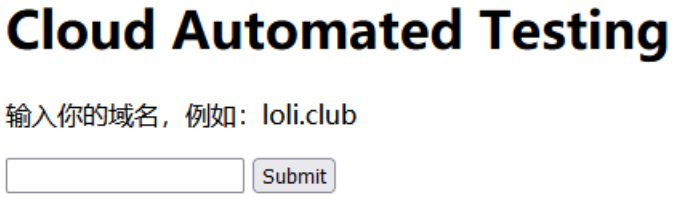
攻防世界-Cat

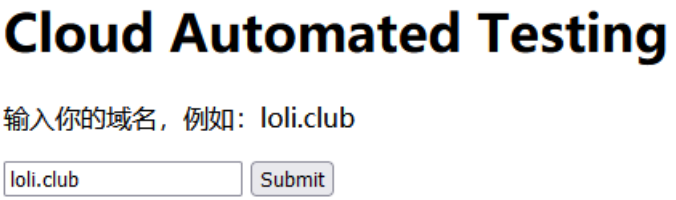
原创

皮皮逗逗逗 于 2021-09-29 10:01:39 发布 1263 收藏
分类专栏： #ctf 文章标签： 安全 web安全

进入环境出现的页面是一个输入框,然后让我们输入域名

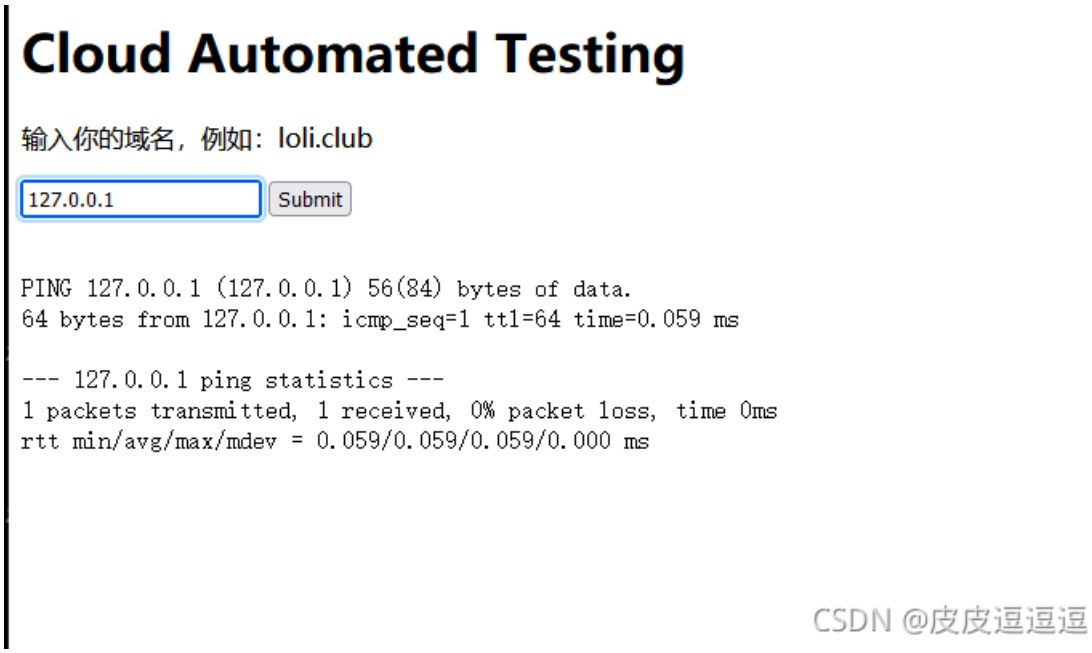


我们顺着思路输入一个域名试一试



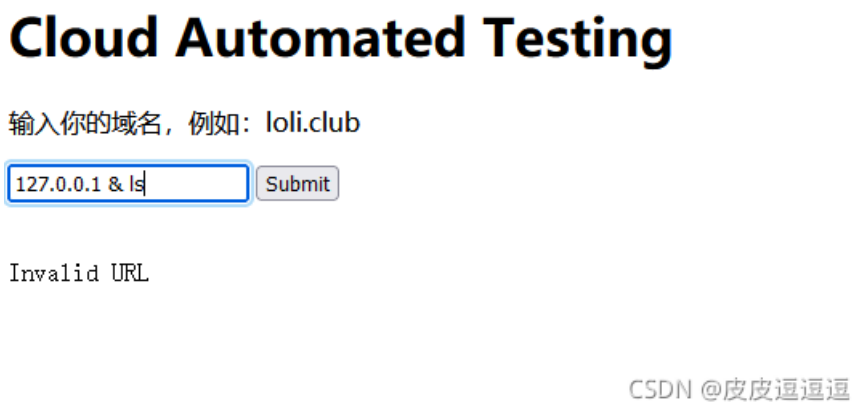
并没有任何的回显内容

想一想,如果输入127.0.0.1会怎么样?

