WeChall-writeup-6-11.24(Limited Access Too;Shadowlamb - Chapter I)

原创

MeliodasC 于 2018-11-29 16:58:56 发布 1197 收藏

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

突然发现之前的没发，今天来补一下~
这一次积分结算前做了两道比较麻烦的题~会写的比较详细！

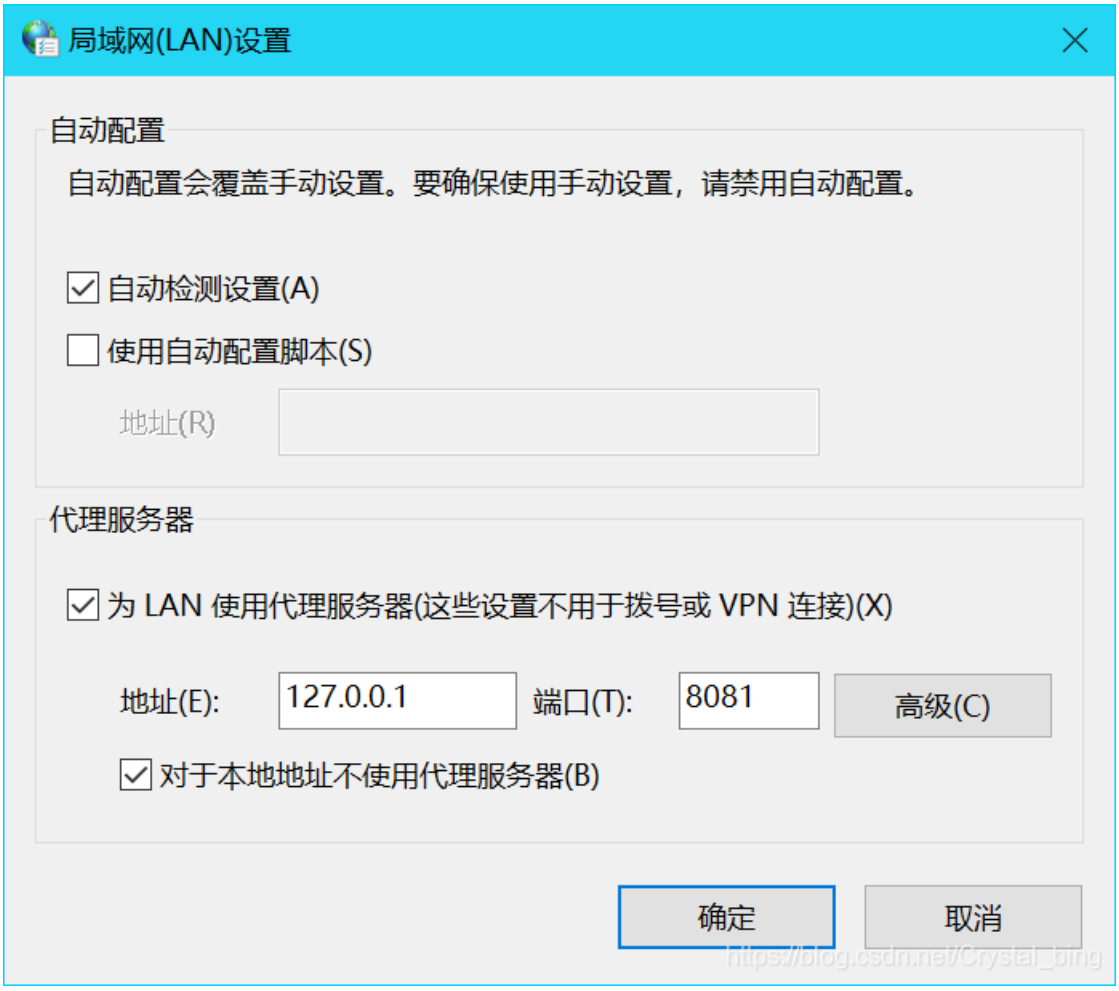
Limited Access Too

这次用burpsuite来解~

> 具体的安装和使用可以参考一下两个链接：
> 1.安装java+burpsuite（Java环境的配置不再赘述，可以看一下我上一篇写的要点，注意了一般就不会出错啦。）
> 2.代理模块讲解
>
> 写一下burpsuite解题的具体步骤：

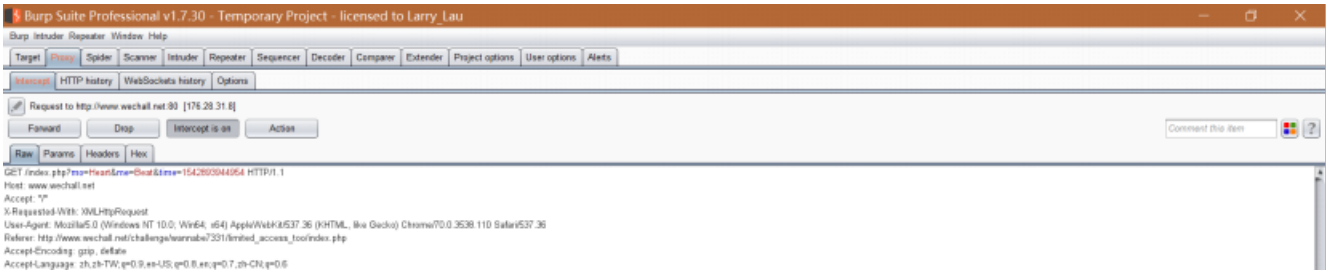
1. Proxy->Options查看监听的地址和端口，默认值是127.0.0.1：8080。Runnning无法勾选的情况我没有正面去解决。我Add了一个新的地址和端口127.0.0.1：8081。

