

web

这TM是啥

JSFUCK

去掉头部和尾部括号，拖到控制台运行，得到FLAG

```
"var f = "hctf{j5fuck_lz_ml233}~"; alert("Hack by LoRexxar, 你的flag被我拿走了")"
```

我是谁我在哪

观察地址为index.html 修改为index.php在头文件中获得FLAG

URL	状态	域
GET index.php	302 Moved Temporarily	115.28.78.16:1333
头信息 响应 HTML 缓存		
响应头信息 原始头信息		
Connection	keep-alive	
Content-Type	text/html	
Date	Sat, 21 Jan 2017 12:44:51 GMT	
Location	index.html	
Server	nginx	
Transfer-Encoding	chunked	
X-Powered-By	PHP/5.4.41	
flag	hctf{1t_iz_4_4mall_trlck}	

不可能的数字

代码分析如下

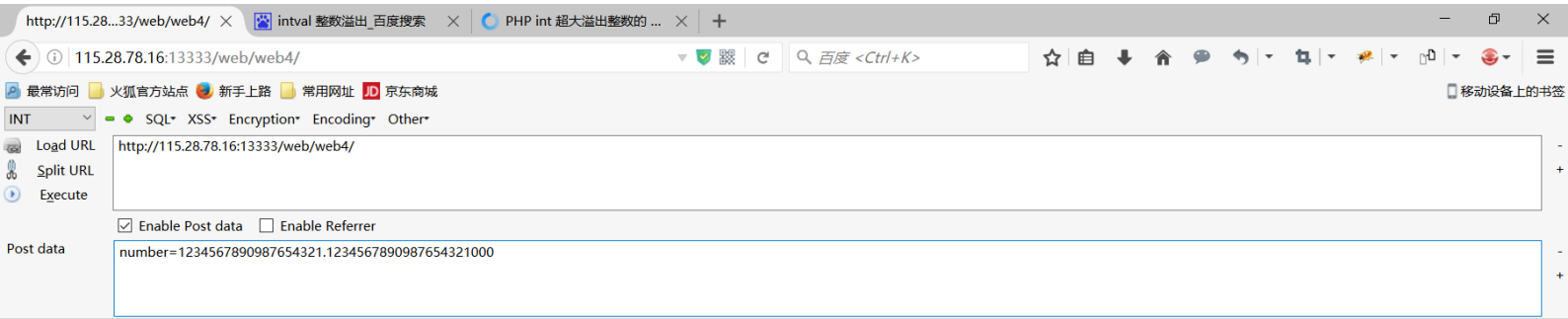
```
<?php
if(empty($_POST)){
    highlight_file(__FILE__);
    exit;
}
include_once("flag.php");

function is_palindrome_number($number) {
    $number = strval($number);
    $i = 0;
    $j = strlen($number) - 1;
    while($i < $j) {
        if($number[$i] != $number[$j]) {
            return false;
        }
        $i++;
        $j--;
    }
    return true;
}

$n1 = intval($req["number"]); //转换为10进制
$n2 = intval(strrev($req["number"])); //翻转字符串再10进制

if($n1 && $n2) {
    if ($req["number"] != intval($req["number"])) {
        $info = "number must be integer!"; //检测是否为整数
    } elseif ($req["number"][0] == "+" || $req["number"][0] == "-") {
        $info = "no symbol!"; //别TM带符号
    }
    elseif ($n1 != $n2) //翻转字符串后转化成的整数值相同 first check
    {
        $info = "no, this is not a palindrome number!";
    }
    else
    {
        //second check
        if(is_palindrome_number($req["number"])) //经过函数后返回false second check
        {
            $info = "nice! {$n1} is a palindrome number!";
        }
    }
}
```

