

0x01:密码学教室入门(一)

首先基于wiki上的实例了解了一波RSA, 然后发现题目所有的信息都有了套公式 $m = c^d \bmod p \cdot q$

然后就用bigintergercalculator 进行计算得出

X	728810842183877139396627111919284569323810228050451291485184320938445 987041656719925456815243467153869759508961782819985243104277960595933 408946505760177712197503214523385
CL	
Y	62409428588657515654582049950308797806016514893335982245
n	
CL	
Z	326954354802240245138938195943897207094307177798068097946378257215236 480874313807929075588470385220105129315155449503167591418461617557239 390449061786134606203927421945159
CL	
A	0
CL	
B	0
LCM	
Rem.	
CL	
GCD	2559974471936860919458779092210355700644412555441745764733
Ans	
CL	
TO V	

再转成16进制, 由于该有的信息都有了最后解出来一个:0x6867616d657b7273615f31735f763372795f65347379217d

再用converter 转化一下

输出(转换值):
hgame{rsa_1s_v3ry_e4sy!}

Flag:hgame{rsa_1s_v3ry_e4sy!}

0x02:密码学教室入门(二)

这是关于凯撒密码的题目:

直接放在在线解密网站crptool-online上

Klartext:
hgame{Caesar_cipher_8s_just_for_fun}
<input type="radio"/> Verschlüs
<input checked="" type="radio"/> Entschlüs

感觉这就是答案 测试一波 不对 说明数字和符号有问题

基于基本的Flag提交格式目测符号是不做改动的 那数字就0-9

而求感觉上1配上这段英文比较靠谱 测试一波果然

Flag:hgame{Caesar_cipher_1s_just_for_fun}

0x03:密码学教室番外篇

这题和上面是一个套路 不过数字必须一个个试了试到第5次答案就对了
Flag:hgame{dgfdyhcry42287235413//+/%}

0x04:密码学教室入门(四)

这还是一道RSA的题目不过给的信息比较少 只有n,e,c 但是通过公式 $c = m^e \bmod n$

因为n非常大, e = 1可以看出如果m/n为1 那也是很大的一个数所以m/n =

0的可能性非常大-》c = m 再用converter转化一下

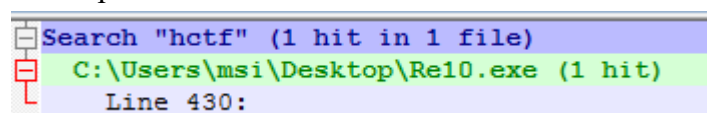
Flag:hgame{rsa_1s_still_e4sy_now!}

输出(转换值):

hgame{rsa_1s_still_e4sy_now!}

0x05:你看看, 逆向多简单

首先下载得到一个re(10).zip的压缩文件 打开后是一个.exe文件
用notepad++打开 然后搜索一波



然后就发现了惊喜
Flag:hctf{It_ls_T0o_ea5y!}

0x06:Explorer图库之一

首先下载得到一张.jpg的图片
用notepad++编辑 **BS**hctf{2e3e3}**!**就直接出来了
Flag:hctf{2e3e3}

0x07:Explorer图库之二

还是那张.jpg的图片 百度了不少解法 最后发现还拼接了一个文件

用Winhex打开找到FFD9将后面的所有块导入到新的.zip文件内 发现

解压开 用notepad++编辑 发现一个1.txt文件 该后缀为zip

打开 再打开.txt文件

文件(F) 编辑(E) 格式(O) 查看(V)
hctf{nizh1dao_tuzh0ngm4}

就可以看到Flag了

Flag:hctf{nizh1dao_tuzh0ngm4}

0x08:我是谁我在哪???

打开网站发现啥都没有 而且网站地址变了 F12打开后台发现还有一个.php
但是没什么发现 用burpsuite对http://115.28.78.16:13333/web/web2/index.php发起请求

Response中发现
X-Powered-By: PHP/5.4.41
flag: hctf{1t_iz_4_4mall_tr1ck}
location: index.html

Flag:hctf{1t_iz_4_4mall_tr1ck}

0x09:这TMD是啥?

打开链接 显示没有Flag 并弹出flag被盗 F12 是一段jsfuck的代码

就上控制台去document.write()一下 结果还是弹出flag被盗

然后问了一下弹窗内容是个玩笑 这我就懵逼了 别的jsfuck跑完就是答案

这个居然啥都没有 但提示的意思答案就在代码里

然后我就想破坏这个结构让他不弹窗。。。最开始我把开头去掉了一部分, 结果提示我错误, 然后我就把结尾的括号去掉了 然后就

function anonymous() { var f = "hctf{j5fuck_1z_m1233}"; alert("Hack by LoRexxar, 你

Flag:hctf{j5fuck_1z_m1233}

0x10:不可能拿到的Flag

```
jhh.sendPost("http://115.28.78.16:13333/web/web3/", "name[]=a&password[]=b" );  
}
```

百度搜索得到的sha1函数漏洞发送post请求就好了

```

public void sendPost(String urlAddress,String paramvalue/*传递参数的值*/
    try {
        //建立连接并发送请求
        HttpURLConnection urlConnection =null;
        URL url = new URL (urlAddress);
        urlConnection = (HttpURLConnection)url.openConnection();
        urlConnection.setDoOutput(true);
        urlConnection.setConnectTimeout(10000);
        urlConnection.setReadTimeout(10000);
        urlConnection.connect();

        PrintWriter pw = new PrintWriter(urlConnection.getOutputStream());
        pw.print(paramvalue);
        pw.flush();

        //获取内容
        BufferedReader bf = new BufferedReader(new InputStreamReader(
        String line = bf.readLine();
        while(line != null){
            System.out.println(line);
            line = bf.readLine();
        }
    }
}

```

Flag: hctf{o0k!!g3t_f14g_s0_ez}

Flag:hctf{o0k!!g3t_f14g_s0_ez}