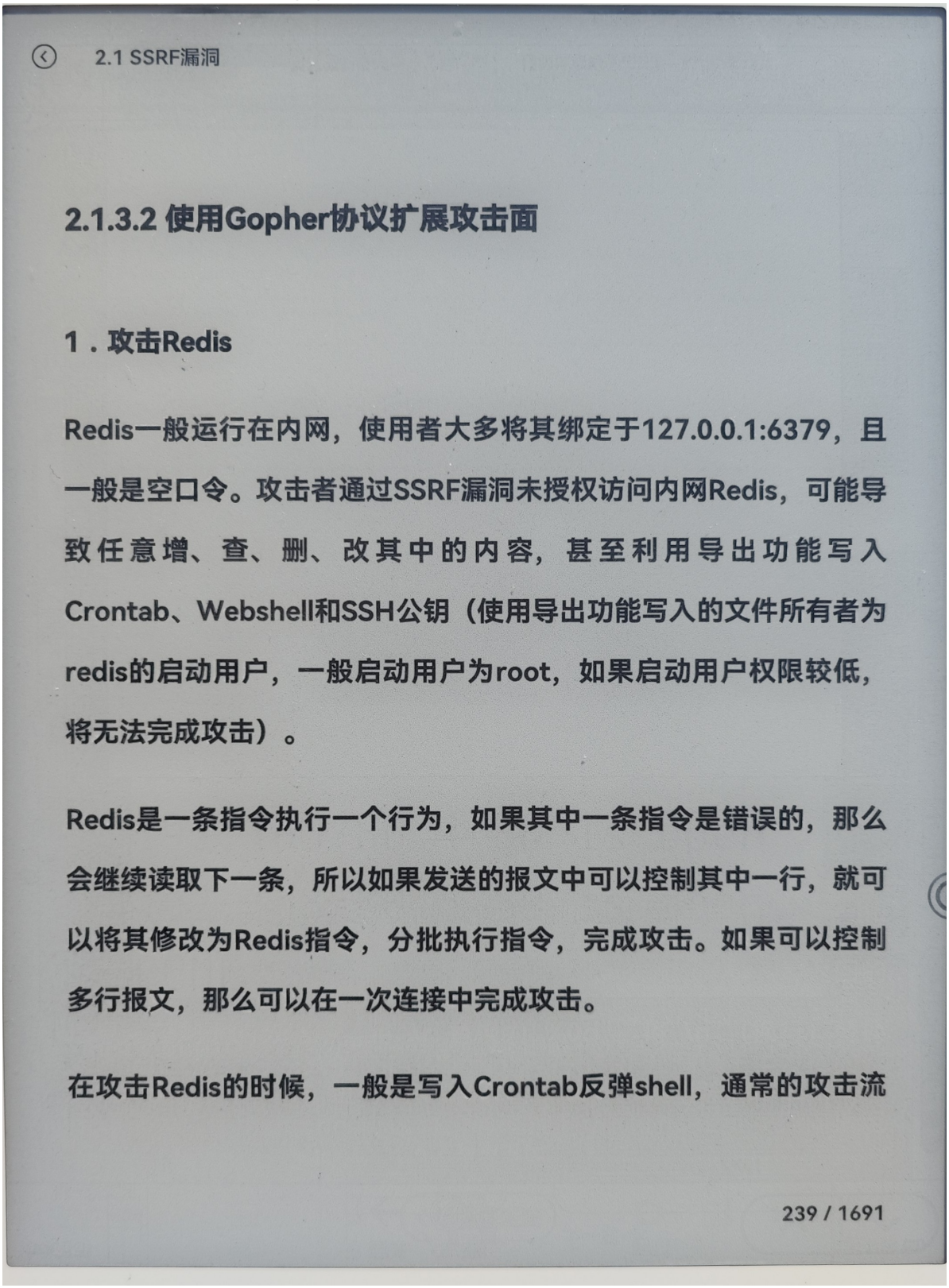
WP合集

Web

2.Gopher Shop

最先开始我看到有个docker想在本地搭建运行一下顺便改一下go文件空手套白狼的，然而发现并不可行。

然后在我去乡下走亲访友顺便晒太阳的路上我看见了这篇文章，看到有个gopher，开始以为大概这题考的是这个协议吧，结果好像这个gopher没什么别的含义确实是土拨鼠。



2.1.3.2 使用Gopher协议扩展攻击面

1．攻击Redis

Redis一般运行在内网，使用者大多将其绑定于127.0.0.1:6379，且一般是空口令。攻击者通过SSRF漏洞未授权访问内网Redis，可能导致任意增、查、删、改其中的内容，甚至利用导出功能写入Crontab、Webshell和SSH公钥（使用导出功能写入的文件所有者为redis的启动用户，一般启动用户为root，如果启动用户权限较低，将无法完成攻击）。

Redis是一条指令执行一个行为，如果其中一条指令是错误的，那么会继续读取下一条，所以如果发送的报文中可以控制其中一行，就可以将其修改为Redis指令，分批执行指令，完成攻击。如果可以控制多行报文，那么可以在一次连接中完成攻击。