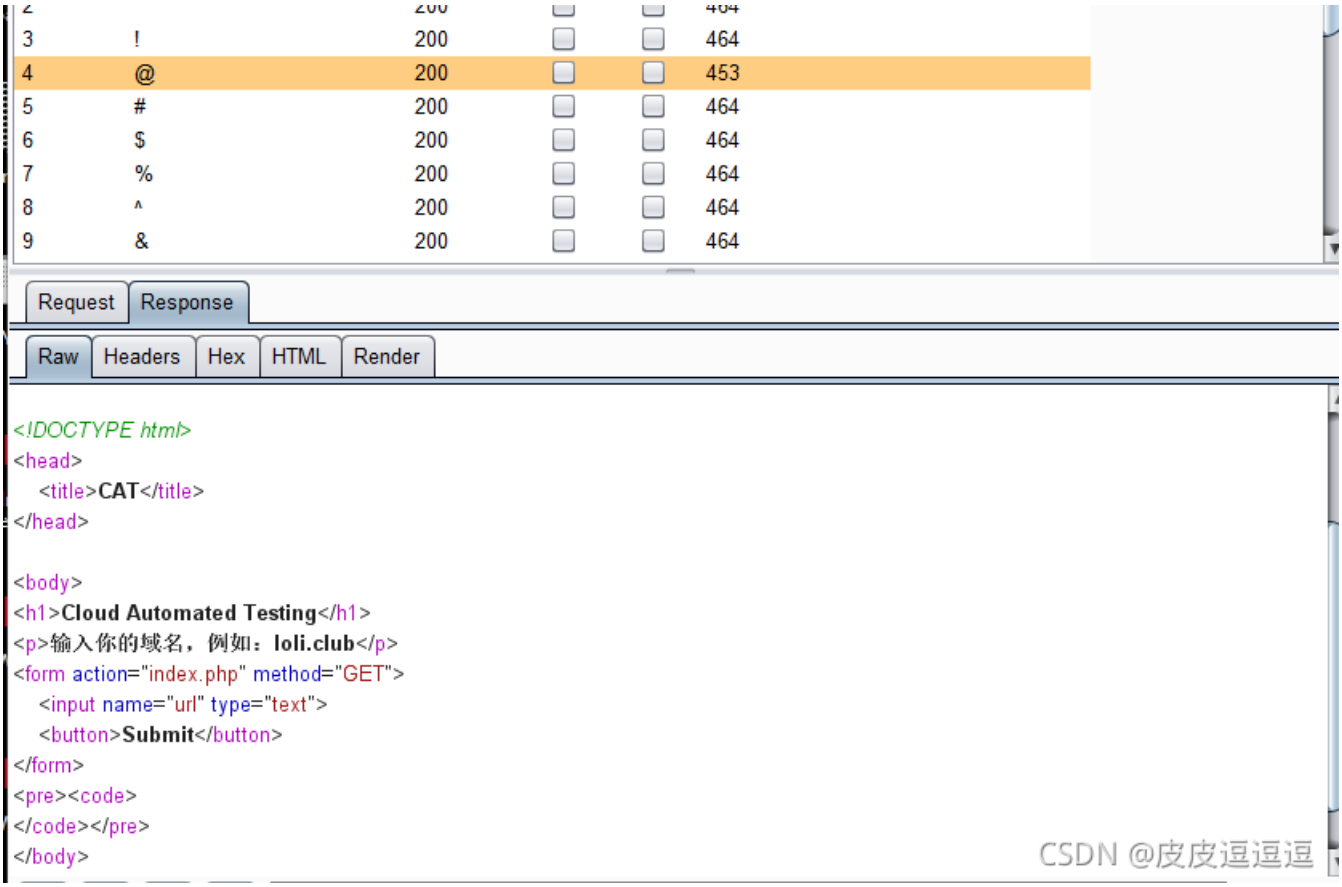


它执行了一个ping命令,那么就会联想到会不会有命令拼接

在框中输入 127.0.0.1 & ls 127.0.0.1 | ls



显示无效的url,应该是被过滤掉了,burp抓一抓,跑一跑看看哪个字符没有被过滤



发现@符号没有被过滤,这有什么用呢,开始思考.没有特别好的思路,这个时候就要脑洞大一点,各种尝试了

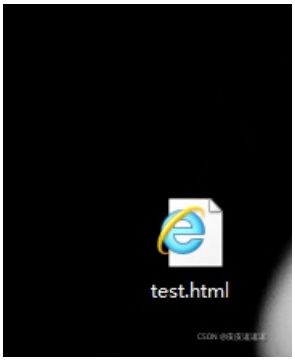
我尝试在url=后面的编码下手

各范围的编码试一试,在试到%80的时候就报错了,首先url编码使用的是16进制的,%80 转换过来也就是128,也就是说超过这个范围它就报错

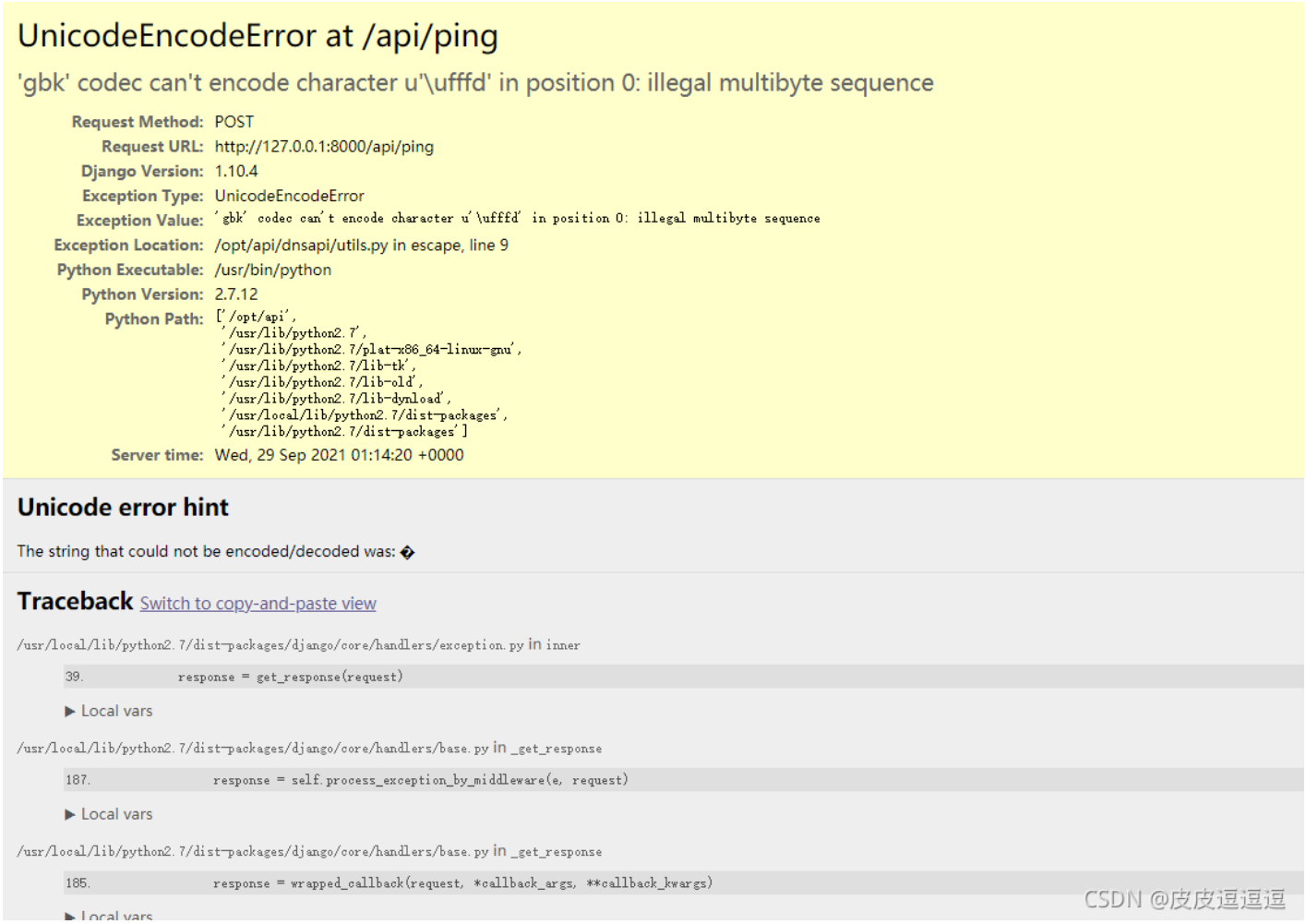
```
        <tr>
          <td>X_FRAME_OPTIONS</td>
          <td class="code"><pre>u&#39;SAMEORIGIN&#39;</pre></td>
        </tr>

        <tr>
          <td>YEAR_MONTH_FORMAT</td>
          <td class="code"><pre>u&#39;F Y&#39;</pre></td>
        </tr>

    </tbody>
  </table>

</div>

  <div id="explanation">
    <p>
      You're seeing this error because you have <code>DEBUG = True</code> in your
      Django settings file. Change that to <code>False</code>, and Django will
      display a standard page generated by the handler for this status code.
    </p>
  </div>

</body>
</html>
```

```
&amp;#39;dnsapi&amp;#39;]
Installed Middleware:
[&amp;#39;django.middleware.security.SecurityMiddleware&amp;#39;,
 &amp;#39;django.contrib.sessions.middleware.SessionMiddleware&amp;#39;,
