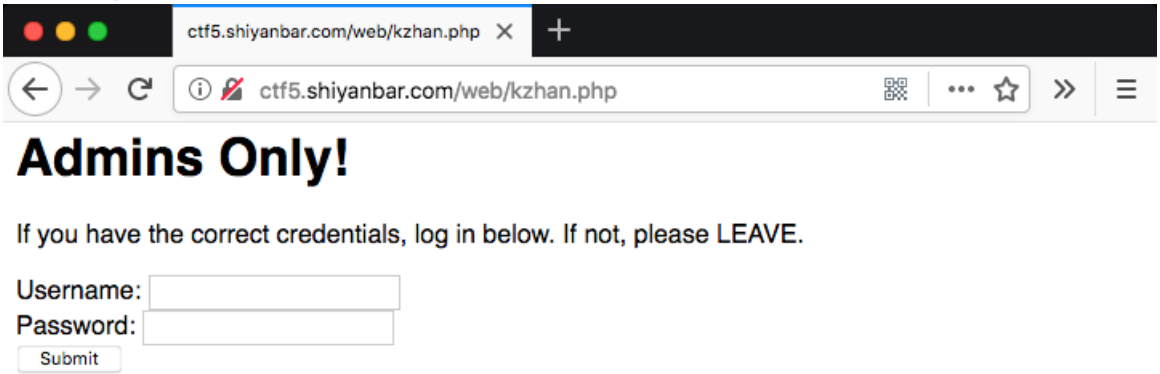
1009.CTF 题目之 WEB Writeup 通关大全 – 3

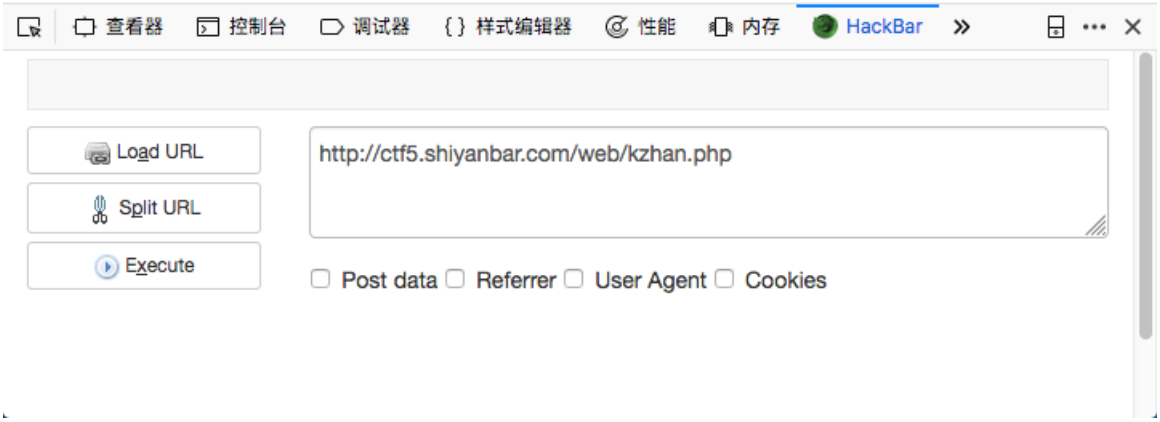
转载

weixin_30595035 于 2019-02-17 23:44:00 发布 178 收藏 1
文章标签： php 开发工具 python
原文链接：http://www.cnblogs.com/beijibing/p/10393314.html
版权
Web题目系列3

