




WeChall CTF Writeup (六)

原创

lmn_  于 2022-02-27 17:00:00 发布  42  收藏

分类专栏: [CTF](#) 文章标签: [CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_43211186/article/details/123156421

版权



[CTF 专栏收录该内容](#)

15 篇文章 0 订阅

订阅专栏

文章目录

[0x04 2 Limited Access Too by wannabe7331 and lordOric](#)

[0x05 2 Shadowlamb -](#)

[0x06 2 Training: Warchall - The Beginning by WarChallStaff](#)

以下题目标题组成:

[Score] [Title] [Author]

0x04 2 Limited Access Too by wannabe7331 and lordOric

 | score: 2 | **3.00** **4.84** **4.57** | Solved By [1702 People](#) | 79057 views | since Feb 02, 2011 - 20:33:07

Limited Access Too (Exploit, HTTP)

Limited Access Too

Haha, thank you so much for your feedback from the [first challenge](#).
Especially thanks to a special person who sent in a fixed [.htaccess](#) to secure [my pages](#).
The protected/protected.php is now secured :)

To prove me wrong, please access protected/protected.php again.

© 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021 and 2022 by [wannabe7331](#) and [lordOric](#)

CSDN @lmn_

题目意思:

哈哈, 非常感谢您对第一个挑战的反馈。

特别感谢一个特殊的人, 他发送了一个固定的.htaccess来保护我的页面。

protected/protected.php 现在是安全的 ☐

为了证明我错了，请再次访问 protected/protected.php。

GeSHi`ed Plaintext code for .htaccess

```
1 AuthUserFile .htpasswd
2 AuthGroupFile /dev/null
3 AuthName "Authorization Required for the Limited Access Too Challenge"
4 AuthType Basic
5 <Limit GET POST HEAD PUT DELETE CONNECT OPTIONS PATCH>
6 require valid-user
7 </Limit>
8 # TRACE is not allowed in Limit if TraceEnable is off, so disallow it completely
9 # to support both TraceEnable being on and off
10 RewriteEngine On
11 RewriteCond %{REQUEST_METHOD} ^TRACE
12 RewriteRule ^ - [F]
13
```

CSDN@imn

```
<Limit GET POST HEAD PUT DELETE CONNECT OPTIONS PATCH>
require valid-user
</Limit>
```

限制了GET POST HEAD PUT DELETE CONNECT OPTIONS PATCH方法

http的方法有：GET, HEAD, POST, PUT, DELETE, CONNECT, OPTIONS, PATCH, PROPFIND, PROPPATCH, LOCK, UNLOCK, TRACE

```
urllib.request.Request(url, data = None, headers = {}, origin_req_host = None, unverifiable = False, method = None)
```


参考大佬的代码：

```
import urllib.request
url='http://www.wechall.net/challenge/wannabe7331/limited_access_too/protected/protected.php'
header={}

req = urllib.request.Request(url, headers = header, method='PROPFIND')
req.add_header('Cookie', 'WC=Value')
text = urllib.request.urlopen(req).read().decode('utf-8')
print(text)
```

运行后直呼666

```
n [3]: import urllib.request
url='http://www.wechall.net/challenge/wannabe7331/limited_access_too/protected/protected.php'
header={}

req = urllib.request.Request(url, headers = header, method='PROPFIND')
req.add_header('Cookie','WC=16312573-jvvFuGR8dPcdZy4')
text = urllib.request.urlopen(req).read().decode('utf-8')
print(text)
```

```
</div>
</div>
</div>
```

```
<div id="page">

<div class="gwf_messages">
  <span class="gwf_msg_t">WeChall</span>
  <ul>
    <li>Your answer is correct. Congratulations you have solved this challenge.<br/>Please <a href="/chal
lvotes/86/Limited+Access+Too">vote this challenge</a>.<br/>You may also access <a href="/forum-bl83/Solution_Limited_
Access_Too.html">the solution board</a> for this challenge now.</li>

  </ul>
</div>
<div class="c1"></div>
<div class="gwf_messages">
  <span class="gwf_msg_t">WeChall</span>
```

CSDN @lmm_

0x05 2 Shadowlamb -

l by Gizmore

? | score: 2 | **2.81** **2.56** **7.18** | Solved By 354 People | 72936 views | since Aug 01, 2011 - 01:05:17

