“百度杯”CTF比赛 十月场 writeup

原创

Senimo_ 于 2019-08-17 13:42:06 发布 2040 收藏 3

分类专栏： 各CTF平台 Writeup 文章标签： 百度杯 十月场 writeup CTF

本文链接：https://blog.csdn.net/weixin_44037296/article/details/99651360

各CTF平台 Writeup 专栏收录该内容

16 篇文章 6 订阅

订阅专栏

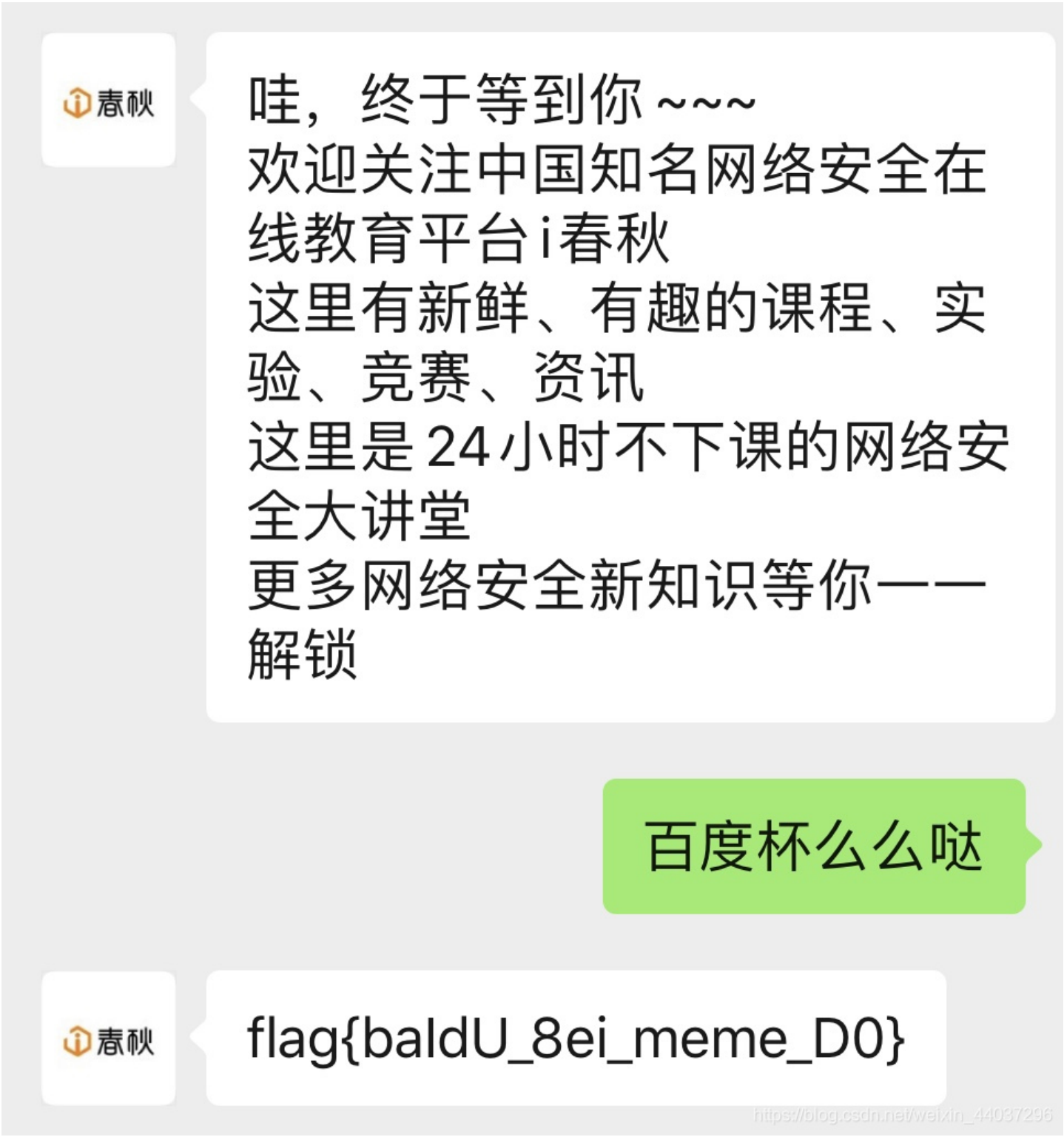
“百度杯”CTF比赛 十月场 writeup

Misc

签到题

分值：10分
题目内容：
对百度杯用时下最流行的表白
（去调戏i春秋公众号）
大声说出你的爱！！！

关注i春秋公众号，发送`百度杯么么哒`，即可获得flag：



那些年我追过的贝丝

分值：10分
题目内容：
贝丝贝丝，我爱你（大声循环2的6次方ing）
ZmxhZ3tpY3FlZHVfZ29nb2dvX2Jhc2U2NH0=

根据提示**2的6次方**，判断为**Base64编码**，在线Base64解码得到**flag**：`flag{icqedu_gogogo_base64}`。

我要变成一只程序员

分值：10分
题目内容：
输入：ba1f2511fc30423bdb
再运行一下
就会有惊喜哦！！
题目地址
解压文件得到一段代码：

```
#include<stdio.h>
#include<string.h>
void main() {
    char str[100]="";
    int i;
    int len;
    printf("input string:\n");
    gets(str);
    len=strlen(str);
    printf("result:\n");
    for(i=0;i<len+1;i++)
    {
        putchar(str[len-i]);
    }
    printf("\n");
}
```

在支持**C语言**的编译器中，运行代码，输入：`ba1f2511fc30423bdb`，得到flag：`bdb32403cf1152f1ab`，直接提交即可。

剧情大反转

分值：10分
题目内容：
