果然本弱鶸鰯嵎篛到最后还是没有做出来Boss写个Writeup骗点分

阿西吧，可惜了……感觉自己SQL和PHP就是个渣，差太多了。

打算进了凝聚……我再好好学渗透……

从game.lc4t.me开始

首先我们都知道……在浏览器里输入`http://game.lc4t.me/`，然后……我检查了Chrome的Network栏，看了下，只发现了本页本身和`favicon.ico`。理所当然地检查了一下`favicon.ico`，好像什么都没有。

然后`curl`了一下`game.lc4t.me`，`curl`了一下`favicon.ico`，还是什么都没有。

重新打开了`game.lc4t.me`发现出现一行`My waf eat your params, it is very delicious.` 后来提示指出是已经没了。`Give up.`

然后某天无聊了又去试了试`curl`，随便试了一下，发现`http://game.lc4t.me/index.html`是有东西的……然后又是那个`find`题的套路自动跳转，当然我用`curl`的话是不会执行`javascript`的。

得到一段莫名其妙的`js`，明显混淆过……

Chrome浏览器是自带反混淆的，F12一下Console扔进去就可以得到反混淆的结果，因为Boss当时没有截图，所以我用另一个做一下演示好了……这个是基于报错的，没报错我也不清楚怎么弄，主要是好像要让`window`这玩意儿没加载出来？

顺便提一下，Boss那个`js`的混淆是`aaencode`，Chrome也可以解决，或者去网上随便找个`aaencode`的反混淆工具跑一下就可以得到`packed`之后的结果，得到这个结果的基本上信息也都有了。

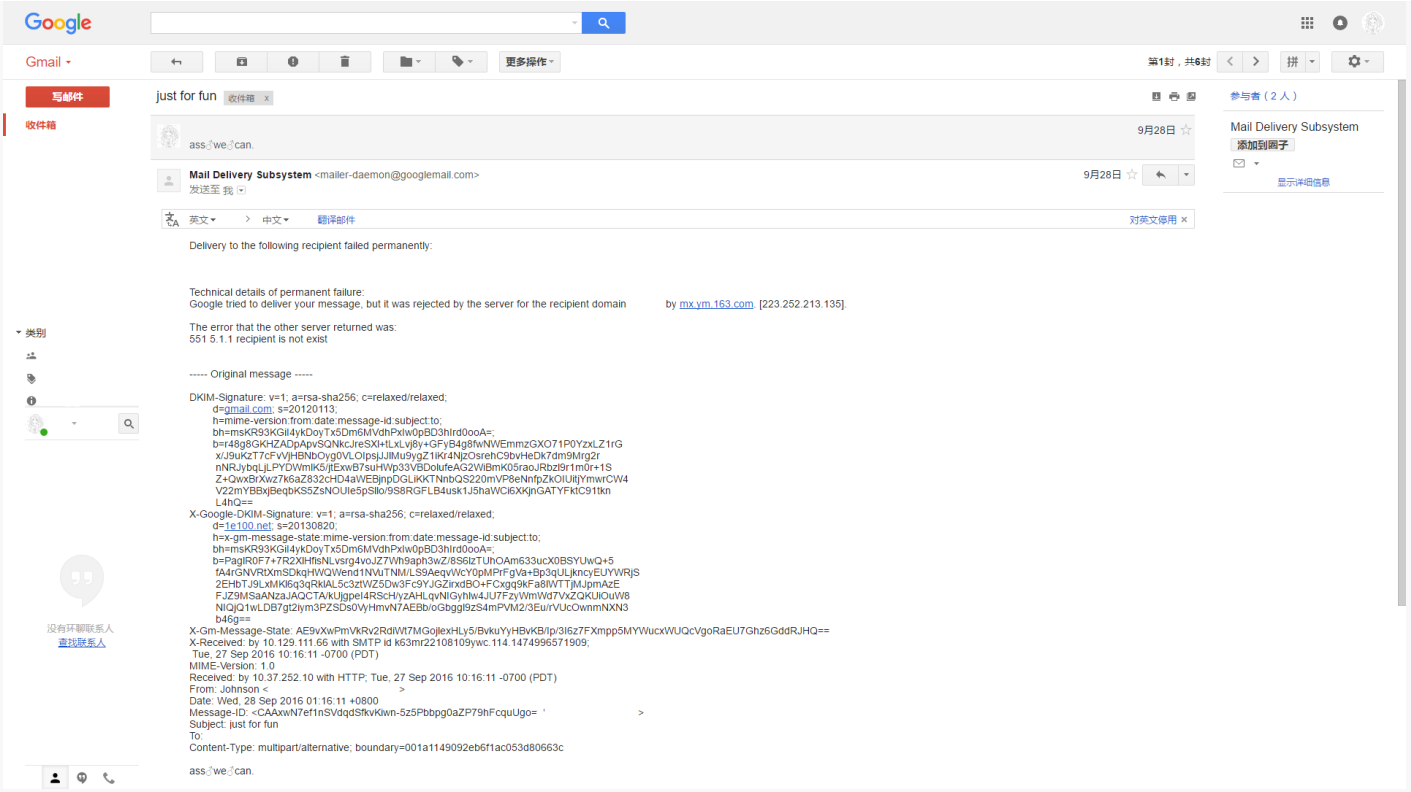
得到代码

```Javascript
(function() {
    window.location.href = "index.php";
    var author = 'liergou';
    var email = 'liergou@lc4t.me'
})()
```