Shadowlamb - Chapter I (Fun)

Shadowlamb - Chapter I

Ugah made game. You play game. You #use ScrollOfWisdom. You play in IRC. The game in english

If you cannot base64, you can connect to rpg network darkmyst: ircs://nebula.uk.eu.darkmyst.org:6697#shadowlamb

Your solution for Shadowlamb - Chapter I

Answer

Submit

© 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021 and 2022 by [Gizmore](#)

CSDN @lmm_

题目意思:

Ugah 制作的游戏。你玩游戏。你#use ScrollOfWisdom。你在 IRC 玩。英文游戏。

如果不能base64, 可以连接rpg网络darkmyst: ircs://nebula.uk.eu.darkmyst.org:6697#shadowlamb

Shadowlamb - Chapter I (Fun)

How to play

VG8gcGxheSB5b3Ugd2lscBUZwVklGFuIElSQtyBjbGllbnQgYW5kIGNvbm5lY3QgdG8gaXJlLnd1Y2hhbGwubmV0IG9uIHBvcnQgNjY2OCBvcjBwb3J0IDY2OTcgZm9yIFNTTC

© 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021 and 2022 by [Gizmore](#)

CSDN @lmm_

VG8gcGxheSB5b3Ugd2lscBUZwVklGFuIElSQtyBjbGllbnQgYW5kIGNvbm5lY3QgdG8gaXJlLnd1Y2hhbGwubmV0IG9uIHBvcnQgNjY2OCBvcjBwb3J0IDY2OTcgZm9yIFNTTC4KVGHlIGNoYW5uZWwgaXMgI3NoYWRvd2xhbWl=

base64解密

解密网站: <https://www.qqxiuzi.cn/bianma/base64.htm>

Base64编码转换

```
VG8gcGxheSB5b3Ugd21sbCBuZWVkaGFuIE1Sb3QyYjBjbG11bnQgYW5kIGNvbm51Y3QgdG8gaXJjLnd1Y2hhbGwubmV0IG9uIHBvcnQ  
gNjY2OCBvcjBwb3J0IDY2OTcgZm9yIFNTTC4KVGHlIGNoYW5uZWwgaXMgI3NoYWRvd2xhbWI=
```

清空 加密 解密 解密为UTF-8字节流

```
To play you will need an IRC client and connect to irc.wechall.net on port 6668 or port 6697 for  
SSL.  
The channel is #shadowlamb
```

CSDN @lmm

To play you will need an IRC client and connect to irc.wechall.net on port 6668 or port 6697 for SSL.