2.以chrome为例，其他浏览器相似设置->高级->打开代理设置->局域网设置设置内容如下（地址端口写与（1）中一致）



我有点疑惑的两种代理间的关系

3.Proxy->Intercept->检查是否为Intercept is on回到题目，点击my pages（这里我截掉了我的cookie，下面应该还有两行。）



4.选中包中所有内容->右键选择Send to Repeater

5.Repeater->Request栏中GET方法改为POST方法->点击GO

Shadowlamb - Chapter I

超链接解出来是下面的信息：

To play you will need an IRC client and connect to irc.gizmore.org on port 6668 or port 6666 for SSL.The channel is #shadowlamb

首先了解一下什么是IRC

我选择了在windows下使用XChat。按照解码出来的信息配置完以后进入频道，发现是要玩一个游戏。

```
Dorisans  #help what_is_it
  Lamb3   Shadowlamb is a full featured mmorpg. You can #(j)oin parties, solve #(qu)ests, runecraft your items and learn magic spells. It combines multiple irc
          networks into a single gameworld, and thus is unique among all irc games.
```

可以用#exp去探索很多地点，路上打打怪抢钱。虽然是全英文但其实还是讲的很清楚的，每次都会告诉你新的指令。（除了有一些卖的东西我是真的不知道什么意思，查了也不明白）

```
-Lamb3-  You know a new Place: Redmond_Alchemist.
-Lamb3-  In a sidestreet you found an interesting store: "Carstens Alchemic Utils".
-Lamb3-  When you find locations, you are outside of them. Use #goto or #enter to enter them. You can #(exp)lore again to find more locations.
Dorisans #enter
-Lamb3-  You enter the alchemistic store. A tall elve greets you as you walk towards the counter.
-Lamb3-  In stores you can use #view, #buy and #sell. Use #talk to talk to the elve.
Dorisans #view
  Lamb3  Items, page 1/1: 1-EmptyBottle(48.70¥), 2-NinjaPotion(243.75¥), 3-StrengthPotion(146.25¥), 4-QuicknessPotion(195.00¥), 5-AimWater(292.50¥), 6-Stimpatch
         (1267.50¥), 7-ScrollOfWisdom(780.00¥), 8-Mandrake(2925.00¥).
```

总的目标就在这张图里写的地点：`Redmond_Alchemist`，攒钱买到`7-ScrollOfWisdom`就能拿到flag！附一些常用的指令（其实lamb3都会告诉你，玩的时候也很快就能记住）：

- `#ny` 查询自己有多少钱
- `#kp` 已知地点（探索过的地点）
- `#exp` 探索新地点（会给出进行探索预计要用的时间）
- `#s` 状态
- `#i` 查看包裹
- `#eq` 查看包裹
- `#use` 使用物品
- `#info` 回到最后一个动作

```
-Lamb3- You enter the alchemistic store. A tall elve greets you as you walk towards the counter.
-Lamb3- In stores you can use #view, #buy and #sell. Use #talk to talk to the elve.
Dorisans #view
  Lamb3 Items, page 1/1: 1-EmptyBottle(48.70¥), 2-NinjaPotion(243.75¥), 3-StrengthPotion(146.25¥), 4-QuicknessPotion(195.00¥), 5-AimWater(292.50¥), 6-Stimpatch
        (1267.50¥), 7-ScrollOfWisdom(780.00¥), 8-Mandrake(2925.00¥).
Dorisans #buy 7
-Lamb3- You received 1xScrollOfWisdom.
  Lamb3 You paid 780.00¥ and bought 1 x ScrollOfWisdom. You now carry 5.46kg / 4.34kg. Inventory ID: 8.
Dorisans #i
  Lamb3 Your Inventory, page 1/1: 1-Pen, 2-FirstAid, 3-LargeBeer(2), 4-BrassKnuckles_with_quickness:0.66, 5-TinfoilGloves, 6-Sandals_with_strength:0.66,
        7-Sneakers_with_wisdom:1.26, 8-ScrollOfWisdom.
Dorisans #use 8
-Lamb3- The scroll reads: `Congrats! Enter "dorisans[14]!78566017fed50865!wisdom" without the quotes`.
-Lamb3- The scroll puffs into magic challenging dust.
```


所以说光明正大地玩了几个小时【误】。