在攻击Redis的时候，一般是写入Crontab反弹shell，通常的攻击流

然后看以前hgame的WP发现cosmos的二手市场和这个像极了

Cosmos的二手市场

涉及内容

条件竞争

打开页面，如下：

简单测试一下，表面上的逻辑很简单，购买/出售，会消耗/获得相应的金额，但是出售的价格是比购买的价格低的，所以通过正常的页面操作是无法“赚取一个亿”的。

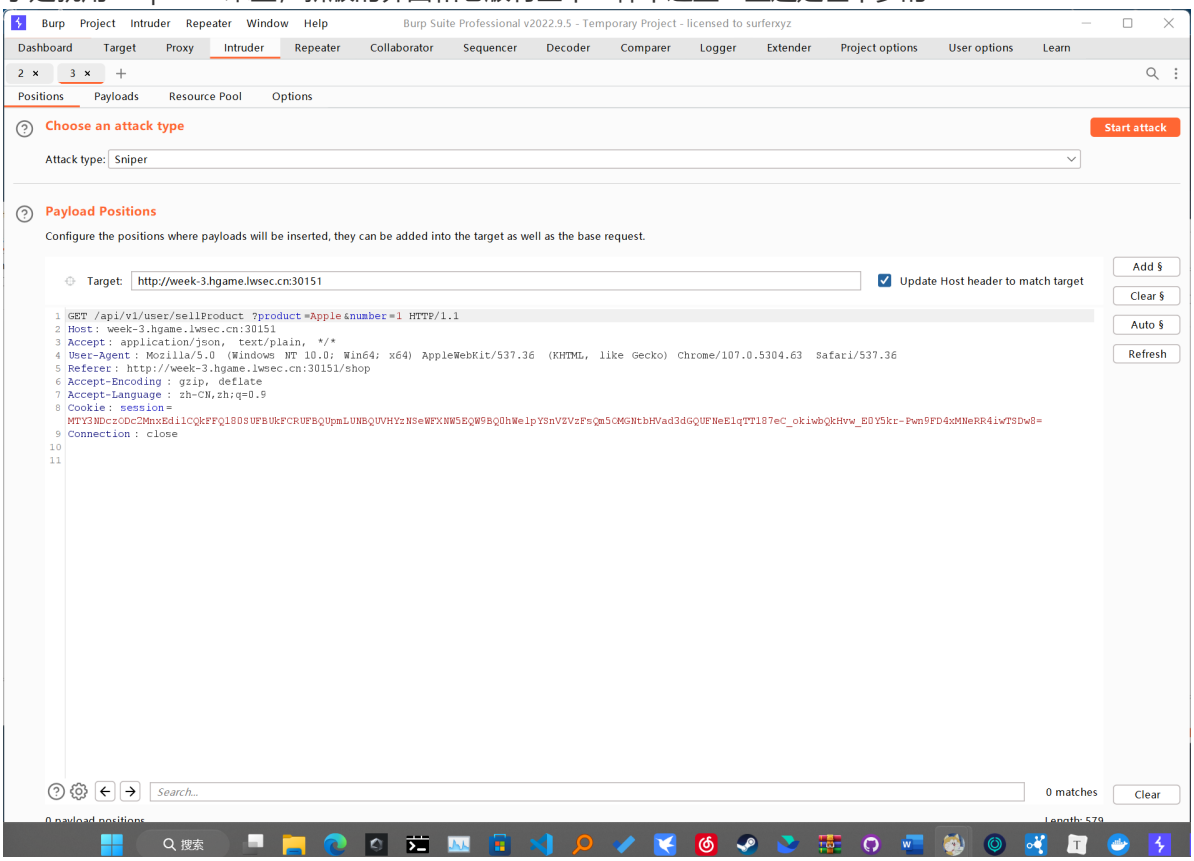
这道题其实我没做出来，最后有师傅提示说是条件竞争，才知道怎么做。

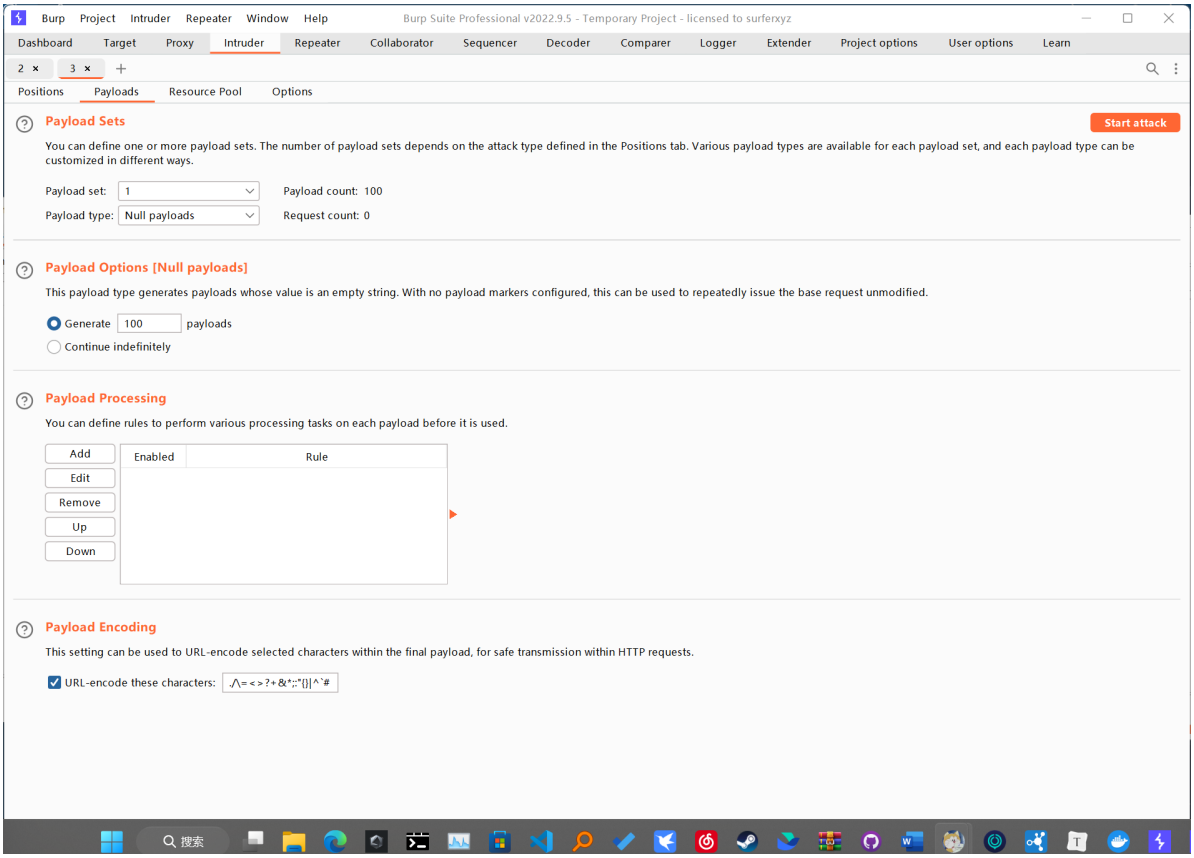
那这样就很简单了，懒得写脚本，`burpsuite`直接发数据包，高线程卖出，低线程买入，摸了几分钟鱼，余额已经刷到8个亿了：

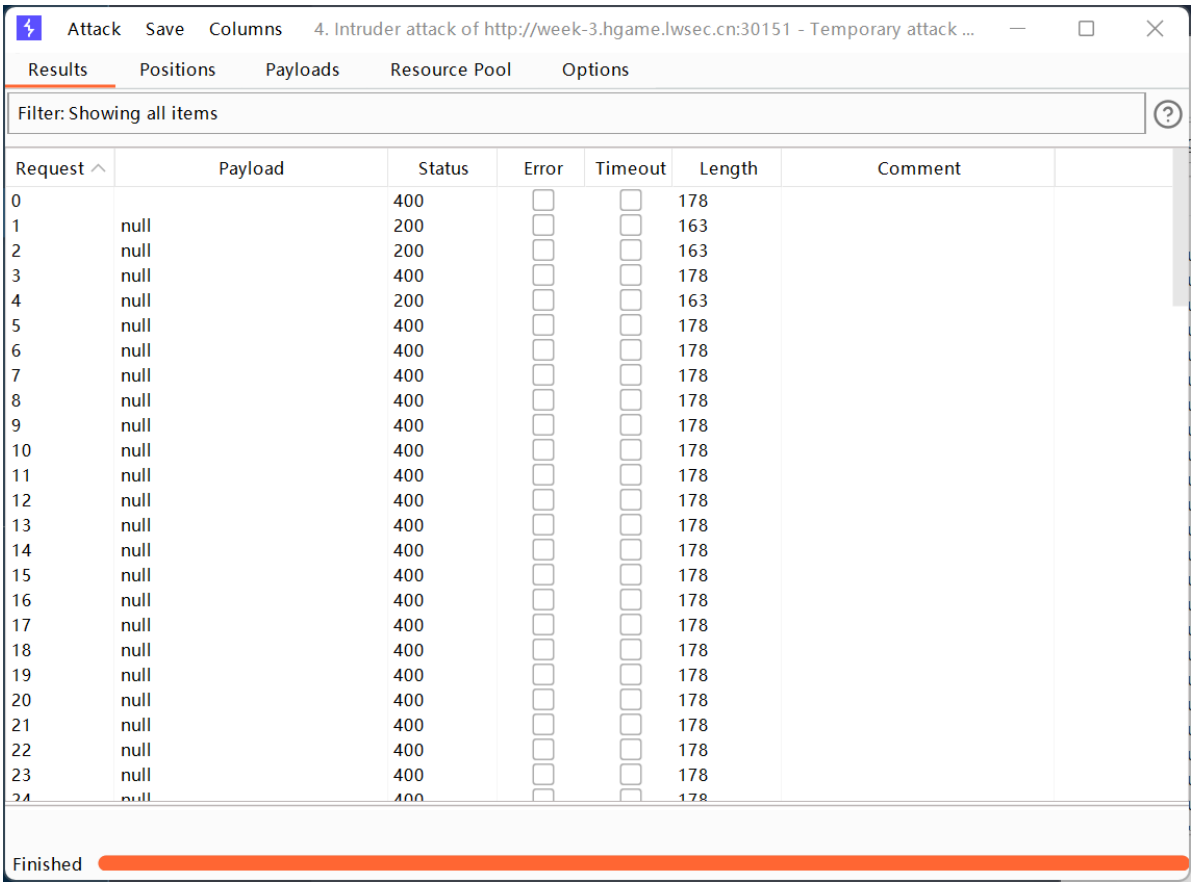
用户名	余额
adminadmin	804312900

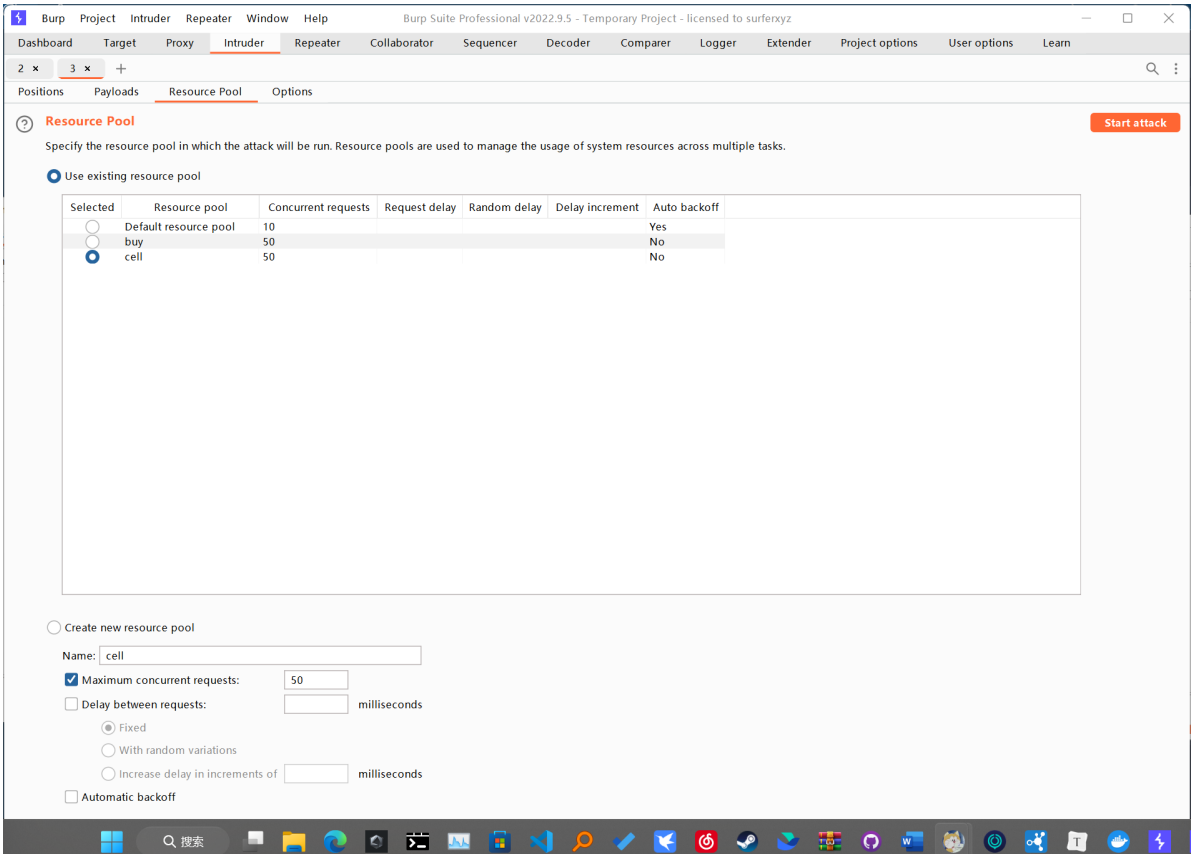
直接getflag即可。

于是就用burpsuite来整，新版的界面和老版有些不一样不过整一整还是差不多的




Burp Project Intruder Repeater Window Help
Burp Suite Professional v2022.9.5 - Temporary Project - licensed to surferxyz
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extender Project options User options Learn
2 × 3 ×
Positions Payloads Resource Pool Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 100
Payload type: Null payloads
Request count: 0
Payload Options [Null payloads]
This payload type generates payloads whose value is an empty string. With no payload markers configured, this can be used to repeatedly issue the base request unmodified.
Generate 100 payloads
Continue indefinitely
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Enabled
Rule
Payload Encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
URL-encode these characters: ./\=<>?+&*;:"{}|^`#
搜索