The channel is #shadowlamb

IRC

+ | ★ 收藏 | 6 | 1

因特网中继聊天

🔊 播报 ✎ 编辑 💬 讨论 + 上传视频

同义词 IRC (互联网中继聊天) 一般指因特网中继聊天

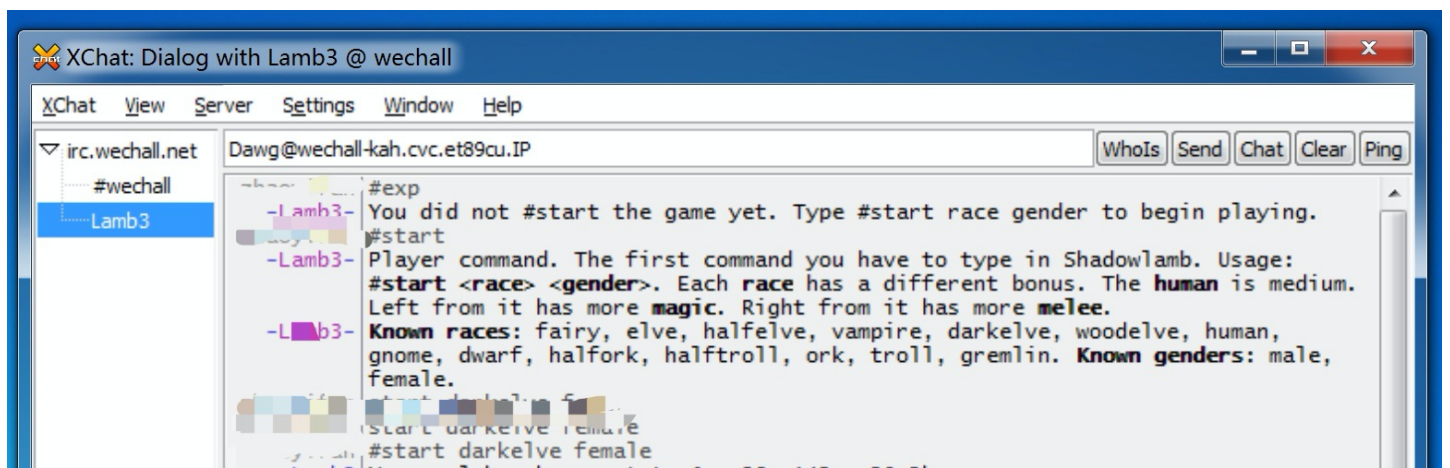
📖 本词条由“科普中国”科学百科词条编写与应用工作项目 审核。

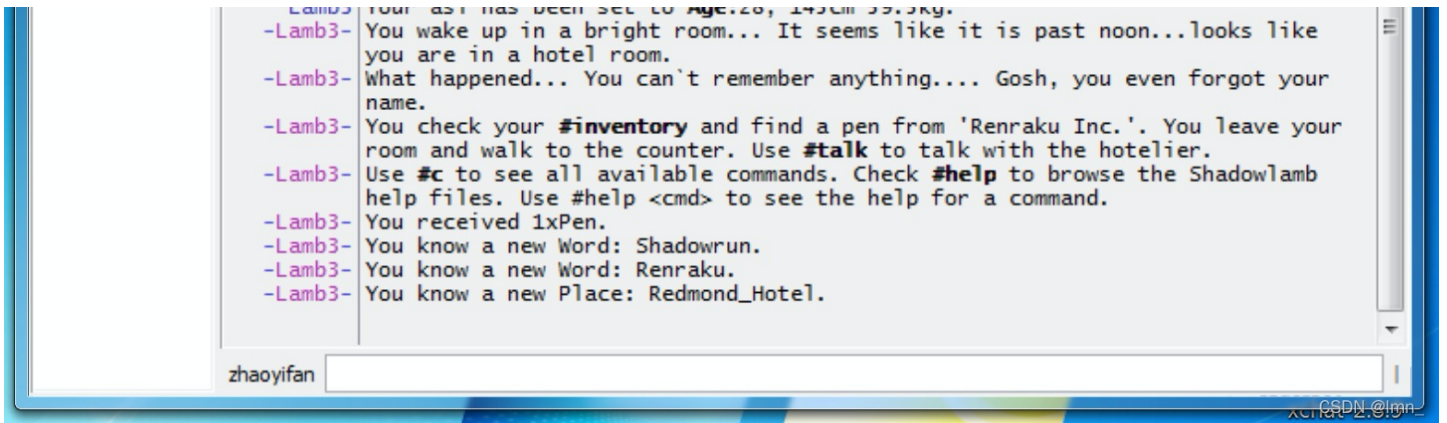
因特网中继聊天 (Internet Relay Chat)，一般称为 [互联网](#) 中继聊天，简称：IRC。它是由芬兰人 Jarkko Oikarinen 于 1988 年首创的一种网络聊天协议。经过十年的发展，世界上有超过 60 个国家提供了 IRC 的服务。IRC 的工作原理非常简单，您只要在自己的 PC 上运行客户端软件，然后通过因特网以 IRC 协议连接到一台 IRC 服务器上即可。它的特点是速度非常之快，聊天时几乎没有延迟的现象，并且只占用很小的带宽资源。所有用户可以在一个被称为“Channel” (频道) 的地方就某一话题进行交谈或密谈。每个 IRC 的使用者都有一个 Nickname (昵称)。