 &amp;#39;django.middleware.common.CommonMiddleware&amp;#39;,
 &amp;#39;django.contrib.auth.middleware.AuthenticationMiddleware&amp;#39;,
 &amp;#39;django.contrib.messages.middleware.MessageMiddleware&amp;#39;,
 &amp;#39;django.middleware.clickjacking.XFrameOptionsMiddleware&amp;#39;]



Traceback:

File &quot;/usr/local/lib/python2.7/dist-packages/django/core/handlers/exception.py&quot; in inner
  39.             response = get_response(request)

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

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

File &quot;/opt/api/dnsapi/views.py&quot; in wrapper
  21.         return f(*args, **kwargs)

File &quot;/opt/api/dnsapi/views.py&quot; in ping
  30.     data = escape(data)

File &quot;/opt/api/dnsapi/utils.py&quot; in escape
  9.     return r.encode(&amp;#39;gbk&amp;#39;)

Exception Type: UnicodeEncodeError at /api/ping
Exception Value: &amp;#39;gbk&amp;#39; codec can&amp;#39;t encode character u&amp;#39;\ufffd&amp;#39; in position 0: illegal multibyte
&lt;/textarea&gt;
  &lt;br&gt;&lt;br&gt;
  &lt;input type=&quot;submit&quot; value=&quot;Share this traceback on a public website&quot;&gt;
  &lt;/div&gt;
&lt;/form&gt;
&lt;/div&gt;
```


