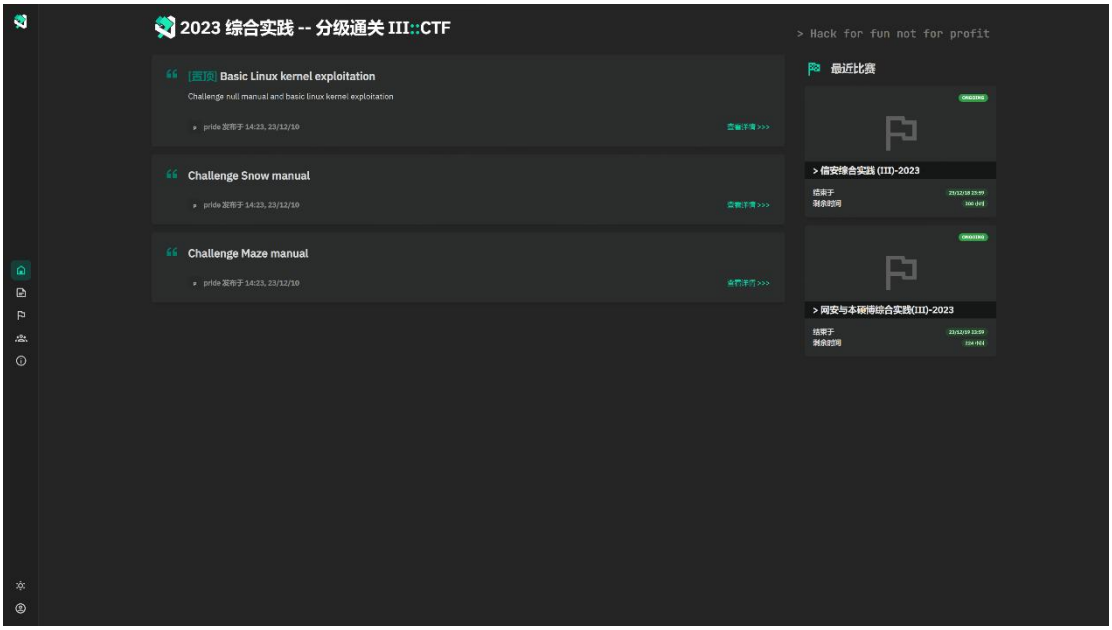
实验网站使用手册-网安版

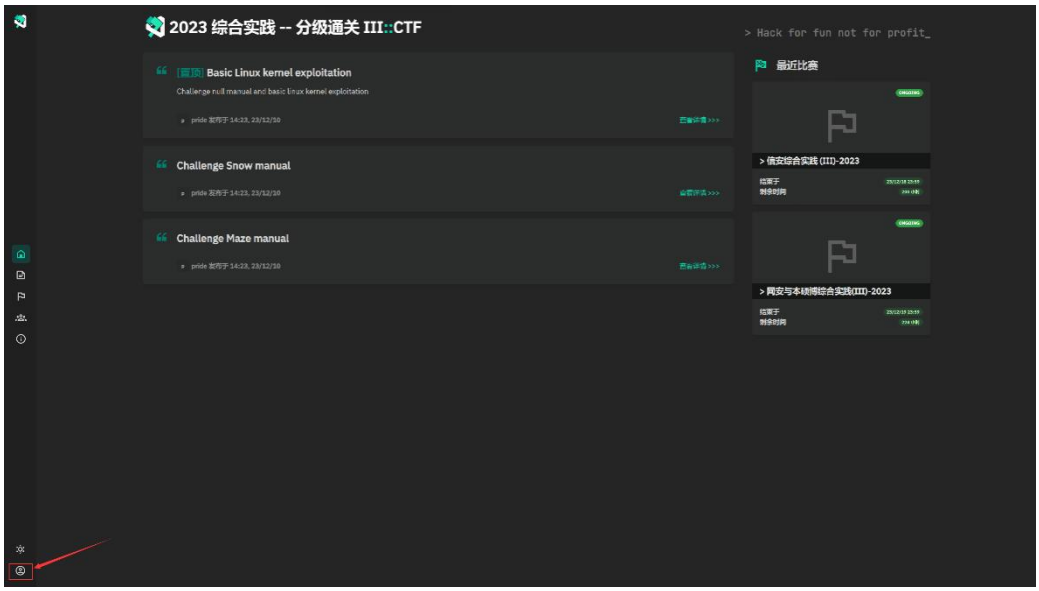
本次综合实践我们的平台网站是：https://kernelpwn.hust.college/