CSDN @lmm

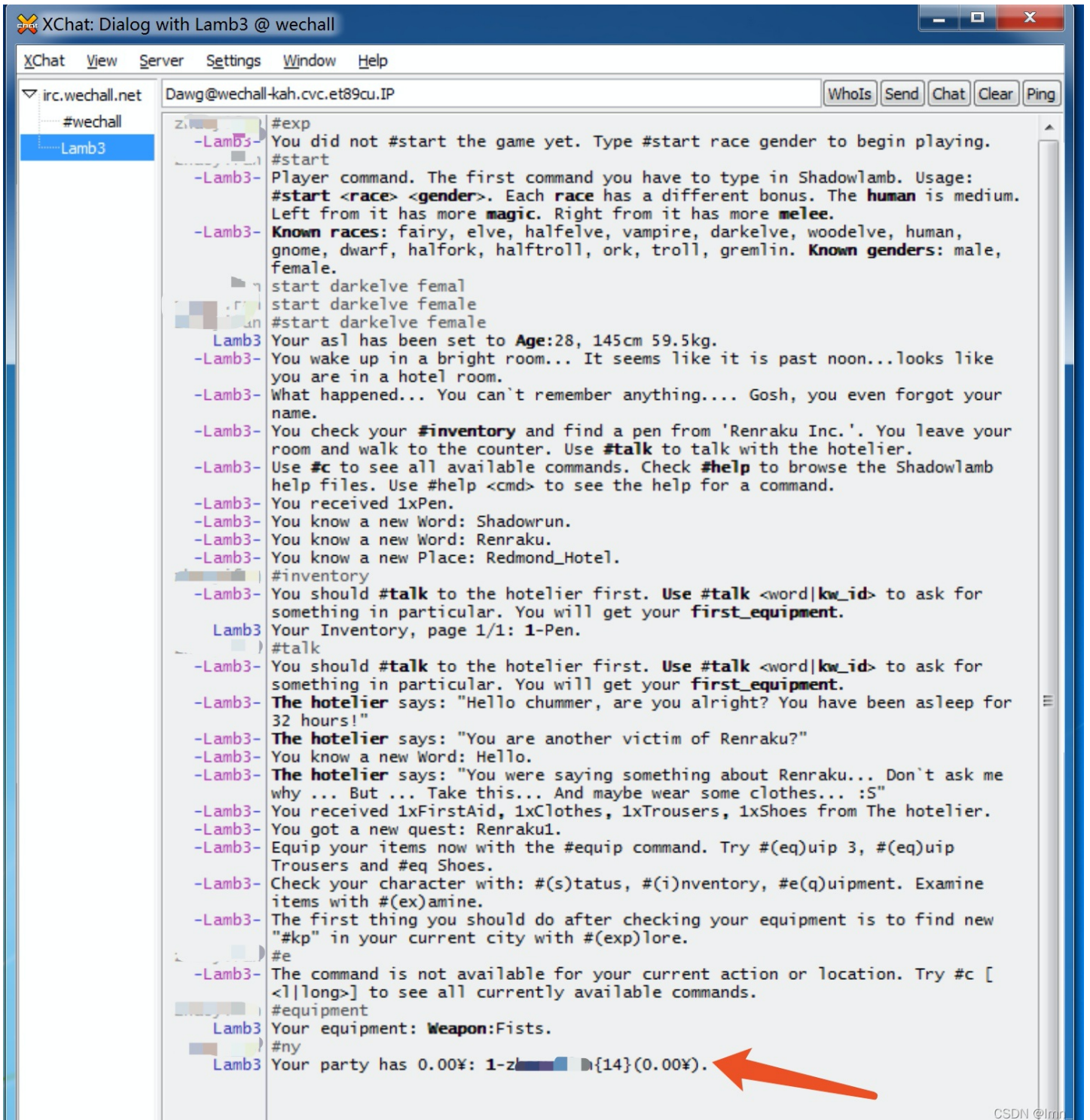
下载xchat地址

<http://xchat.org/windows/>

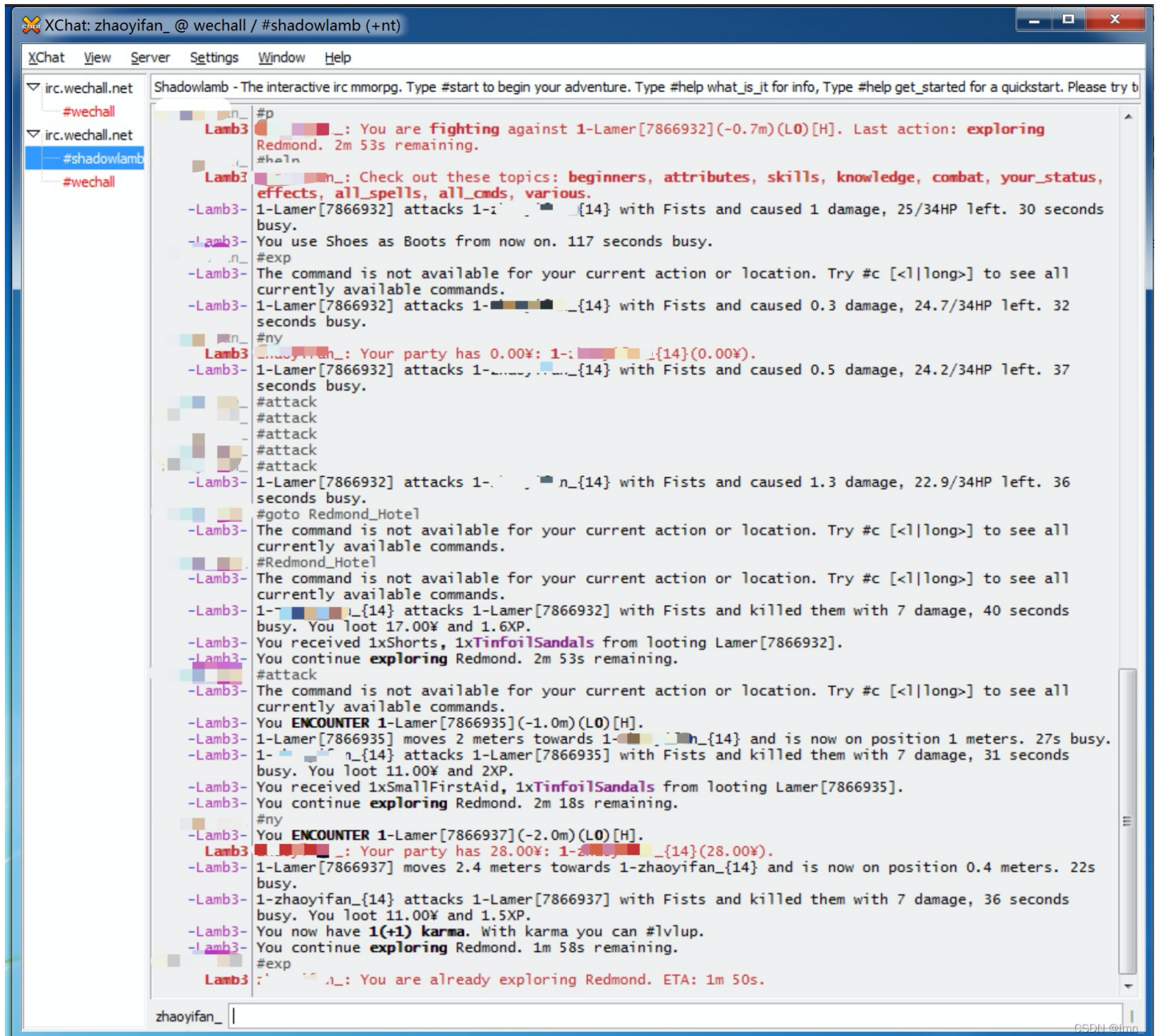




就。一直玩下去



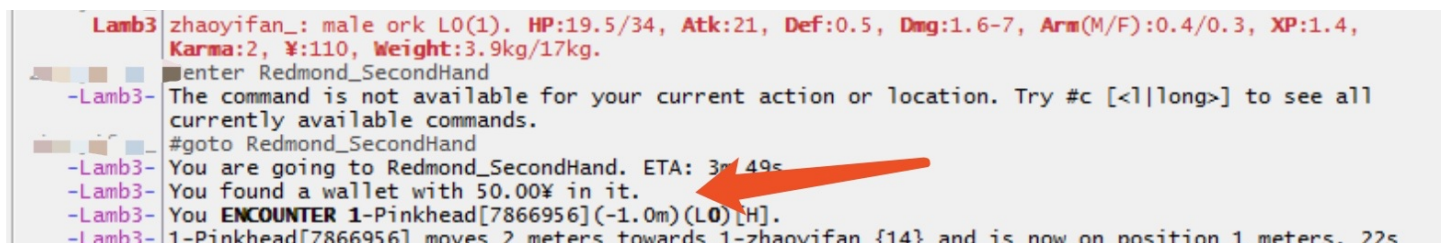
其实也没玩明白 #attack我编的估计没有用



还有1/3的血，只有110块钱



随地sha人又能随地捡钱的命！



```

-Lamb3- busy.
-Lamb3- 1-Pinkhead[7866956] attacks 1-Pinkhead[7866956] with Fists and killed them with 7 damage, 38 seconds
-Lamb3- busy. You loot 17.00¥ and 1.9XP.
-Lamb3- You continue going to Redmond_SecondHand. 2m 14s remaining.

```

CSDN @lrmn_

天生没有游戏命

```

#talk
-Lamb3- Donor says: "Hello Dear Sire, my name is Donor. Are you looking for something special?"
#say Yes.
-Lamb3- fan_{14} says: "Yes."
#say Yes
-Lamb3- fan_{14} says: "Yes"
#say ?
-Lamb3- fan_{14} says: "?"
#say Why are you ignoring me?????
-Lamb3- fan_{14} says: "Why are you ignoring me?????"

```

CSDN @lrmn_

两个小时过去了，终于抢了800

```

-Lamb3- The command is not available for your current action or location. Try #c [<1|long>] to see all
-Lamb3- currently available commands.