报错是一大段html,将它复制出来,粘贴到一个文本文件中,改后缀,然后用游览器打开看一看



打开之后的样子



这时django报错页面,不熟悉的小伙伴,可以去百度一下,这里不再赘述

我到这里已经解不下去了,我去看大佬的题解了,然后发现有个坑,这原题是有,之前找出来@符号不被过滤,怎么用的提示,而这里并没有

> RTFM of PHP CURL===>>read the fuck manul of PHP CURL???
>
> CSDN @皮皮逗逗逗

这里表明@是读取文件的内容需要加上

到这一步,还需要懂一些django的基本知识,django项目下面会有一个settings.py文件,这个文件是设置网站数据库的路径,它还会对项目的整体的设置进行定义.那么接下来的思路就是我们需要去看看settings.py这个文件,看看database的相关信息了(我发现其实也不需要看,之前的报错内容已经有database信息了,狗头)

```
CACHE_MIDDLEWARE_SECONDS        600
CSRF_COOKIE_AGE                 31449600
CSRF_COOKIE_DOMAIN              None
CSRF_COOKIE_HTTPONLY            False
CSRF_COOKIE_NAME                u'csrftoken'
CSRF_COOKIE_PATH                u'/'
CSRF_COOKIE_SECURE              False
CSRF_FAILURE_VIEW               u'django.views.csrf.csrf_failure'
CSRF_HEADER_NAME                u'HTTP_X_CSRFTOKEN'
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': ''}}
DATABASE_ROUTERS                []
DATA_UPLOAD_MAX_MEMORY_SIZE     2621440
```


愉快的去猫一眼

搜一搜关键词ctf,flag等看看,哈,有了

这题的知识点涉及比较广

1.cURL的post文件上传

2.php的curl上传组件

3.python的字符编码

4.django的框架知识

希望各位小伙伴加油,多多去学习知识,在成神道路上越走越远!下次再见!!