Attack Save Columns
4. Intruder attack of http://week-3.hgame.lwsec.cn:30151 - Temporary attack ...
Results Positions Payloads Resource Pool Options
Filter: Showing all items
Request Payload Status Error Timeout Length Comment
0 400 178
1 null 200 163
2 null 200 163
3 null 400 178
4 null 200 163
5 null 400 178
6 null 400 178
7 null 400 178
8 null 400 178
9 null 400 178
10 null 400 178
11 null 400 178
12 null 400 178
13 null 400 178
14 null 400 178
15 null 400 178
16 null 400 178
17 null 400 178
18 null 400 178
19 null 400 178
20 null 400 178
21 null 400 178
22 null 400 178
23 null 400 178
Finished



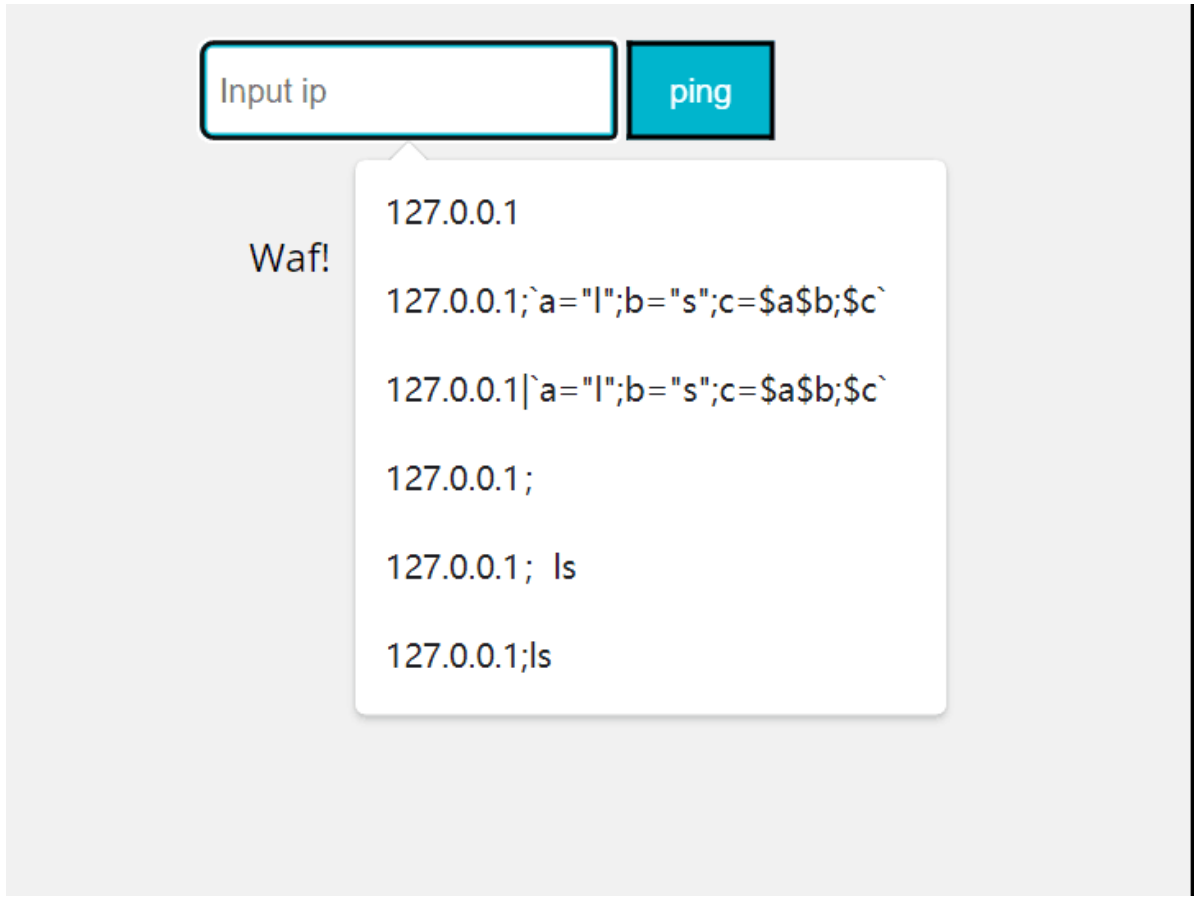
本题的思路就是条件竞争，不过由于有天数的限制所以不能像cosmos的二手市场那道题一样摆完挂机刷钱。

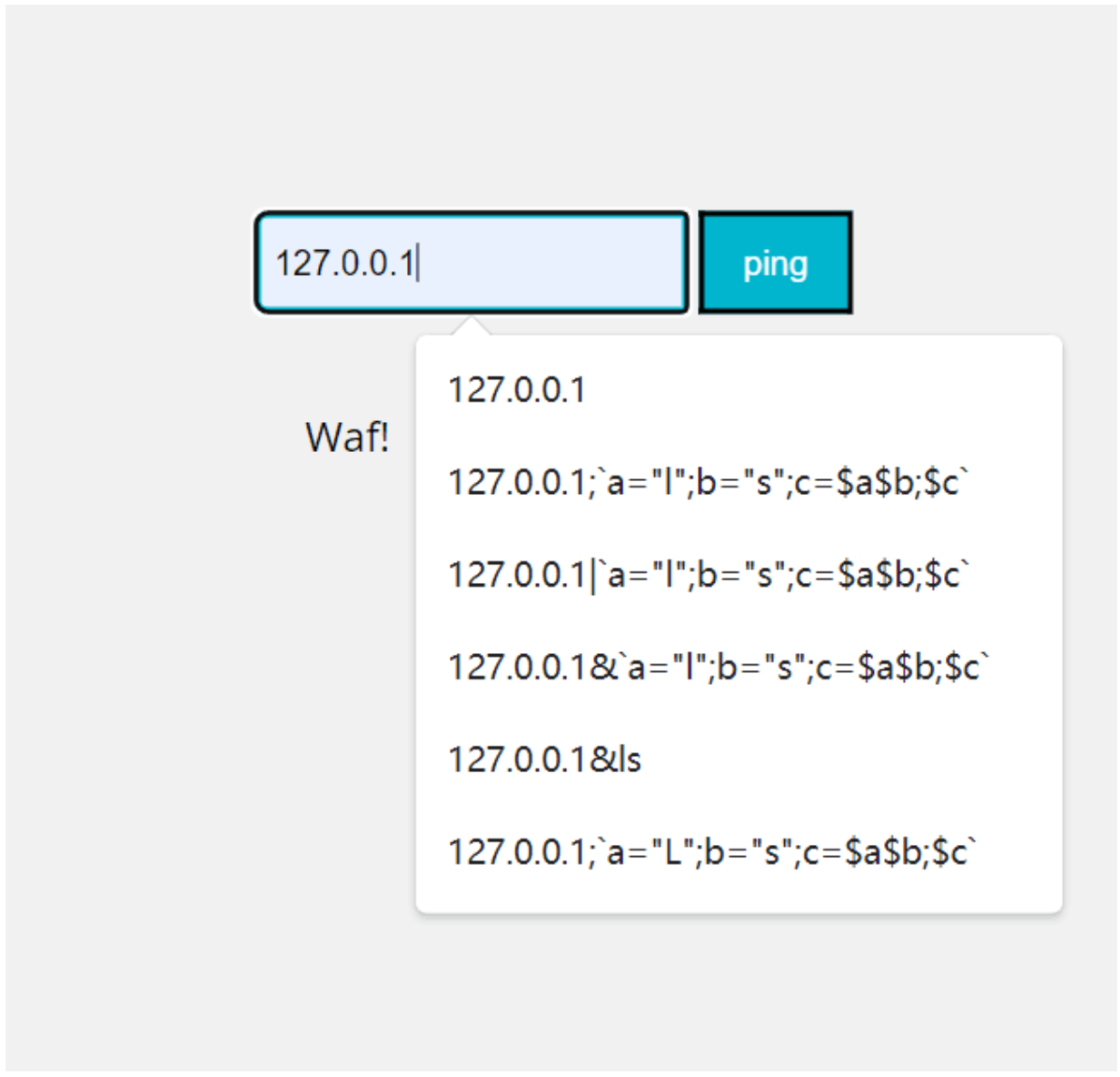
```
flag='hgame{GopherShop_M@gic_1nt_Overflow}'
```