-Lamb3- 1-Pinkhead[7867115] moves 2 meters towards 1-Redmond_Alchemist[14] and is now on position 1 meters. 21s
-Lamb3- busy.
-Lamb3- 1-Redmond_Alchemist[14] attacks 1-Pinkhead[7867115] with BrassKnuckles and killed them with 9.5 damage,
-Lamb3- 31 seconds busy. You loot 17.00¥ and 1XP.
-Lamb3- You now have 13(+1) karma. With karma you can #lvlup.
-Lamb3- The party advanced to level 1.
-Lamb3- You continue going to Redmond_Alchemist. 3s remaining.
-Lamb3- You enter the alchemistic store. A tall elfe greets you as you walk towards the counter.
-Lamb3- In stores you can use #view, #buy and #sell. Use #talk to talk to the elfe.
#goto Redmond_Alchemist
Lamb3- You are already in Redmond_Alchemist.
#ny
Lamb3- Your party has 814.57¥: 1-Redmond_Alchemist[14](814.57¥).

```

CSDN @lrmn_

得到flag! 这个题没点耐心就跳过去吧

```

Lamb3- You are already in Redmond_Alchemist.
#goto Redmond_Alchemist
Lamb3- You are already in Redmond_Alchemist.
#view
zhaoyifan_: Items, page 1/1: 1-EmptyBottle(49.95¥), 2-NinjaPotion(250.00¥), 3-StrengthPotion
(150.00¥), 4-QuicknessPotion(200.00¥), 5-AimWater(300.00¥), 6-Stimpatch(1300.00¥),