让我进去

题目链接
http://shiyanbar.com/ctf/1848





题目描述

```
相信你一定能拿到想要的
Hint:你可能希望知道服务器端发生了什么。。

格式：CTF{}
```

解题思路
用burpsuite抓包后，发现cookie里有一个字段`source=0`，修改为1后获取源码。

源码内容

```
<html>
<body>

<pre>
$flag = "XXXXXXXXXXXXXXXXXXXXXXX";
$secret = "XXXXXXXXXXXXXXX"; // This secret is 15 characters long for security!

$username = $_POST["username"];
$password = $_POST["password"];

if (!empty($_COOKIE["getmein"])) {
    if (urldecode($username) === "admin" && urldecode($password) != "admin") {
        if ($COOKIE["getmein"] === md5($secret . urldecode($username . $password))) {
            echo "Congratulations! You are a registered user.\n";
            die ("The flag is ". $flag);
        }
        else {
            die ("Your cookies don't match up! STOP HACKING THIS SITE.");
        }
    }
    else {
        die ("You are not an admin! LEAVE.");
    }
}

setcookie("sample-hash", md5($secret . urldecode("admin" . "admin")), time() + (60 * 60 * 24 * 7));

if (empty($_COOKIE["source"])) {
    setcookie("source", 0, time() + (60 * 60 * 24 * 7));
}
else {
    if ($_COOKIE["source"] != 0) {
        echo ""; // This source code is outputted here
    }
}
    </pre>
<h1>Admins Only!</h1>
<p>If you have the correct credentials, log in below. If not, please LEAVE.</p>
<form method="POST">
    Username: <input type="text" name="username"> <br>
    Password: <input type="password" name="password"> <br>
    <button type="submit">Submit</button>
</form>

</body>
</html>
```

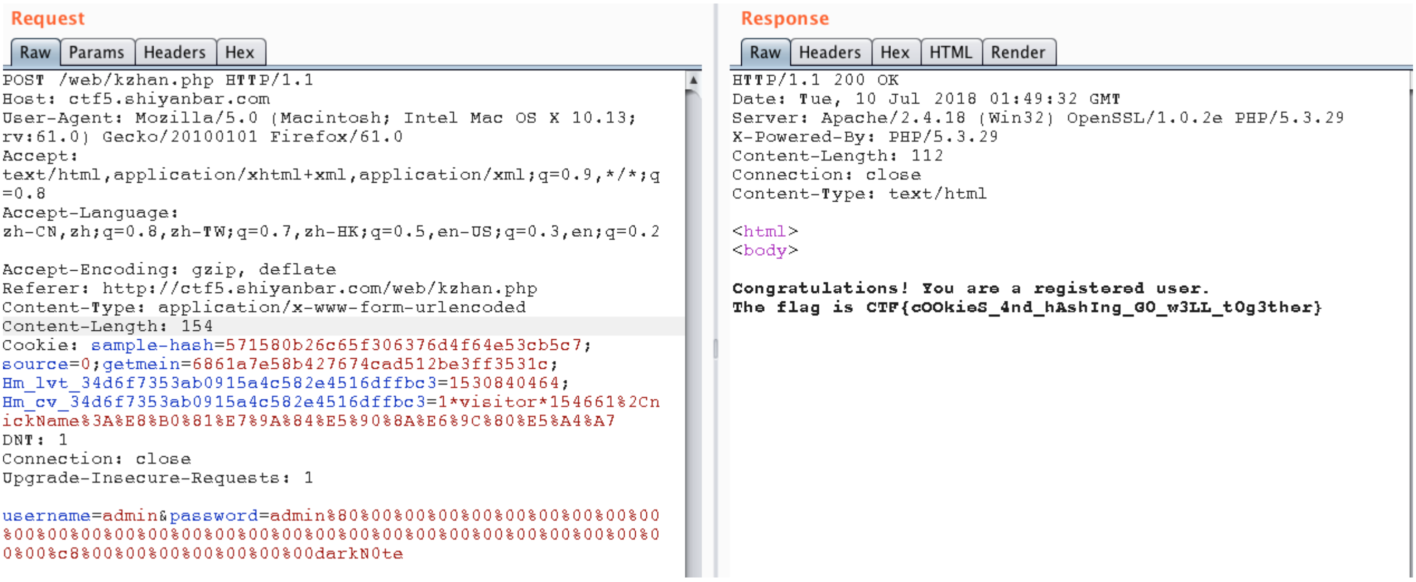
从源码分析，可以看到flag的获取要求是：传进一个cookie `getmein`,使其等于 `secret+urldecode(username . password)` MD5 加密后的结果且要求username为admin，password不能为admin。所以这里利用了hash长度扩展攻击，具体原理请参考文章0、文章1、文章2、文章3，推荐查看文章0和3。