}~144_0t_em0c14w{galf

根据提示：**大反转**，观察得出结尾`galf`字样，将首尾反转即可得到flag：`flag{w41c0me_t0_441~}`

challenge

分值：10分
题目内容：
666c61677b686578327374725f6368616c6c656e67657d

判断为**十六进制**，在线十六进制转字符，得到**flag**：`flag{hex2str_challenge}`。

传说中的签到题

小编保证这次是正常的签到题。
按例，继续调戏小i公众号
输入关键词“答案在哪里”
就能获得你想要的。
诺！扫码直接关注

关注公众号`i春秋`后回复关键字“**答案在哪里**”，推断出**flag**为：`什么`，直接提交关键字即可：

听说是rc4算法

分值：10分

题目内容：key welcometoicqedu

密文UUyFTj8PCzF6geFn6xgBOYSvVTrbpNU4OF9db9wMcPD1yDbaJw==

try again

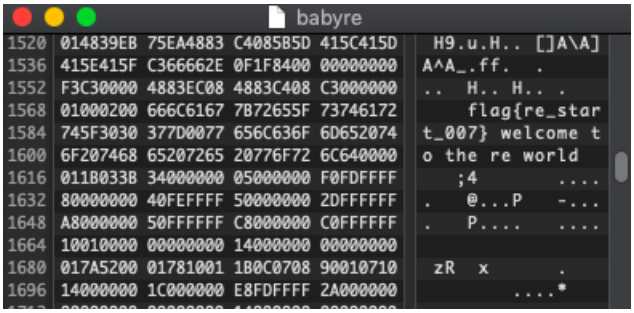
分值：10分

题目内容：

try to find the flag

题目地址

下载得到一个二**进制**文件，将其放入到**Hex Fiend**中，找到**flag**：`flag{re_start_007}`



表姐家的签到题

分值：10分
出题人表示金盆洗手
不坑任何参赛选手
干脆利落，直接奉上答案
就是
123456abcdef

flag内容已经给出，加上正确格式即可。

泄露的数据

分值：10分
题目内容：
听说这是某个数据库的泄漏的重要数据
25d55ad283aa400af464c76d713c07ad，试着找出原始key吧。
flag{key}

判断为**MD5**加密，在线MD5解密，得到**flag**：`flag{12345678}`

考眼力

分值：10分
题目内容：
gmbh{4d850d5c3c2756f67b91cbe8f046eebd}
try to find the flag

根据`gmbh`推断出原字符内容只需要根据给出字符串中，每个字母的**ASCII编码-1**，即可得到**flag**：`flag{4c850c5b3b2756e67a91bad8e046ddac}`

