html ctf查找,Web CTF 解题思路总结—南京邮电大学攻防平台writeup

转载

hi啊 于 2021-06-16 19:26:36 发布 149 收藏
文章标签： html ctf查找

1、直接查看源代码

例：签到题(50)

2、PHP的特性

(1)MD5 碰撞

例：md5 collision(50)

md5碰撞：MD5摘要算法可以从多个字节组成的串中计算出由32个字节构成的“特征串”，对于超过32字节的串来说，MD5计算得出的值必然是其一个子集，所以必然存在不同的串能够得出相同MD5值的情况，即碰撞。

在PHP中的MD5中的0e的比较：PHP在处理哈希字符串时，会利用“！=”或“==”来对哈希值进行比较，它把每一个以“0E”开头的哈希值都解释为0，所以如果两个不同的密码经过哈希以后，其哈希值都是以“0E”开头的，那么PHP将会认为他们相同，都是0。(详见：PHP Hash 缺陷)

$a不等于‘QNKCDZO'，但$a的MD5等于‘QNKCDZO'的MD5，这就很尴尬了。于是将‘QNKCDZO'MD5加密，发现(MD5在线加/解密)md5(QNKCDZO)=0E830400451993494058024219903391,结合上面PHP Hash缺陷，所以下一步很明显制造开头为“0e"的MD5字符串。0e开头MD5值 将所得的值加入到页面地址后就得到了flag。

3、

例：签到2(50)

查看页面源代码，发现口令“zhimakaimen”长度为11，而html源码限制的长度为10。很明显需要去除或者修改限制。

1)利用火狐浏览器的hackbar插件直接越过html代码

4、

例：这题不是WEB(100)

打开题目地址后有一张图片，猜想可能是图片隐藏题，将图片下载后用记事本打开，在最后发现flag。

5、

例：层层递进(100)

0.0脑洞题，查看源代码后发现iframe有问题，一步步点进去，最后到view-source:http://chinalover.sinaapp.com/web3/404.html，获得如下界面

于是，flag就这样出来了.....ntcf{this_is_a_fl4g}

6、

几种特别的加密方式：

ppencode/rrencode/jjencode/aaencode是Perl、Ruby、Javascript的小工具，可以将各自的代码进行混淆，转换成特殊字符，甚至还可以转换成有意思的表情。

ppencode-Perl：它可以把Perl代码转换成只有英文字母的字符串。Demo

rrencode-Ruby：它可以把ruby代码全部转换成符号。Demo

jjencode/aaencode-Javascript：前者将JS代码转换成只有符号的字符串，类似于rrencode，后者可以将JS代码转换成常用的网络表情。Demo

例：