这里我给出一个最简单的方式，使用工具`hashpumpy`进行hash值进行构造，给出代码

```
#!/usr/bin/env python
#-*- coding: utf-8 -*-
"""
@Author : darkN0te
@Create date : 2018-07-10
@description : 哈希长度攻击
@Update date :
"""

import hashpumpy

# def hashpump(hexdigest, original_data, data_to_add, key_length) aaa = hashpumpy.hashpump("571580b26c65f30
```



拐弯抹角

题目链接
http://shiyanbar.com/ctf/1846

题目描述

```
如何欺骗服务器，才能拿到Flag?
格式：CTF{}
```

解题思路
访问链接`http://ctf5.shiyanbar.com/indirection/index.php/index.php`，就可以直接获取到flag。
题目的意思就是通过改变地址栏访问index.php，但是限制了条件不能使用`./ ../ \\`而且只能使用小写字母，不可以在php后加点，这里我们可以利用伪静态技术，使用index.php后的index.php会被当做参数处理，所以服务器只会解析第一个index.php，满足条件成功绕过。

Flag: CTF{PSEDUO_STATIC_DO_YOU_KNOW}

Forms

题目链接
http://shiyanbar.com/ctf/1819

题目描述

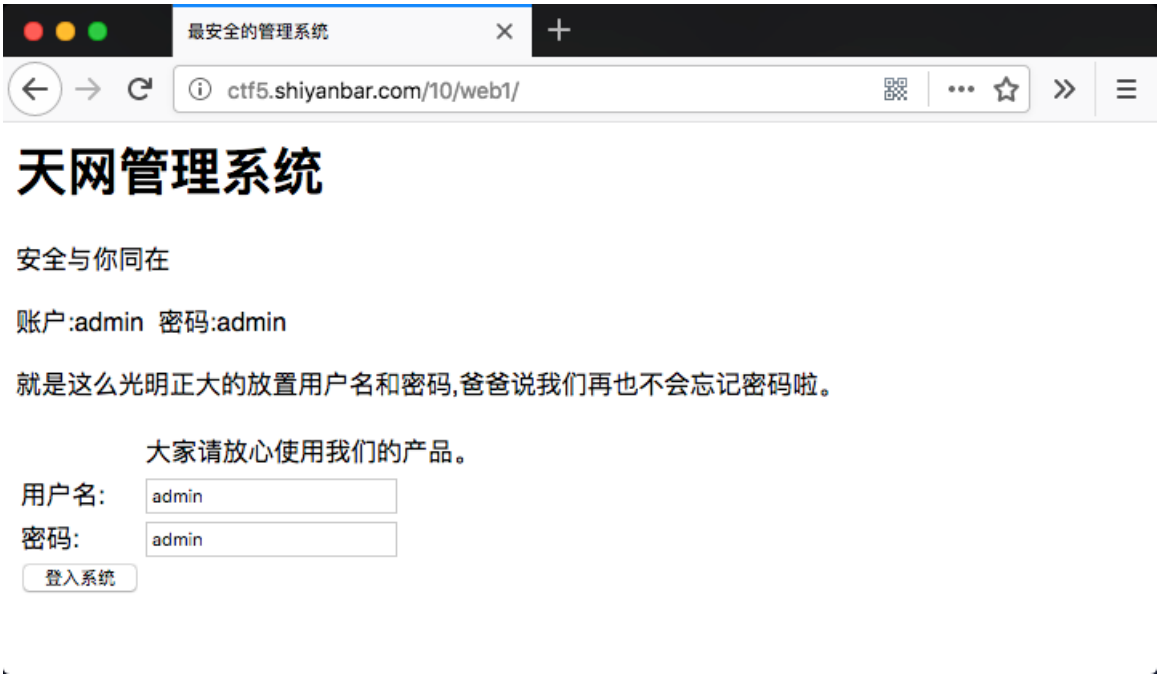
似乎有人觉得PIN码是不可破解的，让我们证明他是错的。
格式：ctf{}

解题思路
进入题目后，点击提交，使用bp拿到包后，发现有一个showsource字段，修改为1然后看到源码，直接把-198277477361611283128371616617277737161667272726161490018238 47填入pin提交拿到Flag。

```
<html>
<head>
<title>Forms</title> </head> <body> <pre> $a = $_POST["PIN"]; if ($a == -19827747736161128312837161661727773716166727272616149001823847
```