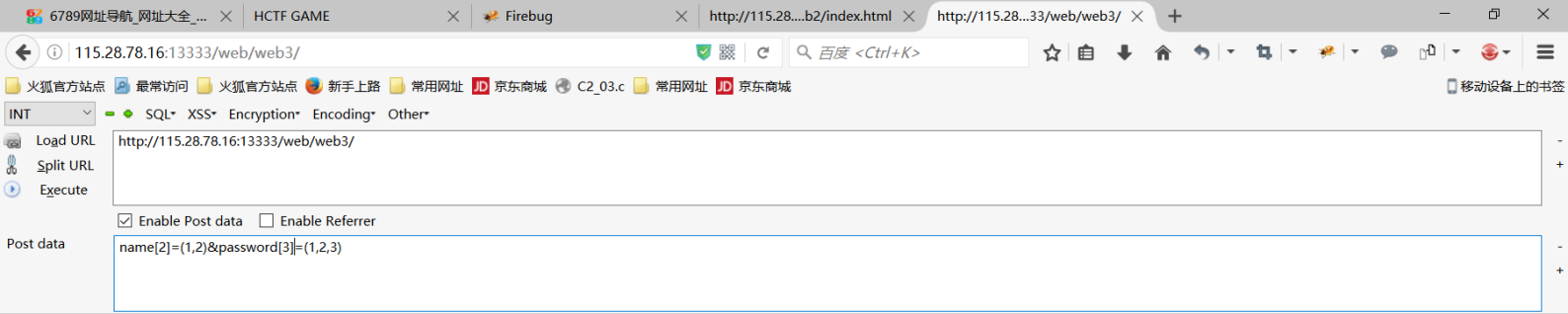
查百度了解intval有两个致命漏洞 一个是整数值溢出 一个是在遇到第一个非0数字字符时才开始转换 使用第一个漏洞 传一个很大的数字



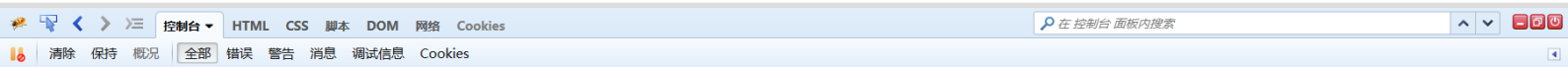
find a strange dongxi: hctf{go0d_job_intv4l_iz_g00d}



不可能拿到的FLAG
要求name和password不同
两个参数传回的sha1返回值相同
一开始想到sha1碰撞，搜了下发现不太可能==
然后想到上传个数组
上传数组，轻松拿到FLAG



Flag: hctf{o0k!!g3t_f14g_s0_ez}



```

1  <?php
2  if(empty($_POST)){
3      highlight_file(__FILE__);
4      exit;
5  }
6  include_once("flag.php");
7
8  $a= "0.1";
9  $b= $_POST['b'];
10 if($b != ''){
11     if(is_array($b)){
12         echo "Something error!";
13         exit;
14     }//不能是数组
15     else if(!is_numeric($b)){//不能是数字或数字串
16         $c  = (int)(( $a + $b) * 10);
17         if($c == "8" && $b[10] == false){
18             echo $flag;
19         }
20         else{
21             echo $c;
22             exit;
23         }
24     }
25     else{
26         echo "something error!";
27     }
28 }
29 else{
30     echo  "something error";
31 }
32
33 ?>

```

强制类型转化，要求c最后结果为8
 随便找了个在线PHP测试网站
 得到符合要求的值

还原到默认code

```

1  <?php
2
3
4  $a= "0.1";
5  $b= "0.77 | 0";
6  $c=(int)(( $a+$b)*10);
7  echo $c;
8
9  ?>

```

run (ctrl+r)

copy

分享当前代码

出现故障，请使用这个[点击这里](#)

☐ 文本方式显示 ☒ html方式显示

MISC

Z神图库3

我明明拿到FLAG了为什么不让我交==，100分没了啊otz
binwalk分析文件
发现文件藏着一个PNG
提取之
发现一个㊟



Stegsolve打开文件，检查0通道，发现头部有奇怪的字符串
以等号结尾，base64解码之。
拿到FLAG

base64

```
hctf{lsb_aabbb_iz_ezzzzzz}
```

交FLAG提示我错误==迷

渗透

我的电脑入群题= =

T

SQLXSSEncryptionEncodingOther

Load URL

Split URL

Execute

http://115.28.78.16:13333/pentest/01/?hacker=HelloGet

☒ Enable Post data

☐ Enable Referrer

st data

hacker=HelloPost

2 http头

使用工具

Modify Headers

Add, modify and filter HTTP request headers

更多

选项

禁用

移除

RefControl

针对每个站点送出想要的 HTTP Referer.

更多

选项

禁用

移除

User Agent Switcher

Adds a menu and a toolbar button to switch the user agent of a browser.