结合flag的内容可以知道，原来是整数溢出了

3.Ping To The Host

尝试了好多回却连waf也绕不过去


Input ip
ping
Waf!
127.0.0.1
127.0.0.1;`a="l";b="s";c=$a$b;$c`
127.0.0.1|`a="l";b="s";c=$a$b;$c`
127.0.0.1;
127.0.0.1; ls
127.0.0.1;ls


127.0.0.1
ping
Waf!
127.0.0.1
127.0.0.1;`a="l";b="s";c=$a$b;$c`
127.0.0.1|`a="l";b="s";c=$a$b;$c`
127.0.0.1&`a="l";b="s";c=$a$b;$c`
127.0.0.1&ls
127.0.0.1;`a="L";b="s";c=$a$b;$c`

在余下的时间里，只能得出这样的结论

```
127.0.0.1 && `a="l";b="s";c=$a$b;$c`
127.0.0.1$IFS$9&&$IFS$9`a="l";b="s";c=$a$b;$c`
127.0.0.1<>&&<>`a="l";b="s";c=$a$b;$c`
127.0.0.1<&&<`a="l";b="s";c=$a$b;$c`

127.0.0.1$IFS&&$IFS`a="l";b="s";c=$a$b;$c`

127.0.0.1,&&,`a="l";b="s";c=$a$b;$c`
127.0.0.1&& `a="l";b="s";c=$a$b;$c`
127.0.0.1${IFS}&&${IFS}`a="l";b="s";c=$a$b;$c`
$IFS
${IFS}
$IFS$1    //$1改成$加其他数字貌似都行
$IFS$9       (Ubuntu下测试通过)后面加个$与{}类似，起截断作用,
<
<>
{cat,flag.php}  //用逗号实现了空格功能
%20
%09

ps:有时会禁用cat:
解决方法是使用tac反向输出命令:
linux命令中可以加\，所以甚至可以ca\t /fl\ag

curl读取文件:

curl file:///home/coffee/flag
```

经测试<,<>是碰都不能碰的，输上去就waf.$IFS，${IFS}似乎可行,但是当输入

```
127.0.0.1${IFS}&&${IFS}`a="l";b="s";c=$a$b;$c`
```

时候依然会有waf这是因为;也是碰都不能碰的，把分号改成&&

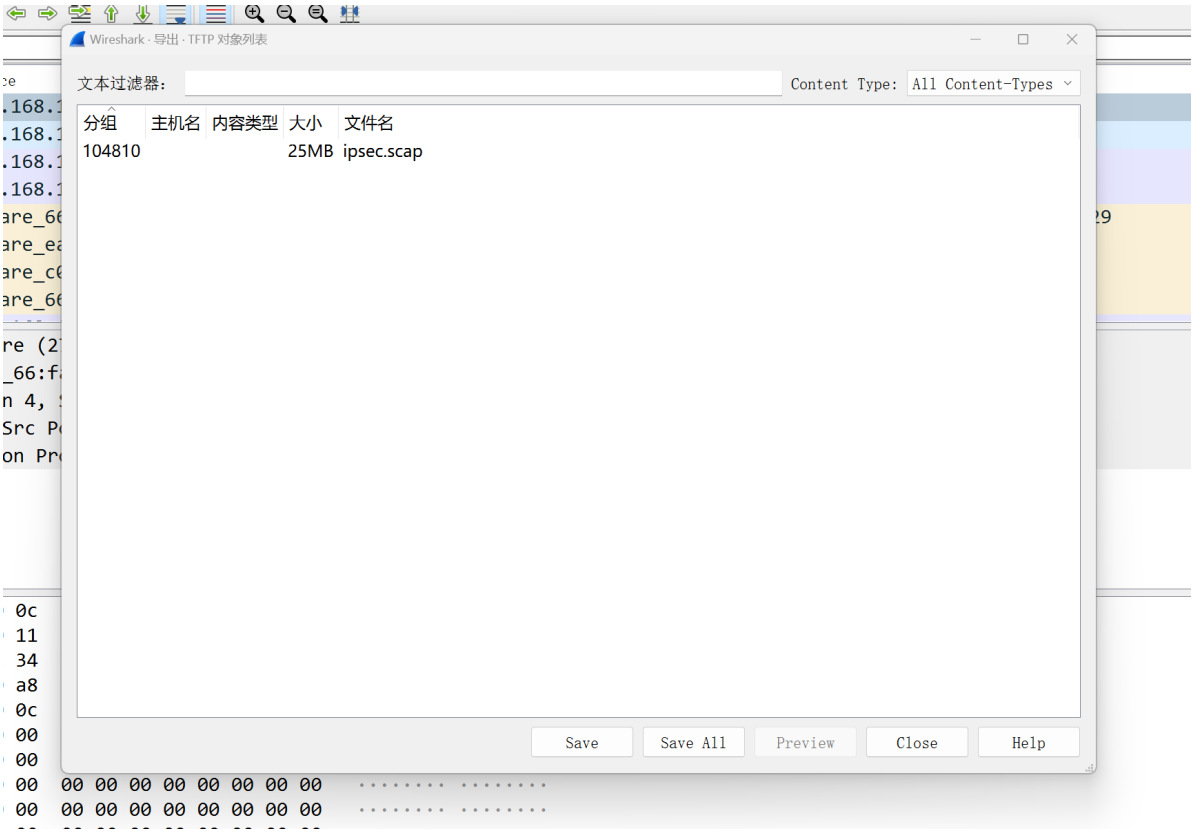
```
127.0.0.1${IFS}&&${IFS}`a="l"{IFS}&&{IFS}b="s"{IFS}&&{IFS}c=$a$b{IFS}&&{IFS}$c`
```