天网管理系统

题目链接
http://shiyanbar.com/ctf/1810



题目描述

天网你敢来挑战嘛
格式：ctf{ }

解题思路
进入题目后，打开网页源码，网页中有提示<!-- test=_GET['username']; test=md5(test); if($test=='0') -->，很明显可以看到是一个Hash比较问题，具体内容请查看文章 PHP Hash比较缺陷，这里我们只需要找到以0e开头的md5，这样和0比较就是相等的。下面一个以0e开头的md5列表

```
QNKCDZO
0e830400451993494058024219903391

s878926199a
0e545993274517709034328855841020

s155964671a
0e342768416822451524974117254469

s214587387a
0e848240448830537924465865611904

s214587387a
0e848240448830537924465865611904

s878926199a
0e545993274517709034328855841020
```

使用s878926199a提交后给出了新的提示。

打开链接看到内容

```
$unserialize_str = $_POST['password'];
     $data_unserialize = unserialize($unserialize_str); if($data_unserialize['user'] == '???' && $data_unse
```

这段语句首先对password字段进行了反序列化，然后让里面的user等于???，同时pass也等于???。
但是我们不知道两处???到底是什么，因此无法考虑用php函数构造这样的值。别忘了还有一个提示： "伟大的科学家php方言道：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。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）
构造password值为： a:2:{s:4:"user";b:1;s:4:"pass";b:1;}
在密码栏中提交构造的值，即可获取flag: ctf{dwduwkhduw5465}

忘记密码了

题目链接
http://shiyanbar.com/ctf/1808

题目描述

```
找回密码
格式：SimCTF{ }
```

解题思路
此题目有点脑洞，首先在step1.php页面提交邮箱，会给出step2.php页面，然后访问step2.php会马上返回step1.php。所以抓包看一下step2.php的内容。

```
<br />
<meta http-equiv=refresh content=0.5;URL="./step1.php">check error!<!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>
</head>
<body>
    <form action="submit.php" method="GET">
        <h1>找回密码step2</h1>
        email:<input name="emailAddress" type="text" value="youmom"  disable="true"/></br>
        token:<input name="token" type="text" /></br>
        <input type="submit" value="提交">
    </form>
</body>
</html>
```

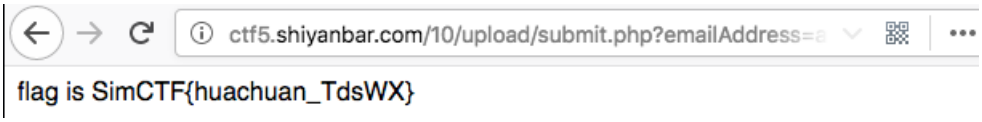
找到了step2.php会将内容提交到submit.php。访问submit.php文件。给出提示

在step2.php的代码中刚好能找到``，构造包访问`submit.php`还是不可以。这里就是个坑，需要访问submit.php的缓存文件`.submit.php.swp`，这个文件是使用vim编辑时会留下的一个文件，访问后得到submit.php源码。

```
if(!empty($token)&amp;&amp;!empty($emailAddress)){
    if(strlen($token)!=10) die('fail'); if($token!='0') die('fail'); $sql = "SELECT count(*) as num from `u
```

这段源码就给出了如何拿到flag，有两个条件：
1. `token`，长度必须等于10。
2. `token`要和`0`相等，这里又用到了php弱类型比较，只要用`0000000000`就可以绕过这两条限制。

得到payload：`http://ctf5.shiyanbar.com/10/upload/submit.php?emailAddress=admin@simplexue.com&token=0000000000` 。



flag is SimCTF{huachuan_TdsWX}

Once More

题目链接
http://shiyanbar.com/ctf/1805

题目描述

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{

解题思路
点击题目页面View the source code，看到源码。

```
<?php
if (isset ($_GET['password'])) {
    if (ereg ("^[a-zA-Z0-9]+$", $_GET['password']) === FALSE) { echo '<p>You password must be alphanumeric<
```