更多

选项

禁用

移除

X-Forwarded-For Header

Inserts X-Forwarded-For field into the HTTP header

更多

选项

禁用

移除

其实这一个就够了

Connection

keep-alive

Content-Encoding

gzip

Content-Type

text/html

Date

Sat, 21 Jan 2017 13:07:07 GMT

Server

nginx

Transfer-Encoding

chunked

Vary

Accept-Encoding

X-Powered-By

PHP/5.4.41

flag

hctf{h77p_He4dEr_50_E4sy_AND_fUn_ohhouhou}

请求头信息

原始头信息

Accept

text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding

gzip, deflate

Accept-Language

zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3

清除

保存

全部

HTML

CSS

Javascript

XHR

图片

插件

媒体

字体

GET /pentest/02/ HTTP/1.1
Host: 115.28.78.16:13333
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 9_1 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13B143 Safari/601.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Forwarded-For: 127.0.0.1
X-real-ip: 127.0.0.1
remoteAddress: 127.0.0.1
Referer: google.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

头文件发现FLAG

3cookie

观察头文件看到提示 admin=1 isLogin=tur

控制台直接使用指令

```
document.cookie="admin=1"
```

```
document.cookie="isLogin=tur"
```

拿到flag

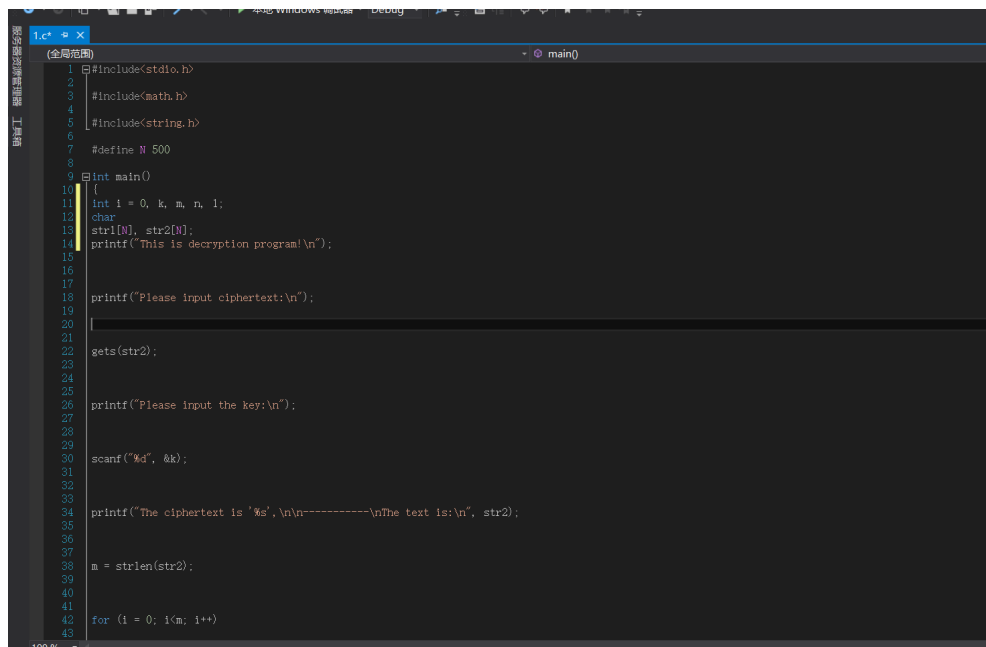
flag: hctf{hao_hao_kan_zi_liao!!!}, 通过伪造cookie, 你可以绕过一些限制, 或是伪造身份。

密码

入门2

凯撒移位 5位

网上找了个脚本



```
1 #include<stdio.h>
2
3 #include<math.h>
4
5 #include<string.h>
6
7 #define N 500
8
9 int main()
10 {
11     int i = 0, k, m, n, l;
12     char
13     str1[N], str2[N];
14     printf("This is decryption program!\n");
15
16
17     printf("Please input ciphertext:\n");
18
19     |
20
21     gets(str2);
22
23
24     printf("Please input the key:\n");
25
26
27     scanf("%d", &k);
28
29
30     printf("The ciphertext is '%s',\n\n-----\n\nThe text is:\n", str2);
31
32
33
34     m = strlen(str2);
35
36     For (i = 0; i<m; i++)
37
38
39
40
41
42
43
```

hgame{Caesar_cipher_3s_just_for_fun}

一开始推测为1s=

把3改1提交成功

后来才知道数字和字母处理不同==