WeChall-writeup-7-12.1(Warchall - The Beginning;Caterpillar)

原创

MeliodasC 于 2018-12-01 23:07:13 发布 828 收藏

分类专栏： WeChall 文章标签： WeChall writeup 安全

上了一下午实验课以后，晚上去看了《无名之辈》，感觉演员的演技和剧本都在线，是一部昆丁式的好作品~
这次总共有两道题，都会写的比较详细。

Training: Warchall - The Beginning

按照题目的提示，登陆进去以后发现有一个WELCOME.txt，看一下里面的内容。

```
dorisans@warchall ~ $ ls
level  WELCOME.txt
dorisans@warchall ~ $ cat WELCOME.txt
Welcome, challenger to warchall.net.

We hope to be able to present some more realistic challenges in a safe (or not so safe environment) and ho
pe you will like the project!

You will find the solution to each level in
/home/level
or
/home/user/yournick/level

=========================
== COOL ASCII ART HERE ===
=========================

noother,bsdhell,livinskull,kwisatz,gizmore,jjk,paipai,dloser,nurfed
(warchall.net)


NEW: checkout /home/features :)
```


嗯…说solution分别在两个文件夹下，就来分别看一下两个文件夹里面的内容。

-> 第一个文件夹：/home/level

```
dorisans@warchall ~ $ cd /home/level
dorisans@warchall /home/level $ ls
0   11          15_live_rfi  20_live_rce  8        matrixman  tropic  w2
1   12          16           21_nurxxed   kwisatz  mgine      w0      ynori7
10  14_live_fi  2            3            level9   space      w1
```

- -> level 0

```
dorisans@warchall /home/level/0 $ cat README.txt
```

```
Welcome to the WarChall box.
We hope you will learn a bit about linux systems here, and enjoy your stay.

================================
= All your activity is logged. =
================================
= If you find a way around our protections,
= please contact us!  =
= support@wechall.net =
=======================
We are looking for bitwarriors that can provide funny and educative challenges.
=======================

Oh .... and your solution to level0 is: "bitwarrior" without the quotes.
```


- -> level 1

一个一个打开找的...一开始看到一个文件以为说在black下，结果提示权限不够，向后再找了一个gray就找到了。（但感觉这样找很慢，于是去查了一波命令）

```
dorisans@warchall /home/level/1/blue/pill/hats/gray/solution/is $ cat SOLUTION.txt
Congratulations.

Your solution for this level is: LameStartup
```

- - >level 2

`ls -a` 可以看到文件夹内的隐藏文件

`grep -rn solution` 不指定目录地递归查找包含solution的信息并显示行号。选择solution是因为前两种答案中有这个关键词，猜测后面格式差不多。

使用grep搜索代码的几个示例

```
dorisans@warchall /home/level/2 $ ls -a
.  ..  .bash_history  .bash_logout  .bash_profile  .bashrc  documents  photos  .porb  .ssh
dorisans@warchall /home/level/2 $ grep -rn solution
.porb/.solution:1:The solution is HiddenIsConfig
grep: .ssh: 权限不够
.bash_history:8:nano .porb/.solution
```

->第二个文件夹：这里发现/home/user/yournick/level就是~/level

```
dorisans@warchall ~ $ cd ./level
dorisans@warchall ~/level $ ls
4  5  6
dorisans@warchall ~/level $
```

- -> level 3

做法同level 2

```
dorisans@warchall /home/level/3 $ grep -rn solution
grep: .ssh: 权限不够
.bash_history:1:The solution to SSH3 is: RepeatingHistory
dorisans@warchall /home/level/3 $
```

- -> level 4

ls -l 查看权限chmod命令详解

```
dorisans@warchall ~/level $ cd 4
```

```
dorisans@warchall ~/level/4 $ ls -a
.  ..  README.txt
dorisans@warchall ~/level/4 $ cat README.txt
cat: README.txt: 权限不够
dorisans@warchall ~/level/4 $ ls -l
总用量 4
---------- 1 dorisans dorisans 63 11月 29 14:31 README.txt
dorisans@warchall ~/level/4 $ chmod -rwx------ README.txt
dorisans@warchall ~/level/4 $ cat README.txt
cat: README.txt: 权限不够
dorisans@warchall ~/level/4 $ chmod +rwx------ REDAME.txt
chmod: 无法访问'REDAME.txt': 没有那个文件或目录
dorisans@warchall ~/level/4 $ chmod 700 README.txt
dorisans@warchall ~/level/4 $ cat README.txt
The solution to level 4 is 'AndIknowchown' without the quotes.
```