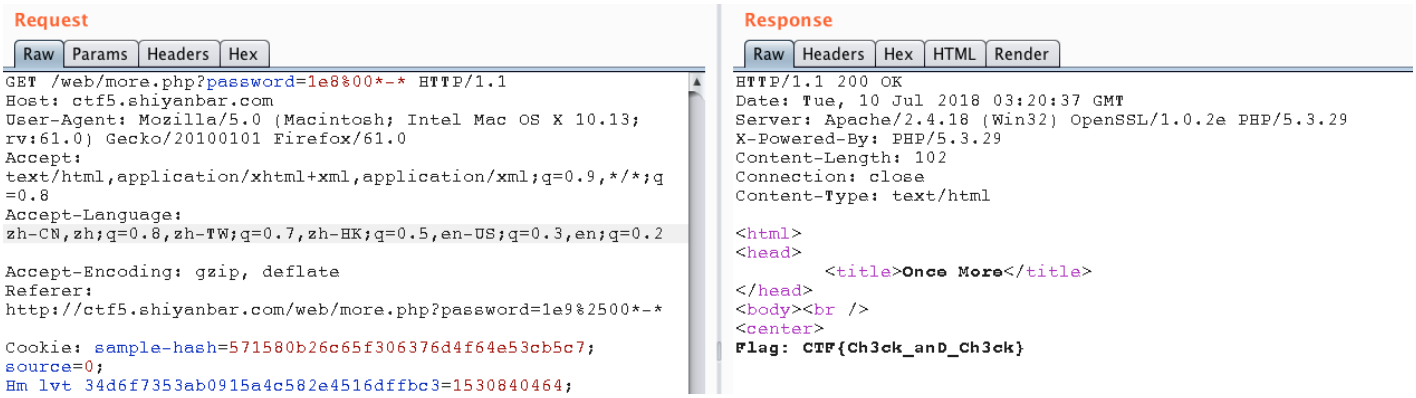
本题目一共有三个条件限制，看如何绕过。
1. ereg ("^[a-zA-Z0-9]+", _GET['password']) === FALSE

> ===类型恒等于
> == 和 != 比较若类型不同，先偿试转换类型，再作值比较，最后返回值比较结果 。
> 而
> === 和 !== 只有在相同类型下,才会比较其值。
> ereg()函数用指定的模式搜索一个字符串中指定的字符串,如果匹配成功返回true,否则,则返回false

这个判断限制了输入只能为只能输入字符和数字，但是该函数存在00截断漏洞。

2. strlen($_GET['password']) 9999999，限制字符串长度小于8，值大于9999999。
3. strpos ($_GET['password'], '*-*') !== FALSE，限制输入的值必须包含*-*。

