

# 攻防世界：Cat

原创

[FW\\_ENJOEY](#) 于 2021-01-11 22:19:56 发布 156 收藏

分类专栏：[攻防世界XCTF CTF\\_Web\\_Writeup](#)

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/qq\\_46230755/article/details/112494346](https://blog.csdn.net/qq_46230755/article/details/112494346)

版权



[攻防世界XCTF 同时被 2 个专栏收录](#)

10 篇文章 1 订阅

订阅专栏



[CTF\\_Web\\_Writeup](#)

50 篇文章 0 订阅

订阅专栏

打开后有个输入框简单测试一下

## Cloud Automated Testing

输入你的域名，例如：loli.club

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.056 ms
```

```
--- 127.0.0.1 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.056/0.056/0.056/0.000 ms
```

[https://blog.csdn.net/qq\\_46230755](https://blog.csdn.net/qq_46230755)

题目提醒了cat那感觉大概率就是要cat /flag了

试了一些简单的姿势发现都被过滤了

## Cloud Automated Testing

输入你的域名，例如：loli.club

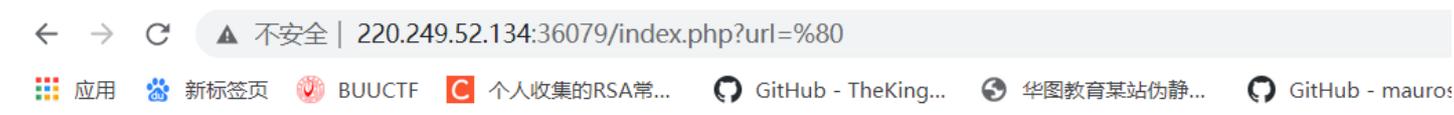
Invalid URL

https://blog.csdn.net/qq\_46230755

观察一下发现可以修改url



会进行自动的解码，于是尝试输入%80发现出现了网页源码



# Cloud Automated Testing

输入你的域名，例如：loli.club

```
<!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; }
    table td.code { width:100%; }
    table td.code pre { font-family:monospace; }
```

```
table td.code pre { overflow: hidden; }
table.source th { color: #666; }
table.source td { font-family: monospace; white-space: pre; border-bottom: 1px solid #eee; }
ul.traceback { list-style-type: none; color: #222; }
ul.traceback li.frame { padding-bottom: 1em; color: #666; }
ul.traceback li.user { background-color: #e0e0e0; color: #000 }
div.context { padding: 10px 0; overflow: hidden; }
div.context ol { padding-left: 30px; margin: 0 10px; list-style-position: inside; }
div.context ol li { font-family: monospace; white-space: pre; color: #777; cursor: pointer; padding-left: 2px; }
```

复制后新建一个html进行打开

## 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/utls.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:** Mon, 11 Jan 2021 13:30:07 +0000

[https://blog.csdn.net/qq\\_46230755](https://blog.csdn.net/qq_46230755)

没什么思路，看了别的师傅的wp，发现原来题目有提示

RTFM of PHP CURL====>>read the fuck manul of PHP CURL???

然后别的师傅说了

## CURLOPT\_POSTFIELDS

全部数据使用HTTP协议中的 "POST" 操作来发送。要发送文件，在文件名前面加上@前缀并使用完整路径。文件类型可在文件名后以 ';type=mimetype' 的格式指定。这个参数可以是 urlencoded 后的字符串，类似 'para1=val1&para2=val2&...'，也可以使用一个以字段名为键值，字段数据为值的数组。如果value是一个数组，Content-Type头将会被设置成 multipart/form-data。从 PHP 5.2.0 开始，使用 @ 前缀传递文件时，value 必须是个数组。从 PHP 5.5.0 开始，@ 前缀已被废弃，文件可通过 [CURLFile](#) 发送。设置 **CURLOPT\_SAFE\_UPLOAD** 为 **TRUE** 可禁用 @ 前缀发送文件，以增加安全性。

[https://blog.csdn.net/qq\\_46230755](https://blog.csdn.net/qq_46230755)

我们使用@进行文件传递，对文件进行读取之后还会把内容传给url参数

然后回到那个html，在setting里找到database。

找database目的是找到数据库文件，看能不能从数据库文件执行，找到flag

```
CSRF_TRUSTED_ORIGINS
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/qq\\_46230755](https://blog.csdn.net/qq_46230755)

然后在url进行输入

```
url=@/opt/api/database.sqlite3
```

在一个小角落发现了flag

```
0\x00\x1c\x01\x02AWHCTF {yoooo_Such_A_GOOD_@} \n&#39;</pre>
```

## Flag

```
WHCTF{yoooo_Such_A_GOOD_@}
```