7-ScrollOfWisdom(800.00¥), 8-Mandrake(3000.00¥).
#buy 7
-Lamb3- You received 1xScrollOfWisdom.
Lamb3- You paid 800.00¥ and bought 1 x ScrollOfWisdom. You now carry 6.11kg / 17kg. Inventory
ID: 10.
#i
Lamb3- Your Inventory, page 1/1: 1-Pen, 2-Shorts, 3-Booze(2), 4-Clothes, 5-Shoes,
6-BaseballBat, 7-SmallFirstAid, 8-Knife, 9-Coke, 10-ScrollOfWisdom.
#use 10
-Lamb3- The scroll reads: `Congrats! Enter 'zhaoyifan_{14}!9e2c91435c29e9' without the quotes`.
-Lamb3- The scroll puffs into magic challenging dust.

```

CSDN @lrmn_

2	Training: Math Pyramid by Gizmore	1776	11y 50d	134	4.09	4.10	5.31	?
2	Training: Baconian by Gizmore	1603	11y 43d	125	3.18	4.45	4.64	?
2	Training: LSB by Gizmore	1955	11y 31d	142	3.46	5.49	5.34	?
2	Training: GPG by Gizmore	1002	11y 18d	95	2.89	6.13	4.65	?
2	Limited Access by wannabe7331	2379	10y 361d	140	2.68	4.61	4.29	?
2	Limited Access Too by wannabe7331 and lordOrie	1703	10y 358d	89	3.00	4.84	4.57	?
2	Shadowlamb - Chapter I by Gizmore	355	10y 179d	62	2.81	2.56	7.18	?