所以给出paylload，1e8%00*-*，1e9%00*-*。

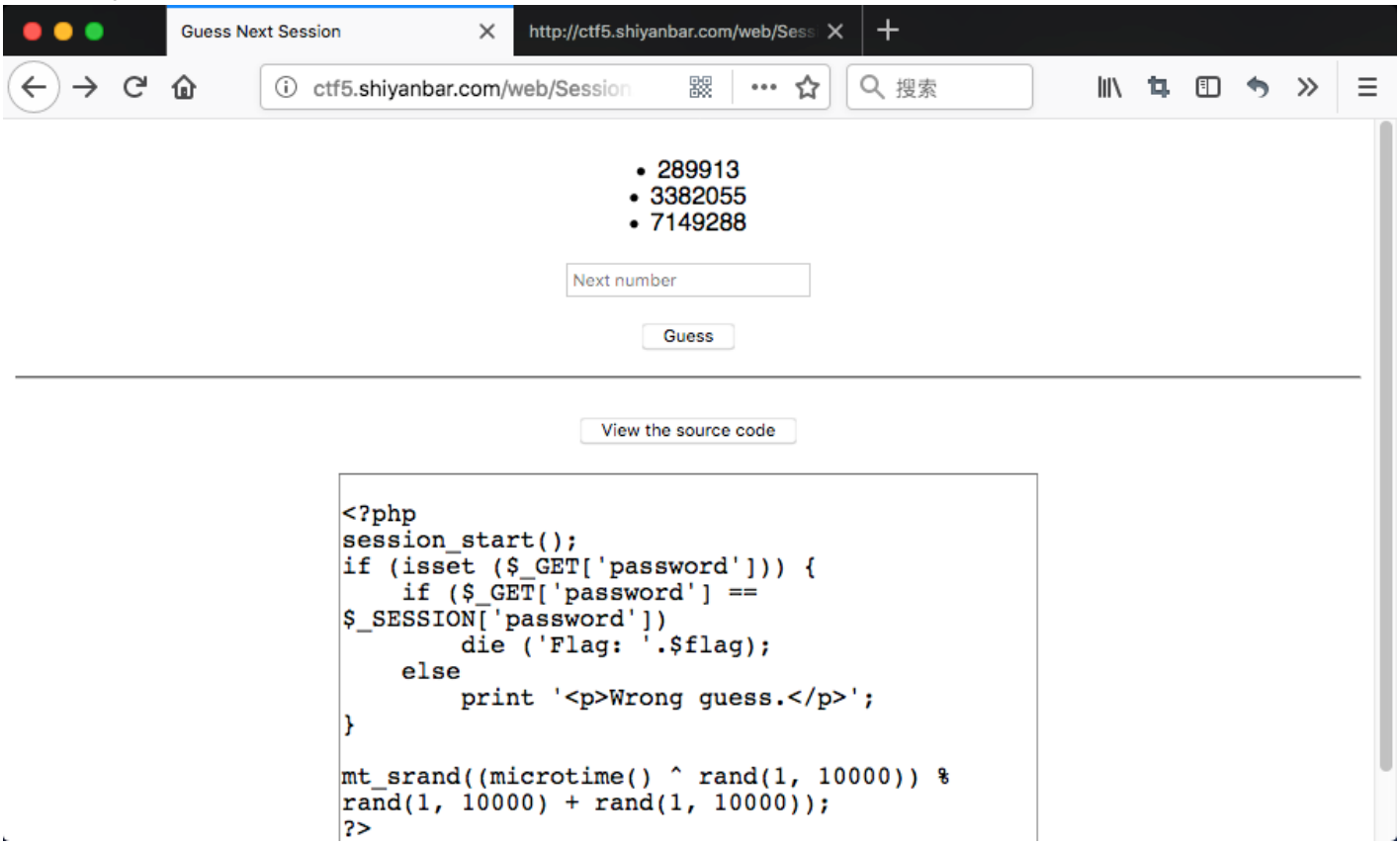


Flag: CTF{Ch3ck_anD_Ch3ck}

Guess Next Session

题目链接

http://shiyanbar.com/ctf/1788



题目描述

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？

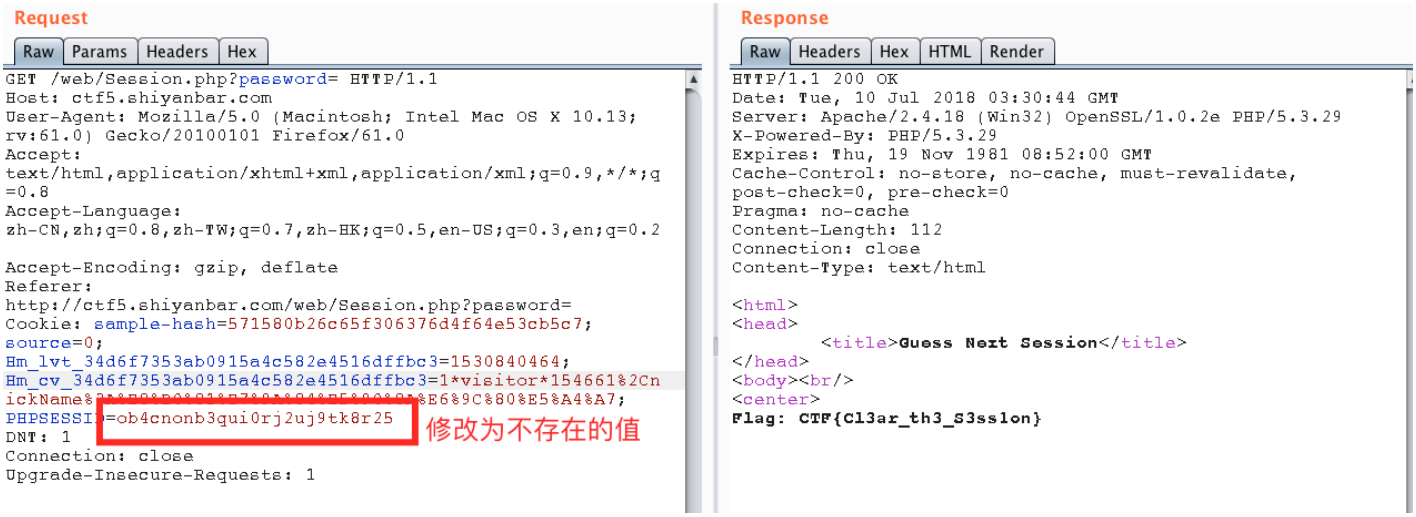
格式：CTF{}

解题思路

点击题目页面View the source code，看到源码。

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

看一下按条件语句，需要session中的password值和用户传的一样，就可以打印flag，所以只需要删掉session值，或者修改session值为一个不存在的session，服务器获取不到session，则password为空，用户传一个空的password的进去即可拿到flag。