李二狗，可以的，很强势。

社工开始

得知了邮箱地址之后，自然而然地要去寻找邮件服务器在哪里，然后我随便发了几条邮件，然后……呃。



得到邮件服务器在163企业邮箱……

这期间闲着发了一些邮件。

然后蜜汁社工……猜密码……我实在是猜不到啊……放了好几天。

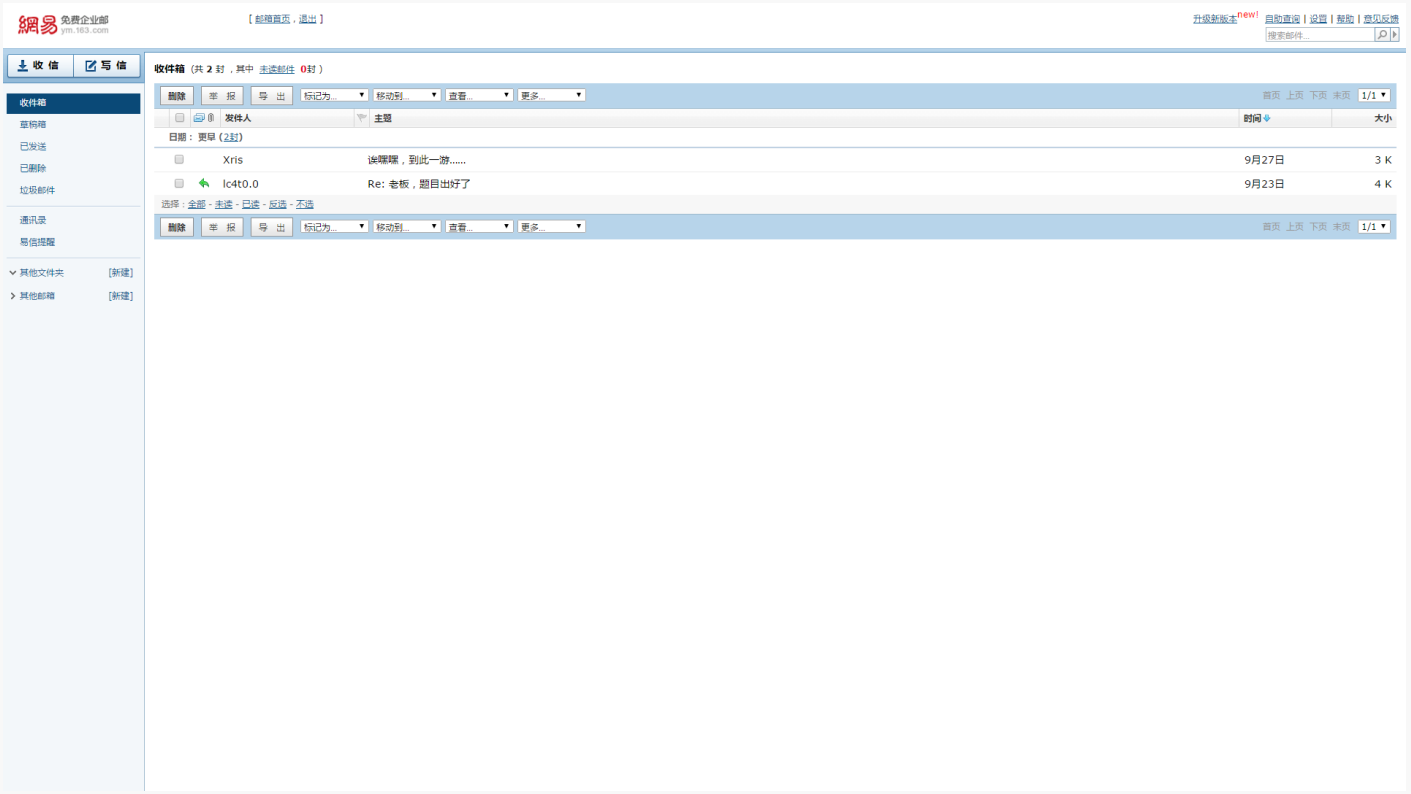
期间为了方便写了个python脚本来登录……

```python
#!/usr/local/bin/python3
import urllib.request
import re
form = {
    'domain'       : 'lc4t.me',
    'account_name' : 'liergou',
    'secure'       : 1,
    'all_secure'   : 0,
    'language'     : 0,
    'ch'           : '',
    'pubid'        : '',
    'passtype'     : '',
    'accname'      : 'liergou@lc4t.me',
    'password'     : input('Please input password: '),
    'verify_code'  : '',
}
url = 'http://entry.ym.163.com/login/login'
msg = re.compile(r'msg=(.*)"')

while form['password']:
    post = urllib.parse.urlencode(form).encode()
    print(msg.findall(urllib.request.urlopen(url, post).read().decode())[0])
    try: form['password'] = input('Please input password: ')
    except EOFError: exit()
```