f	l	a	g

f	l	a	g
102	108	97	103
g	m	b	h
103	109	98	104

flag格式

分值：10分
题目内容：
你真的知道flag格式吗？
尝试提交flag{0ahief9124jfjir}

规范flag格式，**flag**已经给出：`flag{0ahief9124jfjir}`

Web

Login

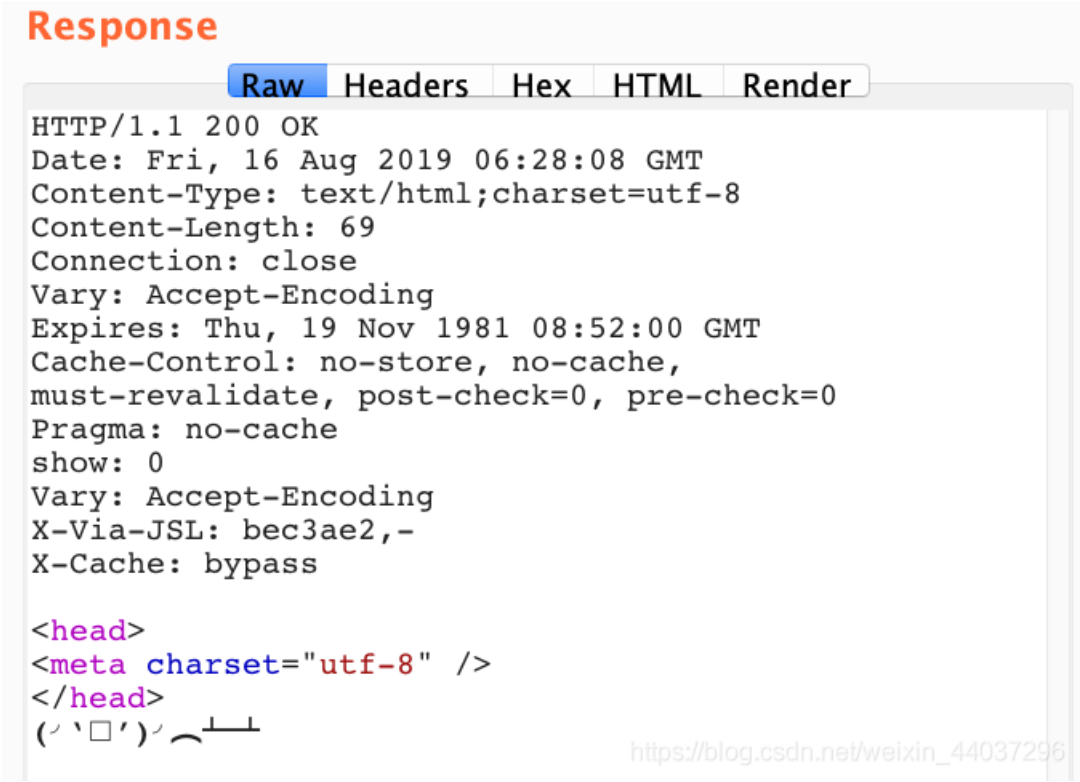
分值：50分

题目内容：

加油，我看好你

本题由擂主Wfox提供

进入后为登陆界面，查看网页源码，在最底部发现提示：`<!-- test1 test1 -->,` 登陆后显示：(ﾉ ｀□′)ﾉ ┻┻，Burp Suite抓取数据包，Send to Repeater后，发送数据包，在Resopnse中找到可以的头信息`show=0`：



将`show=1`添加到Request请求中，重新发送数据包，得到一段源代码：

```php
<?php
include 'common.php';
$requset = array_merge($_GET, $_POST, $_SESSION, $_COOKIE);

class db
{
    public $where;
    function __wakeup()
    {
        if (!empty($this->where)) {
            $this->select($this->where);
        }
    }
    function select($where)
    {
        $sql = mysql_query('select * from user where ' . $where);
        return @mysql_fetch_array($sql);
    }
}
if (isset($requset['token'])) {
    $login = unserialize(gzuncompress(base64_decode($requset['token'])));
    $db = new db();
    $row = $db->select('user=\'' . mysql_real_escape_string($login['user']) . '\'');
    if ($login['user'] === 'ichunqiu') {
        echo $flag;
    } else if ($row['pass'] !== $login['pass']) {
        echo 'unserialize injection!!';
    } else {
        echo "(ノ ˘ □ ˘)ノ ┻┻ ";
    }
} else {
    header('Location: index.php?error=1');
}
?>
```

分析代码：需要向`common.php`页面发送Request请求，传入变量`token`，先对传入的数据进行Base64解码，再解压缩压缩字符串，再反序列化变量，判断`user`是否等于`ichunqiu`。
根据所需构造PHP脚本：

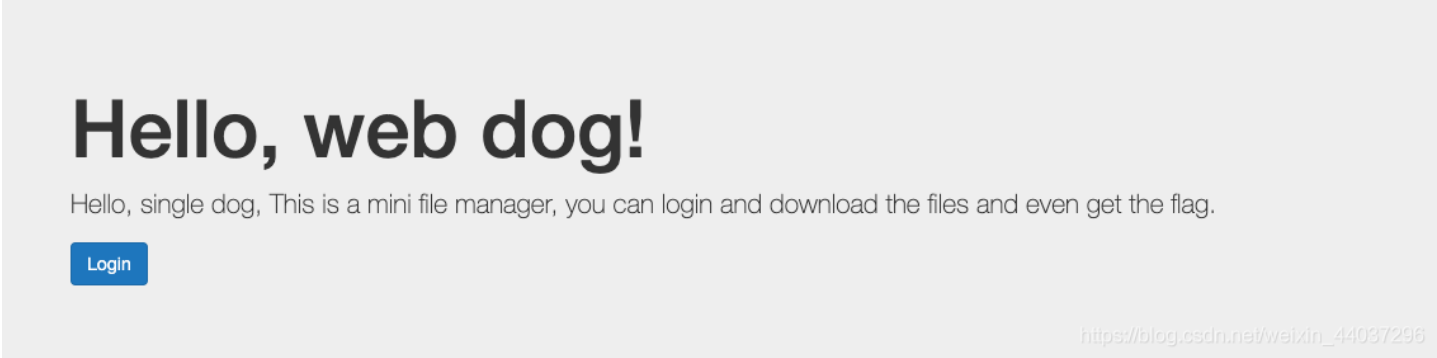
```php
<?php
$a = array('user' => 'ichunqiu');
$b = base64_encode(gzcompress(serialize($a)));
echo $b
?>
```