，结果为failed

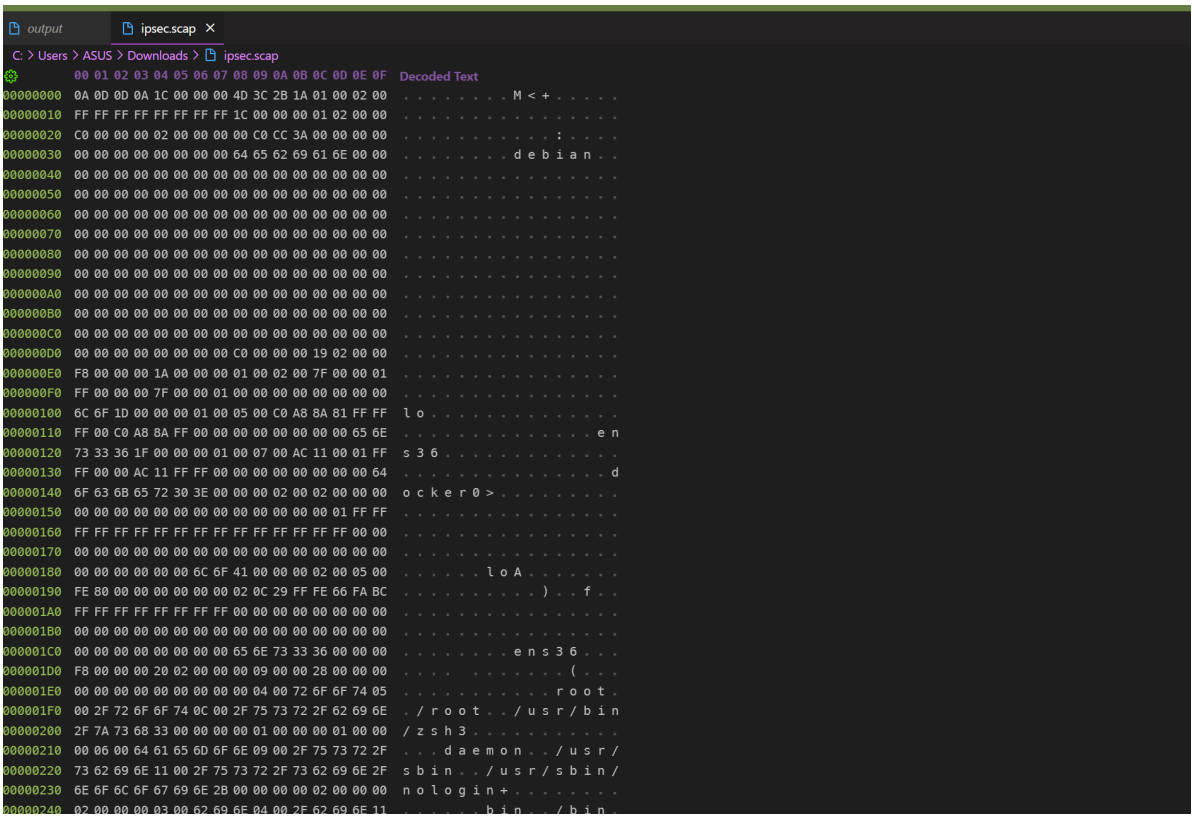
MISC

1.Tunnel

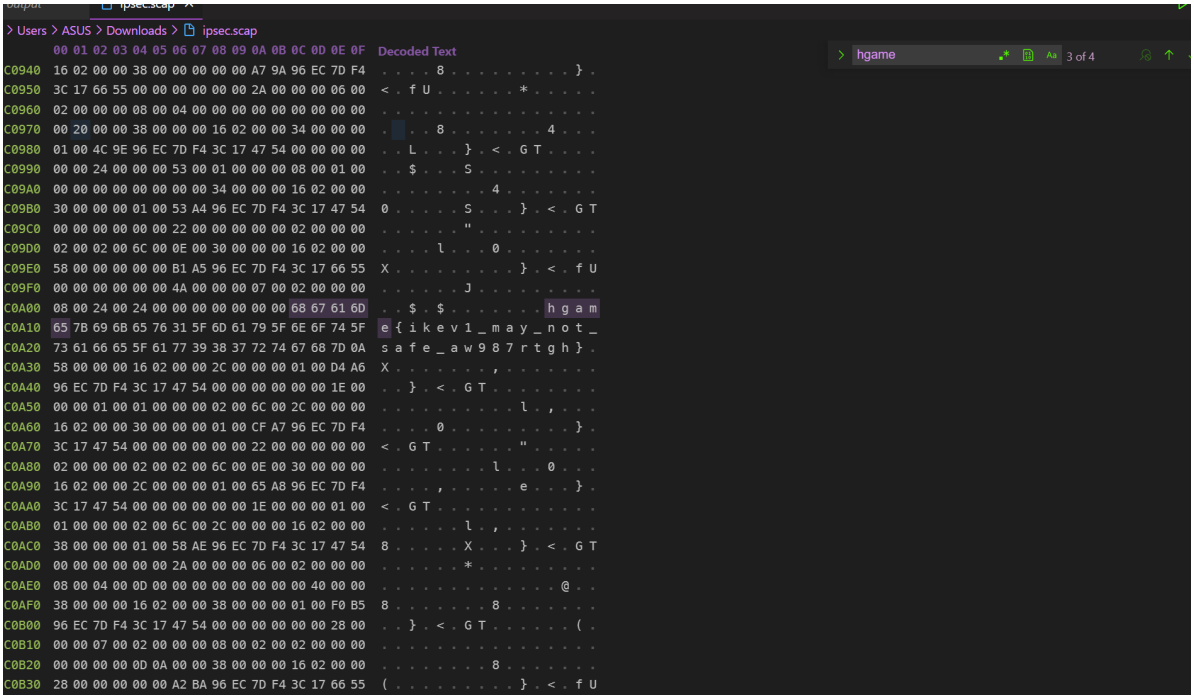
很明显题目说了有非预期，附件打开发现能导出这个玩意



打开看看



很快就找到flag了



3.3ctu4_card_problem

根据提示，与人工智能有关，那么就是我要训练个模型出来整理这些东西

后来给出了hint是CNN，卷积神经网络，这个我是知道的，一开始我也是往这方面想的，所以约等于没有收到hint .QAQ

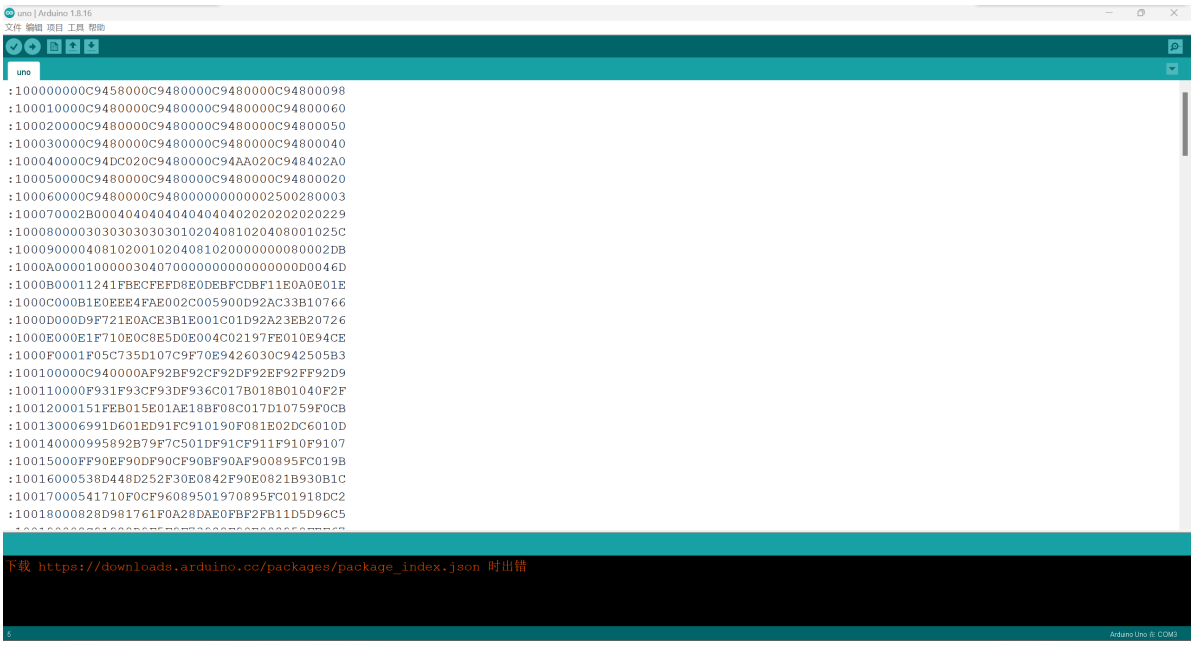
但是我由于不懂训练集咋找，就被搁置了。

IOT

1.another UNO

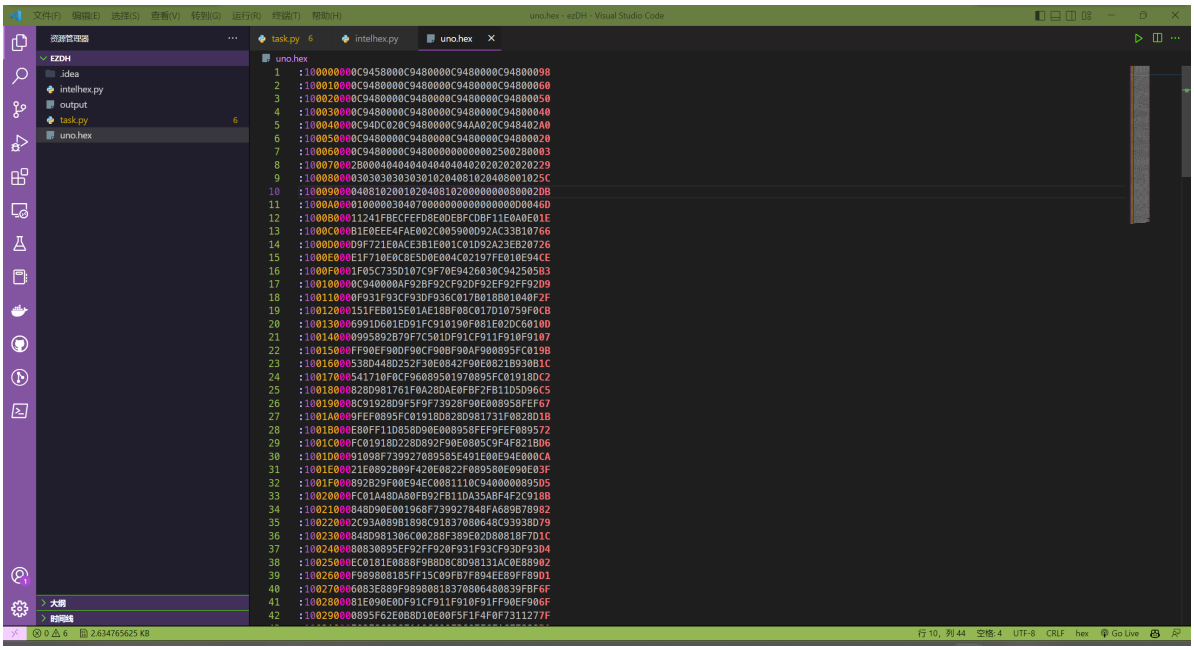
UNO，这个我熟悉，打牌！ （bushi

这个UNO好像不是牌欸，是arduino uno吧大概。这个我也熟悉，我写过巡线小车的代码，也许会吧。也许这个文件丢到arduino 官方的IDE里会有什么发现

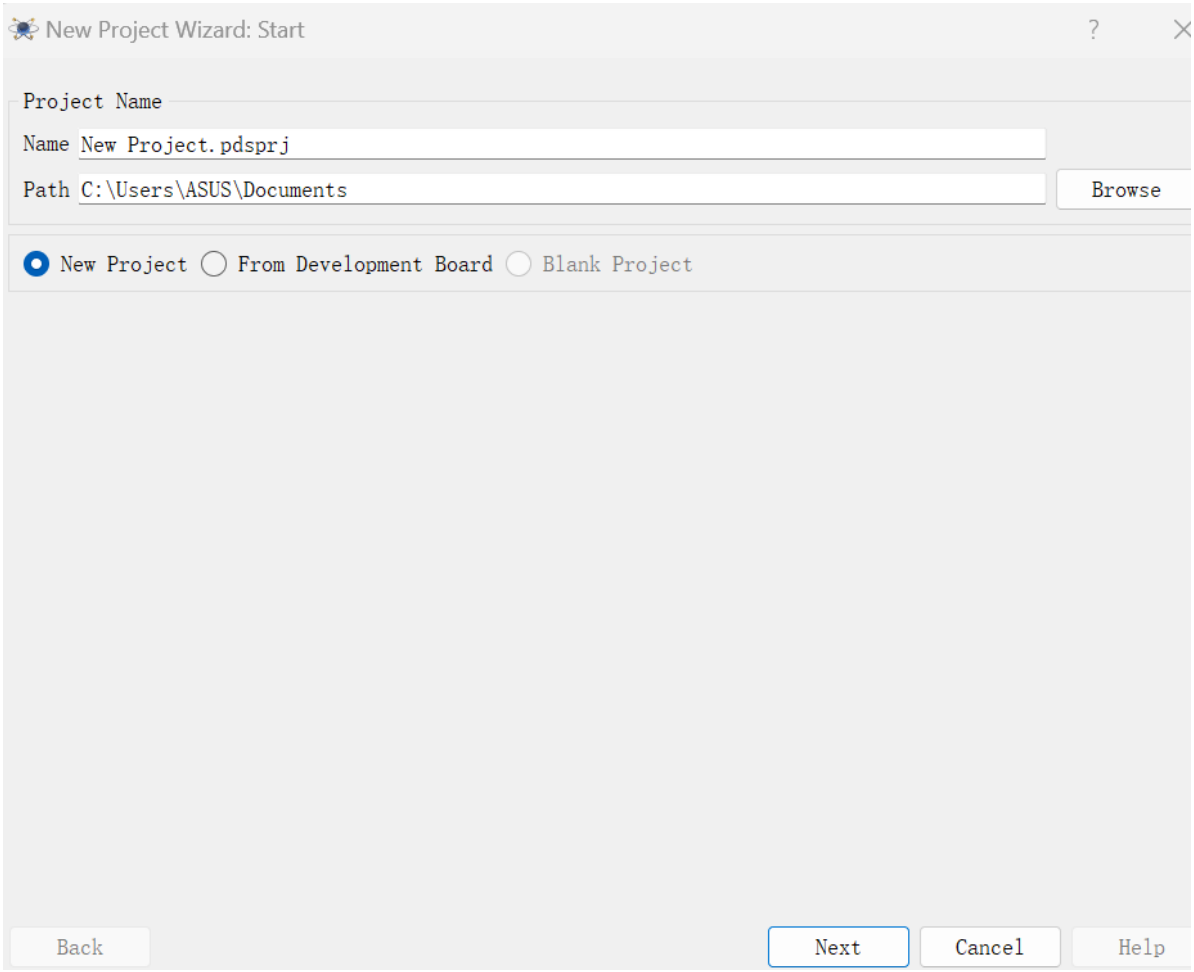


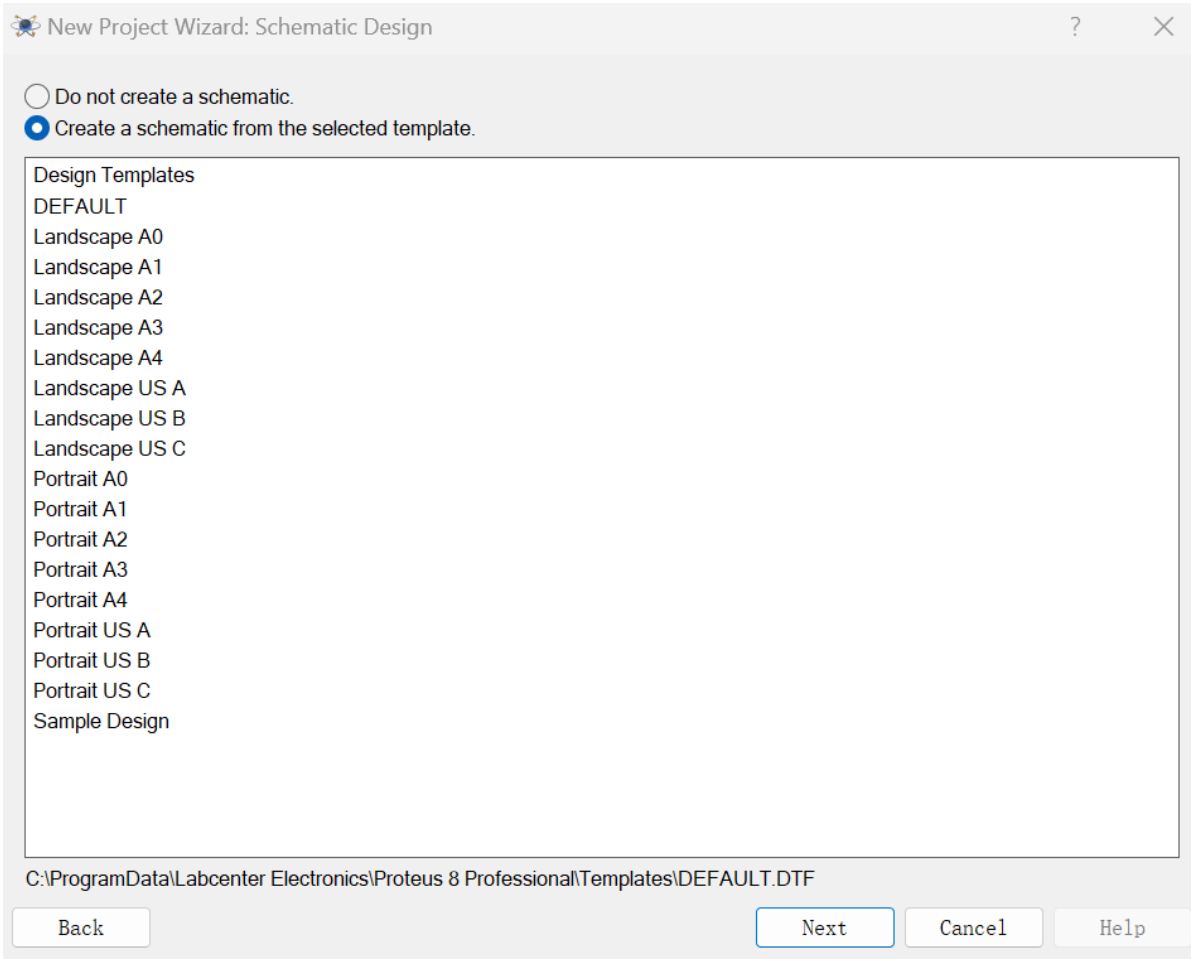
看不懂捏

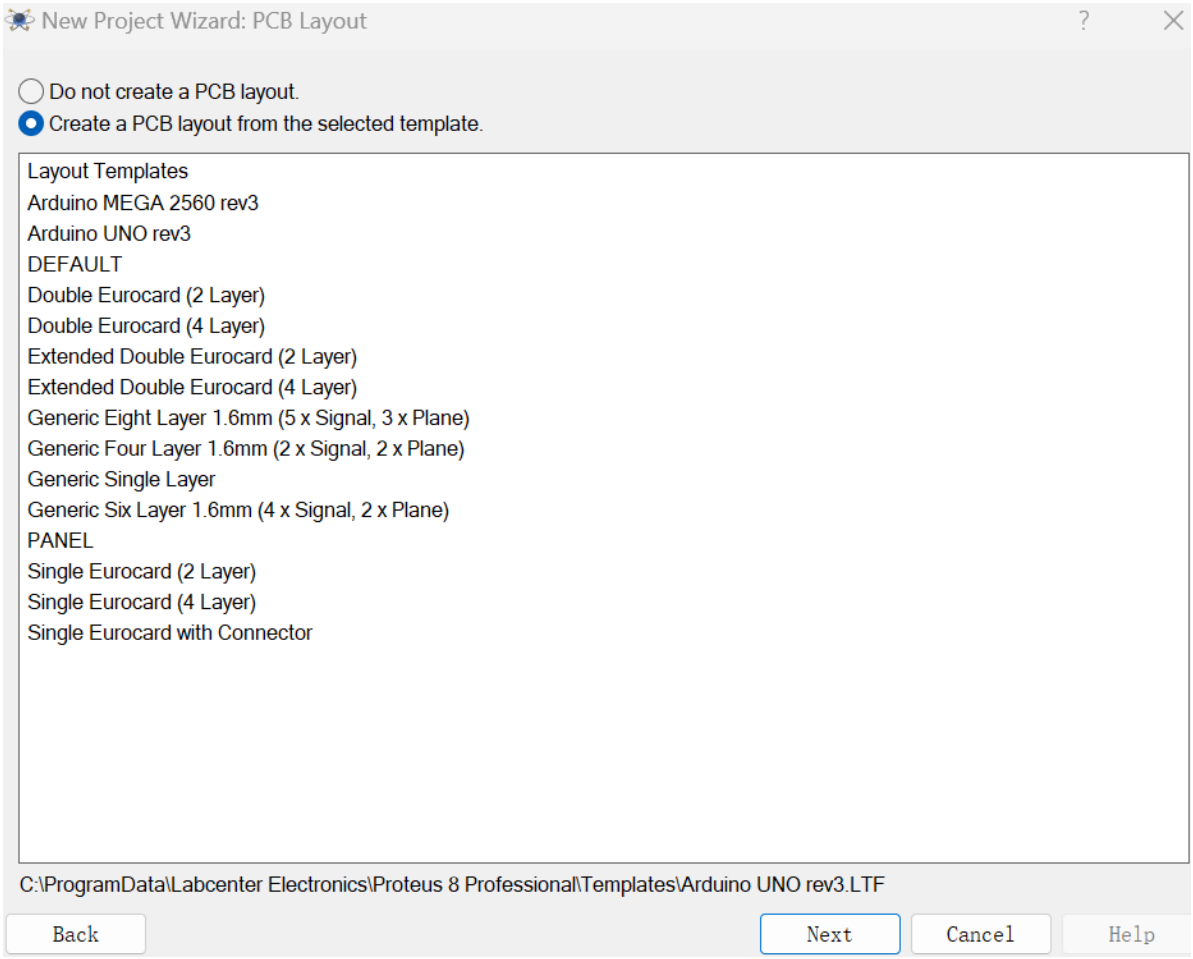
vscode里好像看得更清楚一些。不过还是看不出啥