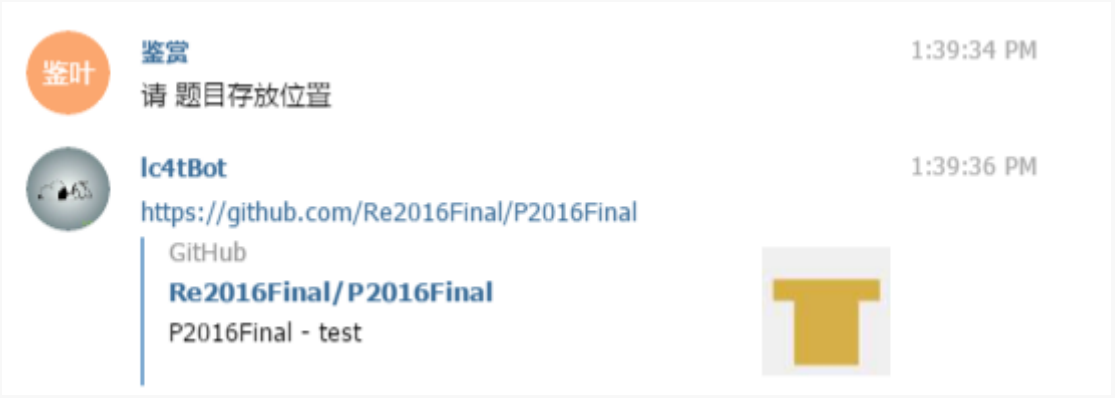
然后在最后不知怎么的密码搞了个LiErGou就进去了……

终于看到了自己发的邮件内牛满面……



死在PHP上

这以后跟着套路走，显示需要和一个在Telegram的机器人lc4t_bot聊天，提示要“礼貌”和“询问题目存放位置”，然后乱试一通得到了两个关键词“请”和“题目存放位置”……因为只是简单地检测，所以直接输入这俩就可以了，换位输入也是可以的……