CSDN @lrmn_

0x06 2 Training: Warchall - The Beginning by WarChallStaff

? | score: 2 | **2.50** **4.69** **7.40** | Solved By 1845 People | 114278 views | since Dec 24, 2011 - 21:15:32

Training: Warchall - The Beginning (Realistic, Linux, Shell, Warchall)

Warchall - Chapter I (Warchall begins)

You are now becoming a linux superhacker.

Create an SSH account with the form below.

Then enter the 6 solutions to level 0-5 separated by comma.

Example: bitwarrior,Solution1,Solution2,Solution3,Solution4,Solution5

Proudly presented by the The Warchall(tm) Staff

Thanks and shouts to xd-- for idea, motivation and inspiration!

Enable logfile EMails

Toggle

(RE)SET your SSH account

Password

Retype

Go!

Your solution for Training: Warchall - The Beginning

Answer

Submit

© 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021 and 2022 by [WarChallStaff](#)

The warchall project is hosted on [vr.org](#), a cloud based hosting service.

The service and support is unique, and they just have added additional 20GB HDD space for us for free! Thank you very much vr.org!

CSDnT@Imm_

题目意思：

你现在正在成为一个 Linux 超级黑客。

使用下面的表格创建一个 SSH 帐户。

然后输入 0-5 级的 6 种解决方案，以逗号分隔。

示例：bitwarrior,Solution1,Solution2,Solution3,Solution4,Solution5

设置好密码

Let the Warchall begin

Ok Challenger, in about 1 minute you should be able to login via `ssh -p 19198 lmn@warchall.net`
Use the password you entered in the form.

Happy Challenging!
The warchall team

CSDN @lmn_

根据 Exp 推测最终的flag为5个flag拼起来的

```
lmn@warchall:~  
lmn@warchall ~ $ ls  
level WELCOME.txt  
lmn@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 hope  
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 ==  
=====
```

```
nooter,bsdhell,livinskull,kwisatz,gizmore,jjk,paipai,dloser,nurfed  
(warchall.net)  
  
NEW: checkout /home/features :)  
  
lmn@warchall ~ $
```

CSDN @lmn_

level 4

cat README.txt 发现无权限，授予权限即可

```
lmn@warchall ~ $ cd level  
lmn@warchall ~/level $ ls  
4 5 6  
lmn@warchall ~/level $ cd 4  
lmn@warchall ~/level/4 $ ls  
README.txt  
lmn@warchall ~/level/4 $ cat README.txt  
cat: README.txt: Permission denied  
lmn@warchall ~/level/4 $ ls -l  
total 4  
----- 1 lmn lmn 63 Jan 24 08:23 README.txt  
lmn@warchall ~/level/4 $ chmod 700 README.txt  
lmn@warchall ~/level/4 $ cat README.txt  
The solution to level 4 is 'AndIknowchown' without the quotes.  
lmn@warchall ~/level/4 $
```

CSDN @lmn_

The solution to level 4 is 'AndIknowchown' without the quotes.

level 5

提示：Protect your /home/user/lmn/level directory from other users. Then wait 5 minutes.

解决办法：删除其他用户权限

```
lmn@warchall ~/level/4 $ cd ../
lmn@warchall ~/level $ cd 5
lmn@warchall ~/level/5 $ ls
README.txt
lmn@warchall ~/level/5 $ cat README.txt
Protect your /home/user/lmn/level directory from other users. Then wait 5 minutes.
lmn@warchall ~/level/5 $ cd ../
lmn@warchall ~/level $ cd ../
lmn@warchall ~ $ ls -l
total 8
drwx---r-x 5 lmn lmn 4096 Jan 24 08:23 level
-r--r--r-- 1 lmn lmn 463 Jan 18 2014 WELCOME.txt
```

