

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

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_44065556/article/details/120541298

版权



[#ctf专栏收录该内容](#)

9 篇文章 1 订阅

订阅专栏

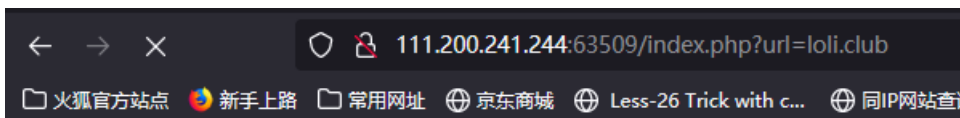
进入环境出现的页面是一个输入框,然后让我们输入域名

Cloud Automated Testing

输入你的域名, 例如: loli.club

CSDN @皮皮逗逗逗

我们顺着思路输入一个域名试一试



Cloud Automated Testing

输入你的域名, 例如: loli.club

CSDN @皮皮逗逗逗

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?

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=0.059 ms  
  
--- 127.0.0.1 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.059/0.059/0.059/0.000 ms
```

CSDN @皮皮逗逗逗

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

Cloud Automated Testing

输入你的域名, 例如: loli.club

Invalid URL

CSDN @皮皮逗逗逗

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

2		200	<input type="checkbox"/>	<input type="checkbox"/>	404
3	!	200	<input type="checkbox"/>	<input type="checkbox"/>	464
4	@	200	<input type="checkbox"/>	<input type="checkbox"/>	453
5	#	200	<input type="checkbox"/>	<input type="checkbox"/>	464
6	\$	200	<input type="checkbox"/>	<input type="checkbox"/>	464
7	%	200	<input type="checkbox"/>	<input type="checkbox"/>	464
8	^	200	<input type="checkbox"/>	<input type="checkbox"/>	464
9	&	200	<input type="checkbox"/>	<input type="checkbox"/>	464

Request
Response

Raw
Headers
Hex
HTML
Render

```

<!DOCTYPE html>
<head>
  <title>CAT</title>
</head>
<body>
<h1>Cloud Automated Testing</h1>
<p>输入你的域名, 例如: loli.club</p>
<form action="index.php" method="GET">
  <input name="url" type="text">
  <button>Submit</button>
</form>
<pre><code>
</code></pre>
</body>

```

CSDN @皮皮逗逗逗

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

🔗 111.200.241.244:63509/index.php?url=%26
CSDN @皮皮逗逗逗

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>

```

CSDN @皮皮逗逗逗

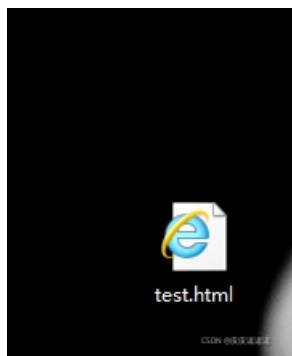
```

27 &#39;django.contrib.staticfiles&#39;],
28 &#39;django.contrib.sitemaps.views.sitemap&#39;],
29 Installed Middleware:
30 [&#39;django.middleware.security.SecurityMiddleware&#39;,
31 &#39;django.contrib.sessions.middleware.SessionMiddleware&#39;,
32 &#39;django.middleware.common.CommonMiddleware&#39;,
33 &#39;django.contrib.auth.middleware.AuthenticationMiddleware&#39;,
34 &#39;django.contrib.messages.middleware.MessageMiddleware&#39;,
35 &#39;django.middleware.clickjacking.XFrameOptionsMiddleware&#39;]
36
37
38
39 Traceback:
40
41 File &quot;/usr/local/lib/python2.7/dist-packages/django/core/handlers/exception.py&quot; in inner
42 39.         response = get_response(request)
43
44 File &quot;/usr/local/lib/python2.7/dist-packages/django/core/handlers/base.py&quot; in _get_response
45 187.         response = self.process_exception_by_middleware(e, request)
46
47 File &quot;/usr/local/lib/python2.7/dist-packages/django/core/handlers/base.py&quot; in _get_response
48 185.         response = wrapped_callback(request, *callback_args, **callback_kwargs)
49
50 File &quot;/opt/api/dnsapi/views.py&quot; in wrapper
51 21.         return f(*args, **kwargs)
52
53 File &quot;/opt/api/dnsapi/views.py&quot; in ping
54 30.         data = escape(data)
55
56 File &quot;/opt/api/dnsapi/utils.py&quot; in escape
57 9.         return r.encode(&#39;gbk&#39;)
58
59 Exception Type: UnicodeEncodeError at /api/ping
60 Exception Value: &#39;gbk&#39; codec can&#39;t encode character u&#39;\ufffd&#39; in position 0: illegal multibyte
61 &lt;/textarea&gt;
62 &lt;br&gt;&lt;br&gt;
63 &lt;input type=&quot;submit&quot; value=&quot;Share this traceback on a public website&quot;&gt;
64 &lt;/div&gt;
65 &lt;/form&gt;
66 &lt;/div&gt;
67
68

```

CSDN @皮皮逗逗逗

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,然后用浏览器打开看一看




打开之后的样子

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: Wed, 29 Sep 2021 01:14:20 +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
39.         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
```

CSDN @皮皮逗逗逗

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

44

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

CSDN @皮皮逗逗逗

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¶2=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CURLOPT_SAFE_UPLOAD发送。设置CURLOPT_SAFE_UPLOAD为TRUE可禁用@前缀发送文件,以增加安全性。

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

```

CSDN @皮皮逗逗逗

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!!