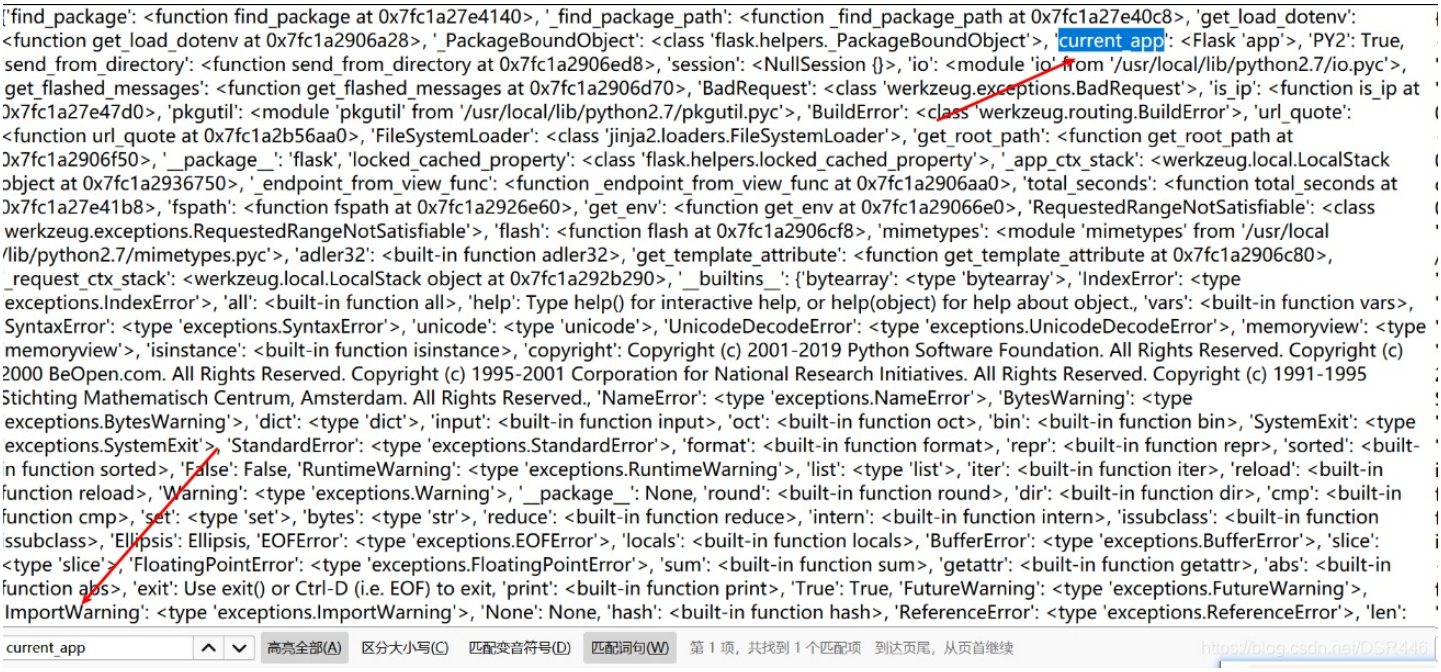
一般我们通过一个URL就可以执行到某一个函数。如果反过来，我们知道一个函数，怎么去获得这个URL呢？url_for函数就可以帮我们实现这个功能。url_for()函数接收两个及以上的参数，他接收函数名作为第一个参数，接收对应URL规则的命名参数，如果还出现其他的参数，则会添加到URL的后面作为查询参数。

get_flashed_messages()

返回之前在Flask中通过 flash() 传入的闪现信息列表。把字符串对象表示的消息加入到一个消息队列中，然后通过调用 get_flashed_messages() 方法取出(闪现信息只能取出一次，取出后闪现信息会被清空)。

首先查：

{{url_for.globals}}



我们这里可以按ctrl +F 快速查找。

注意到这个，我们就获取当前App下的config

/shrine/{{url_for.**globals**['current_app'].config}}

可以看到flag：