南邮 部分 writeup

原创

G_goodstudy 于 2018-08-09 10:11:54 发布 296 收藏
分类专栏： ctf

1、签到题

这道题有点出乎意料的简单，题目地址打开后，先看页面源码发现flag就在源码中

nctf{flag_admiaanaaaaaaaaaaa}

2、web19

这道题主要是代码审计，看懂代码的意思。

php语言　将'QNKCDZO'经过md5加密之后的结果赋值给变量$md51 $a = @$_GET['a'] 以get的方式从用户端获取一个变量a, $md52 = @md5($a); 将变量$a经过md5加密之后的结果赋值给变量$md52

if(isset($a)) 判断变量$a的值是否为NULL，如过不为空，则继续执行括号内的代码，否则执行else之后的代码语句

3、签到2

bursuite抓包然后进行改包，go

flag is：nctf{follow_me_to_exploit}

4、web 100

这题不是web，打开地址之后是一个动态图，有可能是隐藏flag ，我刚开始看完源代码以为是需要修改图片大小，然后下载到桌面之后发现跟图片大小没关系，后来改变图片格式 .txt

nctf{photo_can_also_hid3_msg}

5、层层递进

刚开始没有思路，查看页面源码没有发现有什么问题，以为这个网站有后台，后台存在flag，后来不行，然后我就想是不是跟网站get请求有关，但是利用burpsuite抓包，得到了一个base64编码后的一串字符，解码后没什么用 ，然后继续查看源代码，发现里面还有隐藏的html文件，层层递进打开得到flag

6、AAencode

根据提示js解密在线，解密后是一堆颜文字，然后百度的writeup说是进浏览器控制台跑一遍，浏览器控制台解颜文字。 虽然我没解出来。。。。。。。。。。。

7、单身二十年

扯淡的小题目，进去之后查看源代码。代码提示，点击存在flag

nctf{yougotit_script_now}

8、你从哪里来

这道题题目给的也很清晰，查看题目地址后页面源码信息也没有可用的东西，are you from google

则可以知道这个题目要修改引用页。goole访问。修改referer 修改访问来自谷歌。但是现在一般的浏览器

不能访问外网，不一定可以成功，看你是否有vpn连接外网

获取flag

9、文件包含

文件包含需要构造语句在url后直接添加 file=php://filter/read=convert.base64-encode/resource=index.php，读取到base64加密的index.php文件

base64在线解密

得到flag nctf{edulcni_elif_lacol_si_siht}

10、Mysql

http://chinalover.sinaapp.com/web11/

根据题目提示打开robot.txt文件

然后这里面存在一个php文件，进行代码分析，查看代码就会知道这个代码最关键的依据，你get的数值id是不能id=1024，因为这样会no！ try again ，但是当你get的id=1025的时候页面会显示no more 那么这个就只能get一个id=1024.x这样才能得到sql.php文件的内容

得到flag nctf{query_in_mysql}

11、cookie

http://chinalover.sinaapp.com/web10/index.php

这个题目页面信息告诉你让你首先登陆，那么这个题目很明显是让你抓包然后登陆login=1

12、bypass again

http://chinalover.sinaapp.com/web17/index.php 很明显是代码审计， 那么就是get请求同时get一个a和一个b

http://chinalover.sinaapp.com/web17/index.php?a[]=1&&b[]=2

得flag nctf{php_is_so_cool}

13、/x00代码审计

http://teamxlc.sinaapp.com/web4/f5a14f5e6e3453b78cd73899bad98d53/index.php

明显 需要了解strpos函数的意思以及作用

是比较字符串的 然后看代码get一个

http://teamxlc.sinaapp.com/web4/f5a14f5e6e3453b78cd73899bad98d53/index.php?nctf[]=0#biuibiuibiu

14、变量覆盖

http://chinalover.sinaapp.com/web18/

extract()函数的作用:从数组中将变量导入到当前的符号表,该函数使用数组键名作为变量名，使用数组键值作为变量值。针对数组中的每个元素，将在当前符号表中创建对应的一个变量

15、上传绕过

http://teamxlc.sinaapp.com/web5/21232f297a57a5a743894a0e4a801fc3/index.html

上传php文件不支持，显示只能jpg文件，上传jpg显示只能php文件那么就想着进行截断。修改的内容是upload/后的内容，上传1.php.jpg 在这里截断。内容不需要考虑

在hex中修改截断得到flag

nctf{welcome_to_hacks_world}