得到：`eJxLtDK0qi62MrFSKi1OLVKyLraysFLKTM4ozSvMLFWyrgUAo4oKXA==`
使用Burp suite构造Cookie的值：`token=eJxLtDK0qi62MrFSKi1OLVKyLraysFLKTM4ozSvMLFWyrgUAo4oKXA==`，发送数据包得到flag

Backdoor

GetFlag

分值：50分
题目内容：
一步一步一步的靠近它
本题来自擂主bingtangguan

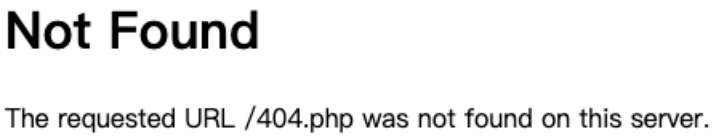


进入页面后显示：**这是一个迷你文件管理器，可以登录和下载文件甚至获得flag。**

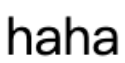
尝试登陆，

Not Found

分值：50分
题目内容：The requested URL…



提示页面找不到，访问给出的`/404.php`：



Vld

EXEC

登录

Gift

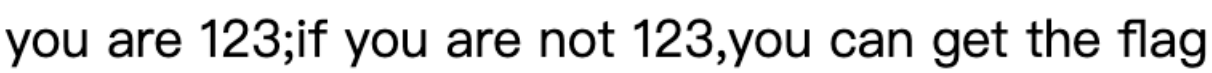
fuzzing

Try

Hash

分值：50分
题目内容：这只是第一步，然后呢？
启动靶机，打开网页：

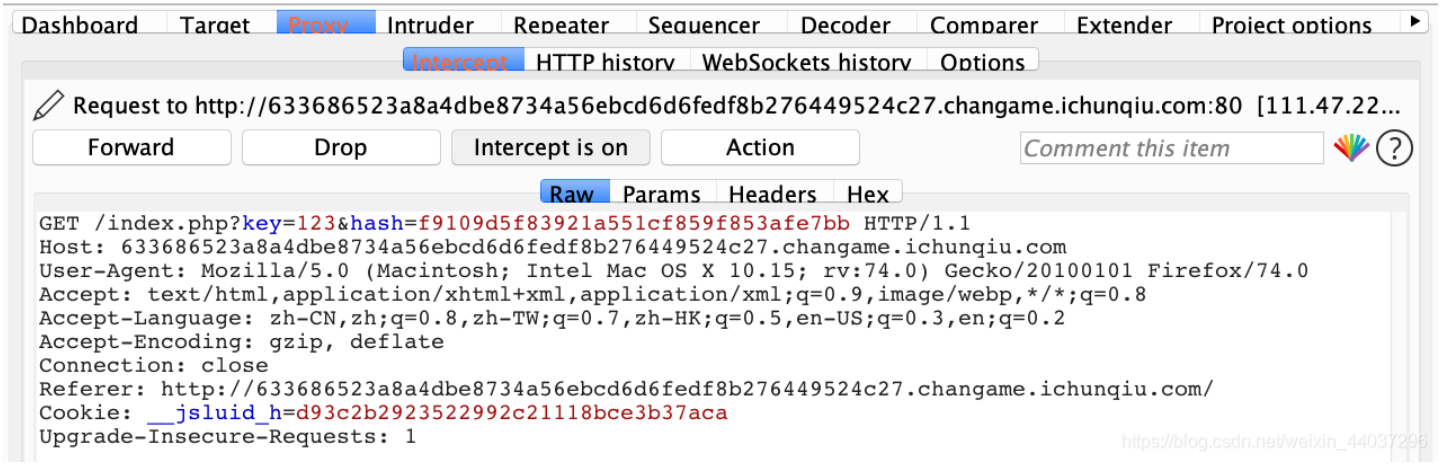
点击`hahaha`跳转：



查看网页源码：

```
you are 123;if you are not 123,you can get the flag<br>
<!--$hash=md5($sign.$key);the length of $sign is 8
```

得到`hash`原码，通过**BurpSuite**抓取数据包：



可以看到传入的参数为`key`和`hash`，解密`hash`的值：

得到加密中`$sign`的值：`kkkkkk`

Nothing