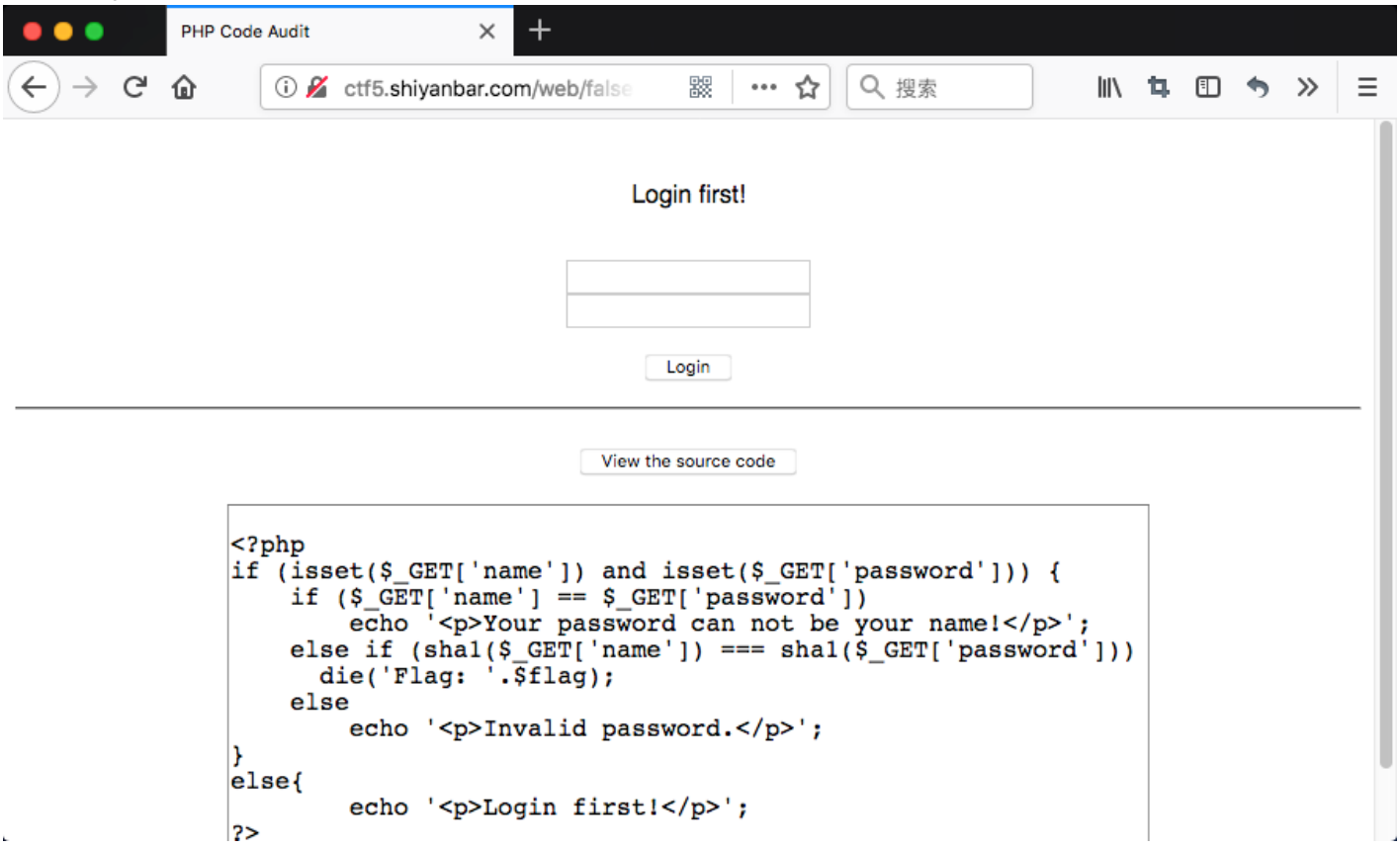


Flag: CTF{Cl3ar_th3_S3ss1on}

FALSE

题目链接

http://shiyanbar.com/ctf/1787



题目描述

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{}

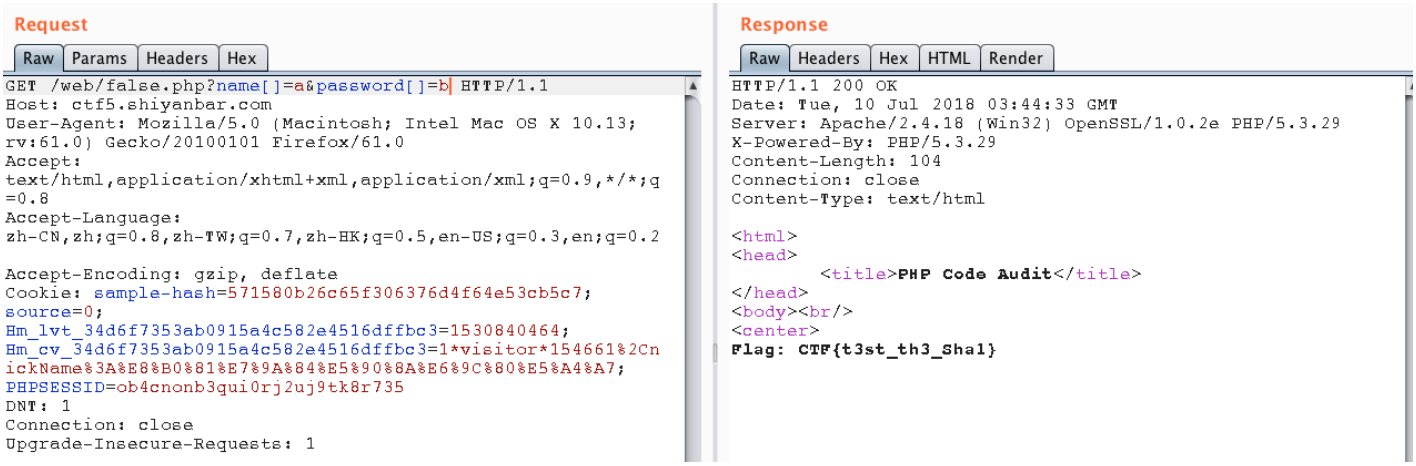
解题思路

点击题目页面View the source code，看到源码。

```
<?php
if (isset($_GET['name']) and isset($_GET['password'])) { if ($_GET['name'] == $_GET['password']) echo '<p>Y
```

本题目给出了两个条件
1. 用户名密码不能相等
2. 用户名密码的sha1()要===

===只有在相同类型下,才会比较其值。sha1()函数默认的传入参数类型是字符串型，可以传入其他类型，使其返回值为false。如数组类型。
所以给出payload为，`name[]=a&password[]=b`。



Flag: CTF{t3st_th3_Sha1}

转载于:https://www.cnblogs.com/beijibing/p/10393314.html