HackThisSite(Realistic missions 第二题)Writeup

原创

zeykevin 于 2021-02-12 15:37:26 发布 426 收藏

分类专栏： HackThisSite(Realistic missions） 文章标签： 安全 网络安全 sql

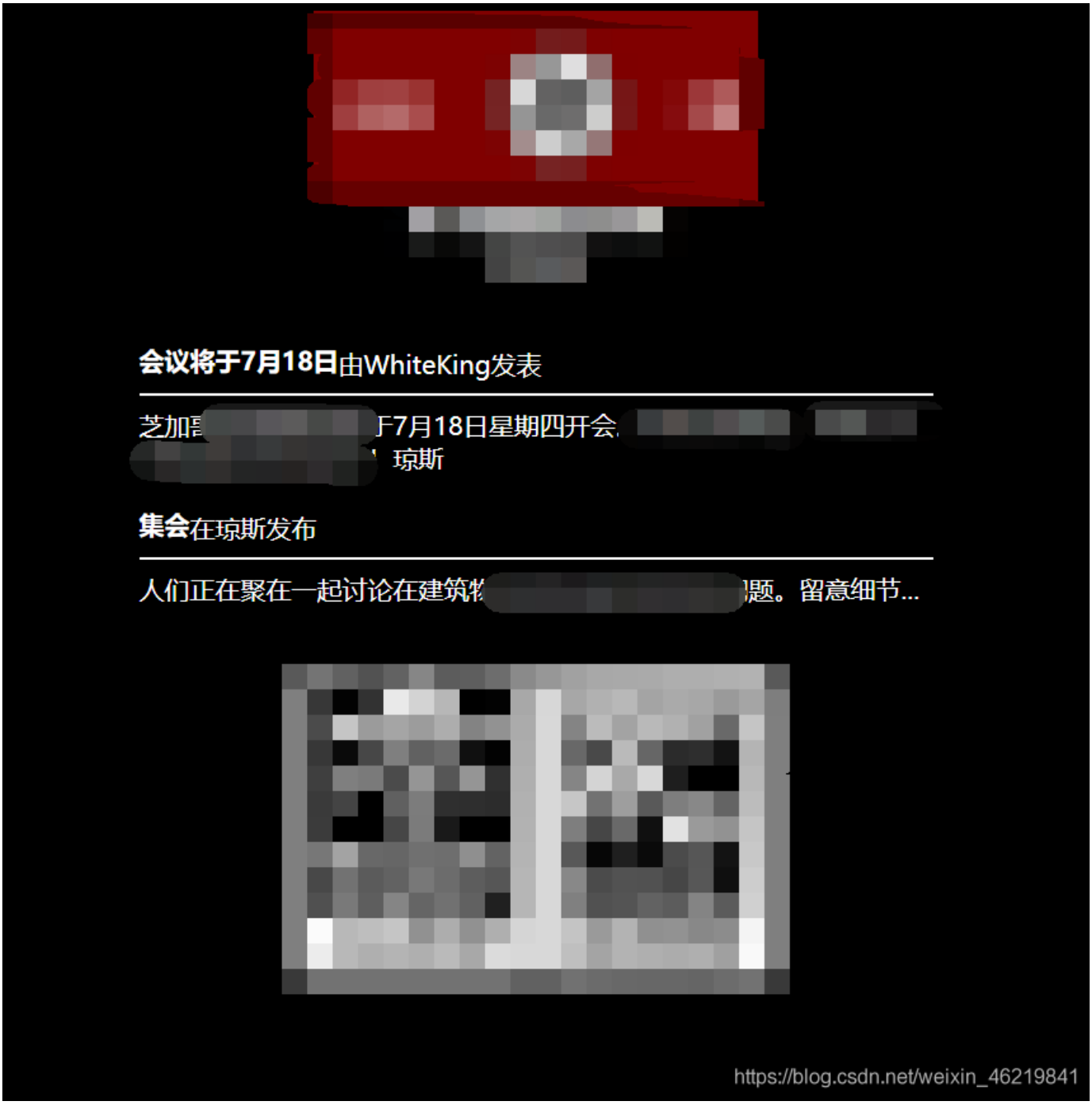
本文链接：https://blog.csdn.net/weixin_46219841/article/details/113794991

文章目录

题目

消息：我被告知您具有相当令人钦佩的黑客技能。好吧，这个种族仇恨团体正在使用他们的网站来组织大量无知种族主义者的混蛋。我们不能允许这种顽固的侵略发生。如果您可以访问他们的管理员页面并将消息发布到他们的主页，我们将非常感激。

过程



ok 进来什么也没有。先看看网页源代码

```
<table width=500 align="center" cellspacing=0 cellpadding=0 border=0><tr><td>
<b>Meeting July 18th</b> posted by WhiteKing<br /><hr color="white">The Chicago American N
<br />
<center><a href="http://www.americannaziparty.com/support/gifs/wigger.gif"><img src="http:

<center><a href="/missions/realistic/2/update.php"><font color="#000000">update</font></a>

</body>
</html>
```


发现了一个update.php的链接，点开看看。

enter your username and password, white brother!

username

password

提交

一个登录页面，什么也不知道。这个时候就需要SQL注入了

恶意填入：usename: 1’or’1’=‘1 pwd: 1’or’1’='1
这时将导致原本正常的SQL字符串被填为
“SELECT * FROM users WHERE (name = ‘1’ or ‘1’=‘1’) AND (pwd= ‘1’ or ‘1’=‘1’);”