CSDN @lmn_

5文件夹中出现solution.txt，授予权限

```
lmn@warchall ~/level $ cd 5
lmn@warchall ~/level/5 $ ls
README.txt solution.txt
lmn@warchall ~/level/5 $ cat solution.txt
cat: solution.txt: Permission denied
lmn@warchall ~/level/5 $ ls -l
total 8
-----r-- 1 root root 83 Jan 24 08:23 README.txt
--w-rwxr-T 1 lmn lmn 66 Jan 24 08:46 solution.txt
lmn@warchall ~/level/5 $ chmod 700 solution.txt
```

CSDN @lmn_

The solution to level 5 is 'OhRightThePerms', without the quotes.

level 0

```
lmn@warchall ~ $ cd /home/level
lmn@warchall /home/level $ ls
0 10 12 15_live_rfi 2 21_nurxxed 8 level9 mgine tropic w1 ynor7
1 11 14_live_fi 16 20_live_rce 3 kwisatz matrixman space w0 w2
lmn@warchall /home/level $ cd 0
lmn@warchall /home/level/0 $ ls
README.txt
lmn@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.
```

CSDN @lmn_

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

level 1

```
lmm@warchall /home/level/1 $ ls -A
.bash_history .bash_logout .bash_profile .bashrc blue README.txt red .ssh
lmm@warchall /home/level/1 $ cat README.txt
Follow the black cursor.
```

where??

我是在当前目录做完level 45才开始0123的，发现每个flag都伴随着关键字“solution”那直接搜索一下方便快捷

```
12/pytong2.py:57:          #      solution.close()
grep: 12/compile.sh: Permission denied
grep: 12/pytong2: binary file matches
12/pytong.py:6:SOLUTION = "/home/level/12/solution.txt"
12/pytong.py:11:          # We want to prevent some noobish solutions
12/pytong.py:27:          # The file does not exists anymore, you have found a solution
grep: 12/solution.txt: Permission denied
grep: 12/wrap.c: Permission denied
grep: w0: Permission denied
grep: 14_live_fi: Permission denied
grep: 8/.bash_profile: Permission denied
grep: 8/.ssh: Permission denied
grep: 8/.bashrc: Permission denied
grep: 8/.bash_history: Permission denied
grep: 8/.bash_logout: Permission denied
grep: 8/solution.txt: Permission denied
2/.porb/.solution:1:The solution is HiddenIsConfig
grep: 2/.ssh: Permission denied
2/.bash_history:8:nano .porb/.solution
grep: 20_live_rce: Permission denied
grep: 1/blue/pill/hats/black: Permission denied
1/blue/pill/hats/gray/solution/is/SOLUTION.txt:3:Your solution for this level is: LameStartup
grep: 1/.ssh: Permission denied
1/.bash_history:33:mkdir solution
1/.bash_history:34:cd solution/
grep: tropic/7/Y00      H0\0: Permission denied
grep: tropic/7/;lЯ* : Permission denied
grep: tropic/7/+050:r0 : Permission denied
grep: tropic/7/00: Permission denied
grep: tropic/7/00D0@00: Permission denied
grep: tropic/7/0F0}0: Permission denied
grep: tropic/7/P0A00: Permission denied
grep: tropic/7/0600j=': Permission denied
grep: tropic/7/A00Pj0: Permission denied
grep: tropic/7/000000f: Permission denied
grep: tropic/7/s00+b\0: Permission denied
grep: tropic/7/Z^0Kw0: Permission denied
grep: 15_live_rfi: Permission denied
grep: 0/.ssh: Permission denied
0/README.txt:15:Oh ... and your solution to level0 is: "bitwarrior" without the quotes.
grep: ynorl7/6/real_solution.txt: Permission denied
grep: ynorl7/6/solution.txt: Permission denied
grep: 10/compile.sh: Permission denied
grep: 10/solution.txt: Permission denied
grep: 11/solution.txt: Permission denied
grep: 3/.ssh: Permission denied
```



```
3/.bash_history:1:The solution to SSH3 is: RepeatingHistory
grep: mgine: Permission denied
w2/WELCOME.txt:5:You will find the solution to each level in
grep: w2/.ssh: Permission denied
```

CSDN @Imn_

bitwarrior,LameStartup,HiddenIsConfig,RepeatingHistory,AndIknowchown,OhRightThePerms