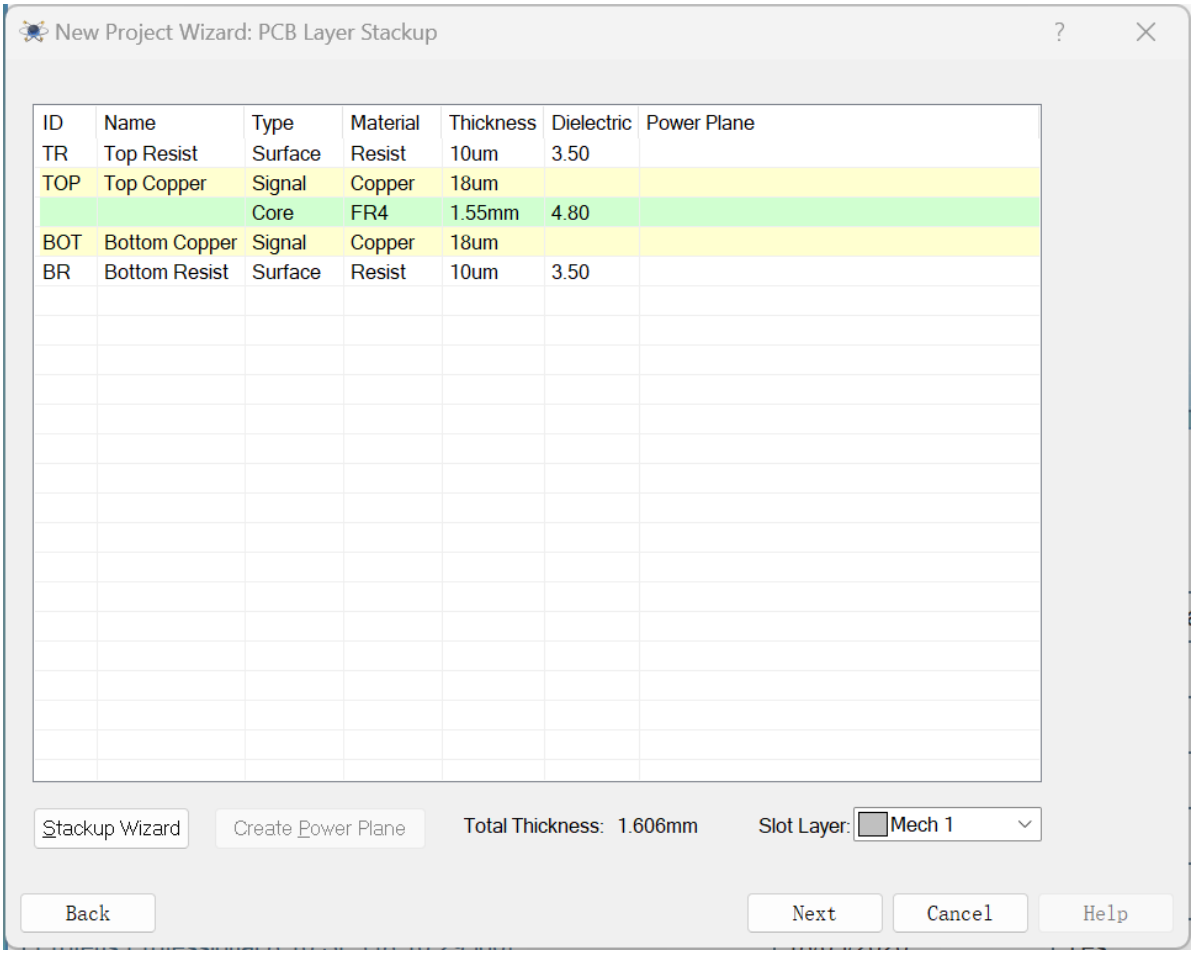


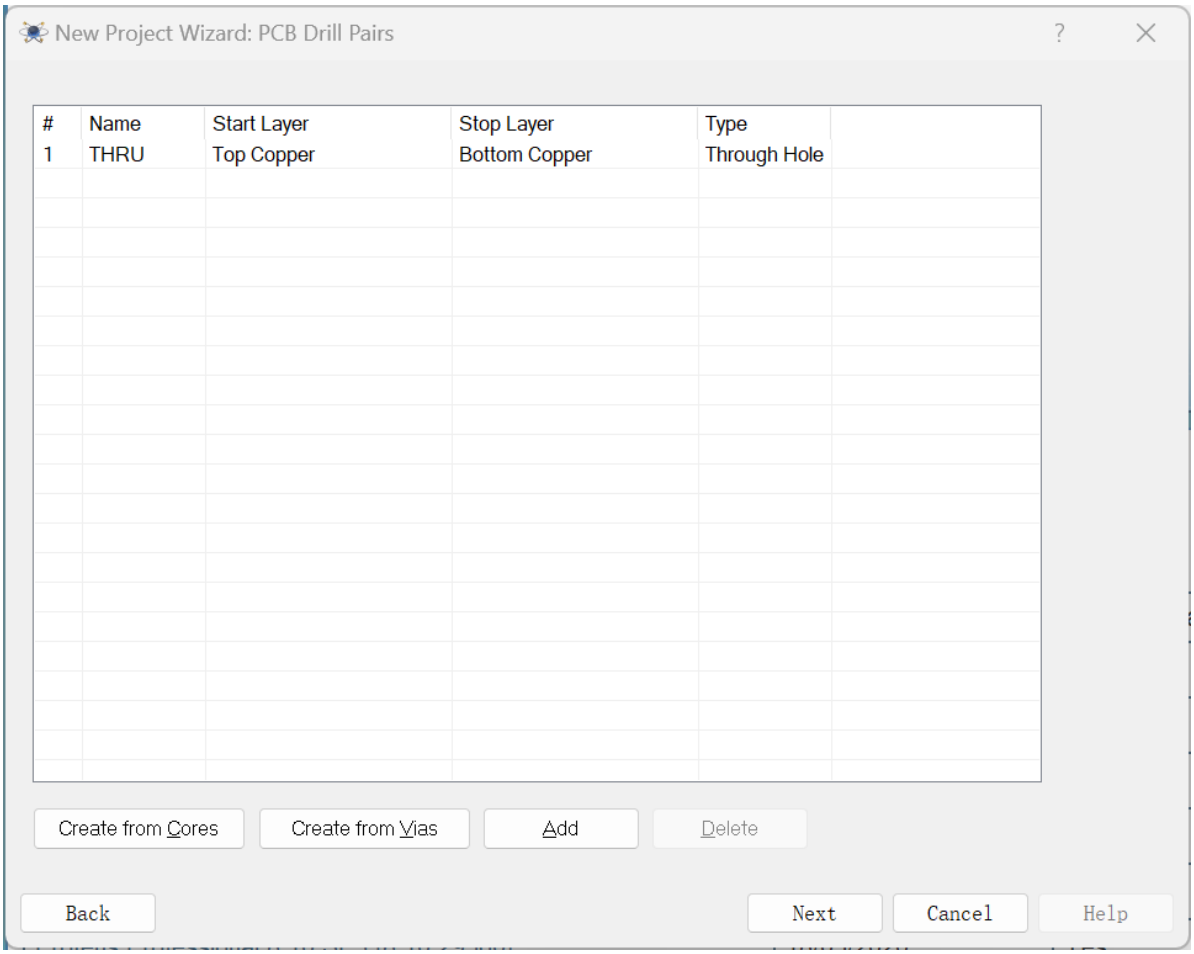
后来有hint用proteus我就去下了一个

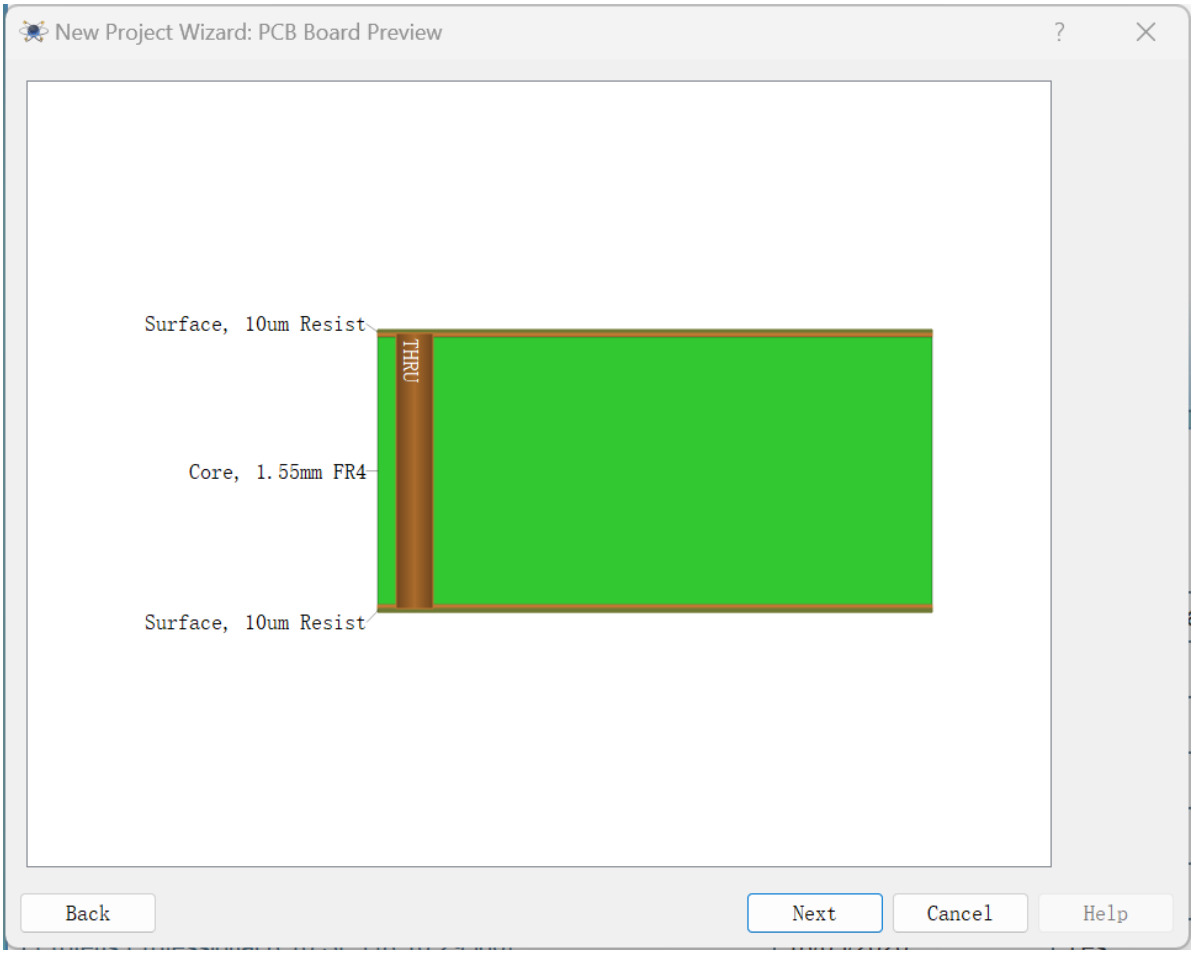



New Project Wizard: Schematic Design
Do not create a schematic.
Create a schematic from the selected template.
Design Templates
DEFAULT
Landscape A0
Landscape A1
Landscape A2
Landscape A3
Landscape A4
Landscape US A
Landscape US B
Landscape US C
Portrait A0
Portrait A1
Portrait A2
Portrait A3
Portrait A4
Portrait US A
Portrait US B
Portrait US C
Sample Design
C:\ProgramData\Labcenter Electronics\Proteus 8 Professional\Templates\DEFAULT.DTF
Back
Next
Cancel
Help

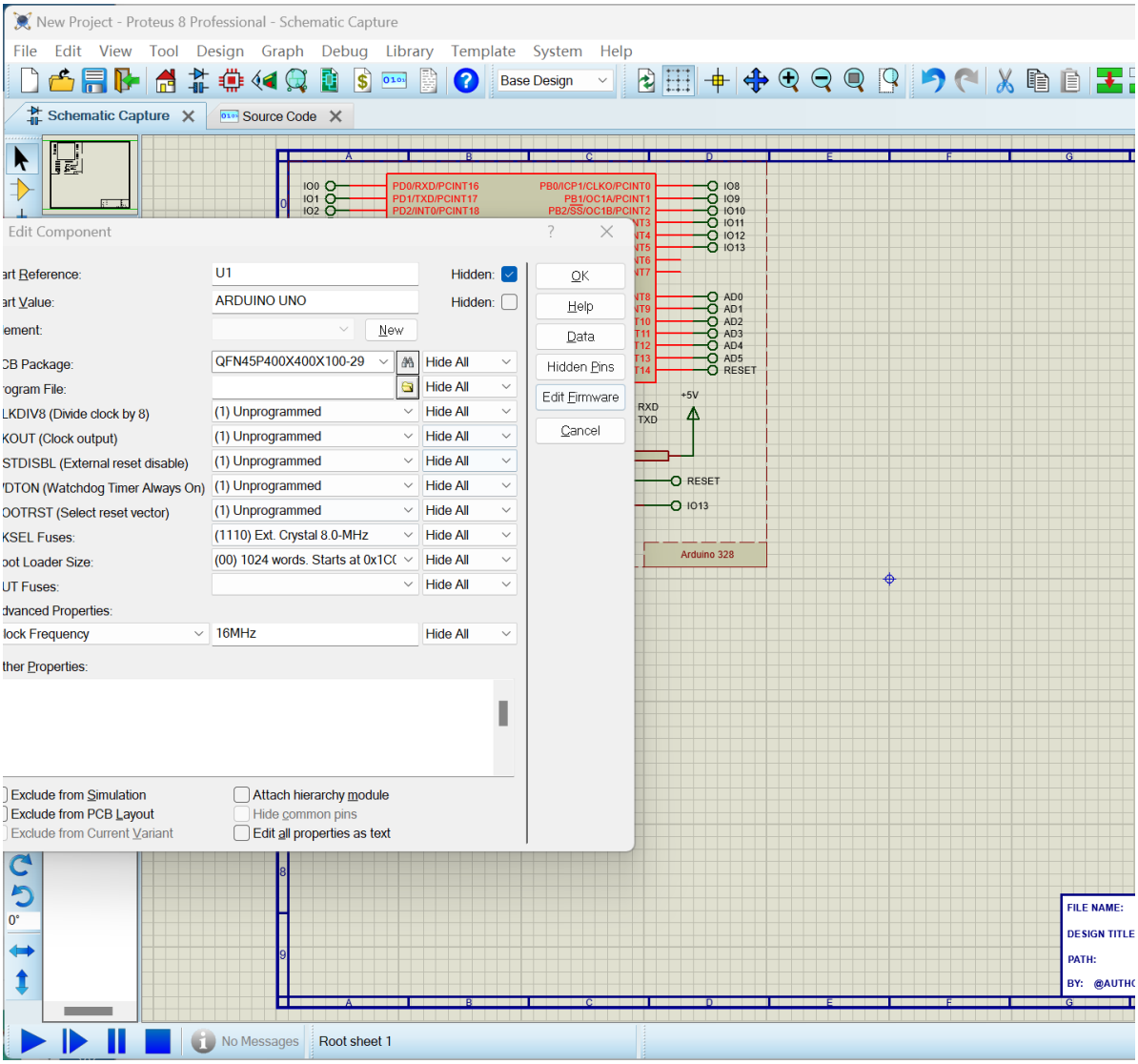

