攻防世界 cat

原创

whisper_ZH 于 2019-09-28 15:21:45 发布 511 收藏 3

**

学习知识点

1.当 CURLOPT_SAFE_UPLOAD 为 true 时，如果在请求前面加上@的话phpcurl组件是会把后面的当作绝对路径请求，来读取文件。当且仅当文件中存在中文字符的时候，Django 才会报错导致获取文件内容

TRUE为禁用 @ 前缀在 CURLOPT_POSTFIELDS 中发送文件。
FALSE为启用，@开头的value会被当做文件上传。

PHP 5.5.0 中添加，默认值 FALSE。
PHP 5.6.0 改默认值为 TRUE。
PHP 7 删除了此选项。

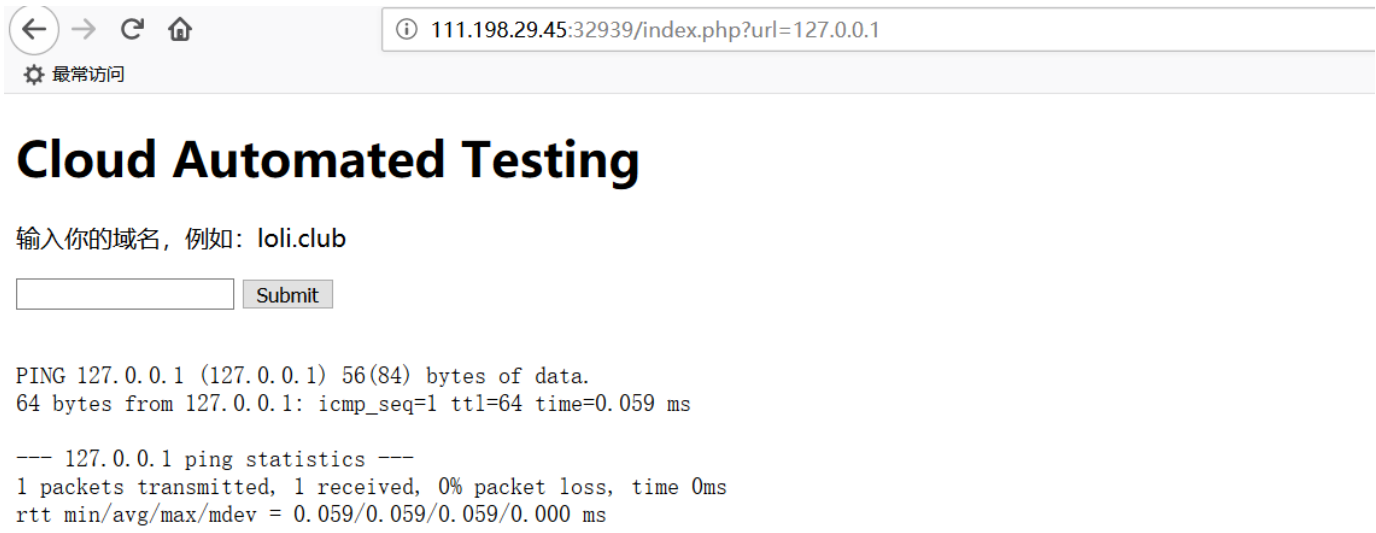
影响：CURLOPT_SAFE_UPLOAD选项配置不当结合其他情况可造成任意文件读取。

详情参见PHP libcurl 安全之 CURLOPT_SAFE_UPLOAD
2.django未关闭报错回显

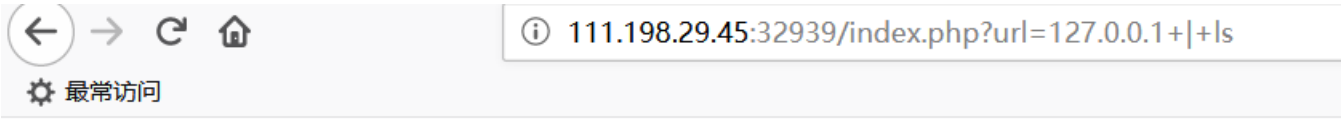
3.url编码采用16进制范围为0-127 ， %79为最大127
**

以下为做题思路复现

首先打开题目根据提示输入一个127.0.0.1进行测试，返回如下



考虑管道符执行系统命令，提示报错



Cloud Automated Testing

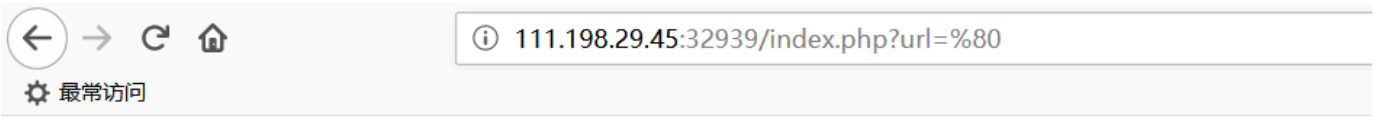
输入你的域名，例如：loli.club

127.0.0.1 | ls Submit

Invalid URL

尝试一波 &，|等管道符号和ls dir等命令均报错了

3.细看url可以直接发现 空格直接被url编码为了+，考虑报错回显，输入url=%80,出现报错信息



Cloud Automated Testing

输入你的域名，例如：loli.club

Submit

```
<!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; }
```

通过过报错信息我可以发现后台运行了两个应用分别为php.和Django应用

4.查看报错信息，得到很多有用信息，例如python版本，文件路径，以及接口位置信息如下：

```
    </tr>

    <tr>
      <th>Python Executable:</th>
      <td>/usr/bin/python</td>
    </tr>
    <tr>
      <th>Python Version:</th>
      <td>2.7.12</td>
    </tr>
    <tr>
      <th>Python Path:</th>
```



```
  <tr>
    <th>Request Method:</th>
    <td>POST</td>
  </tr>
  <tr>
    <th>Request URL:</th>
    <td>http://127.0.0.1:8000/api/ping</td>
  </tr>

  <tr>
    <th>Django Version:</th>
    <td>1.10.4</td>
  </tr>

  <tr>
    <th>Exception Type:</th>
    <td>UnicodeEncodeError</td>
  </tr>


  <tr>
    <th>Exception Value:</th>
```



```
    </tr>

    <tr>
      <td>DATABASES</td>
      <td class="code"><pre>{&#39;default&#39;: {&#39;ATOMIC_REQUESTS&#39;: False,
        &#39;AUTOCOMMIT&#39;: True,
        &#39;CONN_MAX_AGE&#39;: 0,
        &#39;ENGINE&#39;: &#39;django.db.backends.sqlite3&#39;,
        &#39;HOST&#39;: &#39;&#39;,
        &#39;NAME&#39;: &#39;/opt/api/database.sqlite3&#39;,
        &#39;OPTIONS&#39;: {},
        &#39;PASSWORD&#39;: u&#39;**********&#39;,
        &#39;PORT&#39;: &#39;&#39;,
        &#39;TEST&#39;: {&#39;CHARSET&#39;: None,
                &#39;COLLATION&#39;: None,
                &#39;MIRROR&#39;: None,
                &#39;NAME&#39;: None},
        &#39;TIME_ZONE&#39;: None,
        &#39;USER&#39;: &#39;&#39;}}</pre></td>
    </tr>

    <tr>
```

5.搜索到链接数据库的接口，利用 CURLOPT_SAFE_UPLOAD 为 true这个特性进行读取数据库文件，读取文件后搜索flag如下