提示扔在GitHub上，我去看了一眼，空空如也……Removed by cnss然后就没有然后了……

后来去检查了这个项目的release、user和commits，在commits里发现了以前的记录，一段长长的PHP代码。

```php
<?php

header("Content-type: text/html; charset=utf-8");

function waf($str)
{
    $black_list = array(
        "}", "{", "]", "[", "_", "-", "(", "/",
        "\\", "*", ")", " ", "#", "'", "%", "a",
        "b", "c", "e", "f", "g", "h", "j", "k",
        "l", "m", "n", "o", "p", "q", "r", "s",
```

```php
        "t", "u", "v", "w", "x", "y", "z"
    );
    foreach ($black_list as $key => $value)
    {
        if (stripos($str, $value !== false))
        {
            die ("My waf eat your params, it is very delicious");
        }
    }
}

function waf_each($arr)
{
    foreach ($arr as $key => $value)
    {
        waf($key);
        waf($value);
    }
}

waf_each($_GET);
waf_each($_POST);
waf_each($_COOKIE);

function get_flag($var)
{
    $connect = mysql_connect("localhost","***","***");
    if (!$connect)
    {
      die('I am die, help me! Call 110 please.');
    }
    $sqlstr = "select content from ids where id='" . urldecode($var) . "'";
    $result = @mysql_db_query("cnsstest", $sqlstr, $connect);
    $row = @mysql_fetch_row($result);
    if ($row)
    {
        die ($row[0]);
    }
    else
    {
        die("哦，我是一个高冷的waf，懒得给你这个id的内容");
    }
    mysql_close($connect);
}

$uri = explode("?",$_SERVER['REQUEST_URI']);

if(isset($uri[1]))
{
    $parameter = explode("&",$uri[1]);
    foreach ($parameter as $key => $value)
    {
        $var = explode("=", $value);

        if ($var[0] !== 'id')
        {
            die ("PHP eat your params, it is not delicious.\
            <!--Please use another key. if you guess it success, also no egg use:) -->");
```

```
        }
        else
        {
            get_flag($var[1]);
        }

    }
}
else
{
  echo "你猜猜我这里有什么";
}

?>
```

噫，好了，我中了。

并不会PHP，但是初步分析那些字符串可以看得出来……这应该就是game.lc4t.me/index.php里的内容……

// 既然有说最好把代码扔上来我就扔上来了……

// 顺便一提貌似有地方和game.lc4t.me上的不一样

// 补充：那个不同的地方是我高亮的第16行，明显有错误嘛，我扔到自己服务器上的已经给改成了

```php
if (stripos($str, $value) !== false)
```

又回到最初的起点

大家好我回到game.lc4t.me了……

稍微研究了一下PHP，大致搞懂了那段长长的代码是什么意思。首先从Cookie、POST和GET里面检测有没有waf屏蔽掉的字符。然后检测GET的key是不是id，然后再去查询数据库。

我试了一下，貌似数字、汉字都可以，而且id从1到10都有值，然而如果说要我注入，我真不会注入，基本上已经把能屏蔽的给屏蔽完了……我所知道的方法都行不通……

手动搭环境

然后滚去做了几道服务器题目，期间搭了自己博客，纯粹在玩耍地稍微折腾了一下Arch和LFS之类的玩意儿……

最后，在我的xris.co下又搞了了个子域名****来折腾这题（那个网页会检查IP，不知道不用那个IP能不能用特殊手段上去……我是指X-Forwarded-For之类的

然而我估计PHP版本和MySQL版本完全不同……加之我对于这方面知识实在浅薄，我最后拿那个页面来进行了SQL注入的学习……

尽管搞了半天我都甚至没有办法注入我自己的页面……一脸懵逼……

最后注入成功了，貌似也不能执行一些复杂的语句。我怀疑和PHP版本有关系。

总结

先这样吧，如果这最后两天还有进展的话，我再次提交新的Writeup。

果然还是太菜了……

到最后还是没有搞出来……如果有人知道这个怎么注入请联系我……（哭