New Project Wizard: PCB Layout
Do not create a PCB layout.
Create a PCB layout from the selected template.
Layout Templates
Arduino MEGA 2560 rev3
Arduino UNO rev3
DEFAULT
Double Eurocard (2 Layer)
Double Eurocard (4 Layer)
Extended Double Eurocard (2 Layer)
Extended Double Eurocard (4 Layer)
Generic Eight Layer 1.6mm (5 x Signal, 3 x Plane)
Generic Four Layer 1.6mm (2 x Signal, 2 x Plane)
Generic Single Layer
Generic Six Layer 1.6mm (4 x Signal, 2 x Plane)
PANEL
Single Eurocard (2 Layer)
Single Eurocard (4 Layer)
Single Eurocard with Connector
C:\ProgramData\Labcenter Electronics\Proteus 8 Professional\Templates\Arduino UNO rev3.LTF
Back
Next
Cancel
Help


New Project Wizard: PCB Layer Stackup
ID Name Type Material Thickness Dielectric Power Plane
TR Top Resist Surface Resist 10um 3.50
TOP Top Copper Signal Copper 18um
Core FR4 1.55mm 4.80
BOT Bottom Copper Signal Copper 18um
BR Bottom Resist Surface Resist 10um 3.50
Stackup Wizard
Create Power Plane
Total Thickness: 1.606mm
Slot Layer: Mech 1
Back
Next
Cancel
Help


New Project Wizard: PCB Drill Pairs
Name Start Layer Stop Layer Type
1 THRU Top Copper Bottom Copper Through Hole
Create from Cores
Create from Vias
Add
Delete
Back
Next
Cancel
Help



一系列操作之后得到了一块赛博UNO板，根据百度知道的内容我可以双击它导入hex文件



导入后查看串口通信什么的还是不太会，感觉还是实物的arduino用起来方便（其实是自己太废物了

本来打算后一天起来再做的，结果肚子不舒服倒在床上躺了一天