- -> level 5

```
dorisans@warchall ~/level/5 $ cat README.txt
Protect your /home/user/dorisans/level directory from other users. Then wait 5 minutes.
dorisans@warchall ~/level/5 $ ls -l
```

发现有一条提示，要求保护自己的权限，就把权限只设给自己就好啦。回到主目录 chmod 700 level，再去看level/5里面出现了一个solution文件。

```
dorisans@warchall ~/level $ cd ./5
dorisans@warchall ~/level/5 $ ls
README.txt  solution.txt
dorisans@warchall ~/level/5 $ cat solution.txt
cat: solution.txt: 权限不够
dorisans@warchall ~/level/5 $ chmod 700 solution.txt
dorisans@warchall ~/level/5 $ cat solution.txt
The solution to level 5 is 'OhRightThePerms', without the quotes.
```

ls -l文件权限解释

TIPS：答案注意是英文的逗号= =

Training: Caterpillar

首先拿010editor，stegslove轰炸了一通，没有拿到什么有用的结果。

然后就回到了我第一眼看到就猜的，是不是颜色对应着什么信息，毕竟不同的绿色特别显眼。然后就去请教了学广告的姬友聊了一下关于色彩的事情，小姐姐给了我拾色器分析出来的结果，感觉有点靠谱。因为我认为要拿到的肯定是一个字符串（包括也许有空格）。

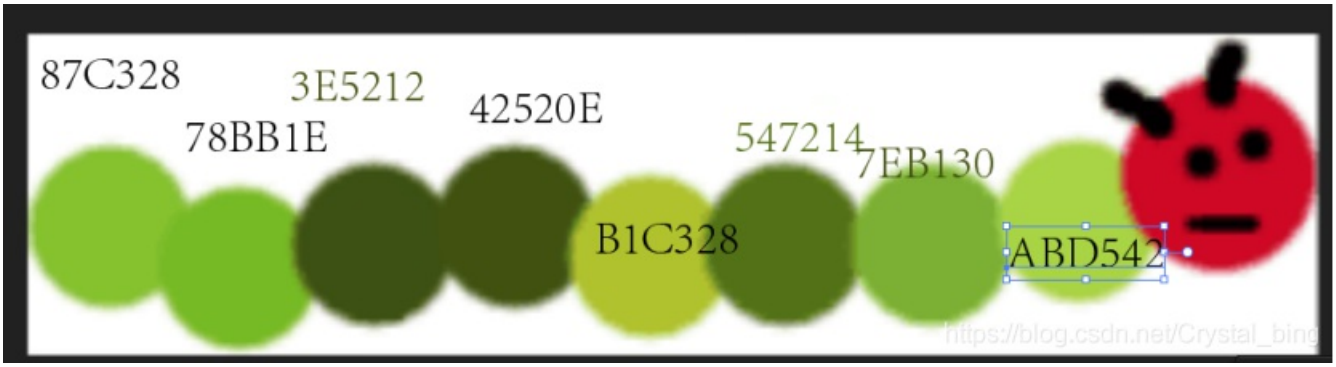
但是她给我的RGB数值结果有个很大的问题是有数值超过了0-127的范围，这意味着不能一一对应转换成单个字符。看了其他几种常见编码后还是觉得ASCII是转换的桥梁，就回过来看关于颜色的表示。在AI中其实还有一种HSB颜色表示，但是一开始我和小姐姐都觉得不太可能（HSB表示不是整数数值）。

但是还是要尝试一下，于是转换了前三个字符，发现是SOL，很符合solution的开头对不对！按照网上找的一个颜色转换器，我得到了下面这个结果：

SOLUSION JS COLOR-TIEMET

这很明显是不对的…从SOLUTION看出来，在记录过程中我对数值进位取舍没有保持一个标准（也是想看一下到底该怎么取）。于是这个答案修正一下就得到了正确结果！

但我还是觉得网上那个颜色转换器有点问题…有时间应该装一个PS…



贴一下小姐姐给我转的RGB！后面也间接用上了，因为我在网上找的是一个可以同时表示RGB和HSB的工具…没有原始的RGB误差肯定更加大…