登陆注册

首先当我们打开平台网站的时候，我们可以看到如下图所示的界面。

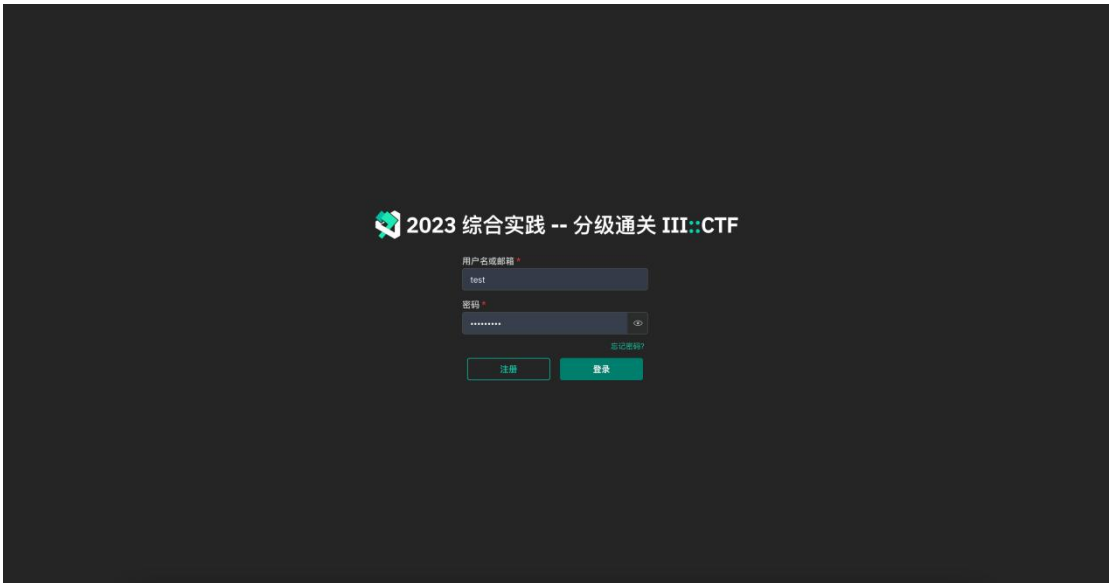


我们点击左下角头像，进行登陆。

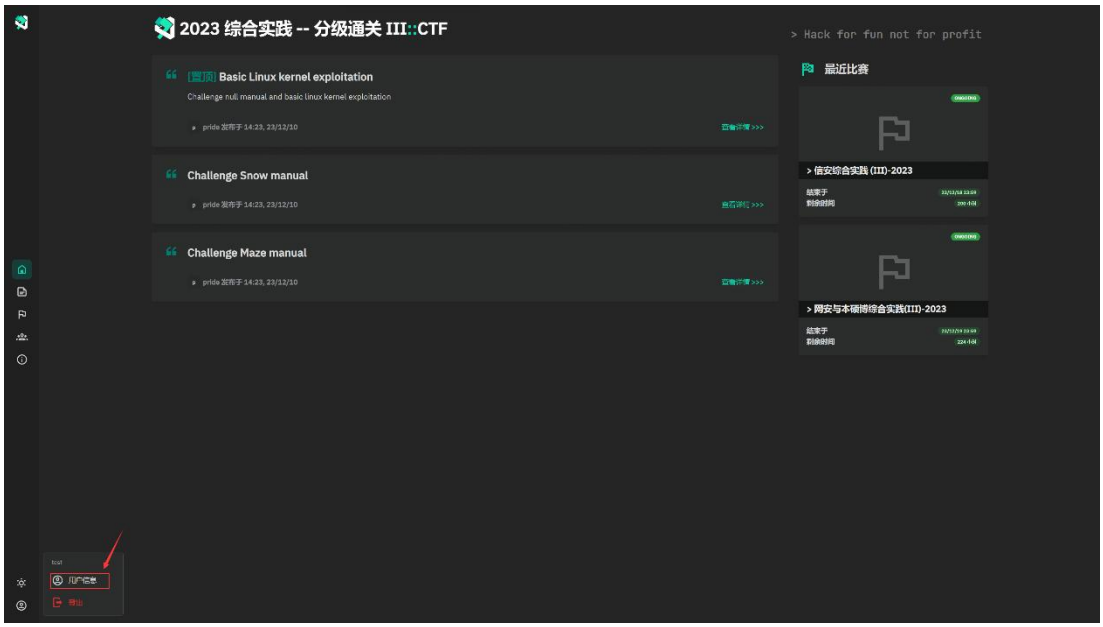


本次综合实践无需注册账户，由管理员统一进行生成，**用户名为学号，密码统一**

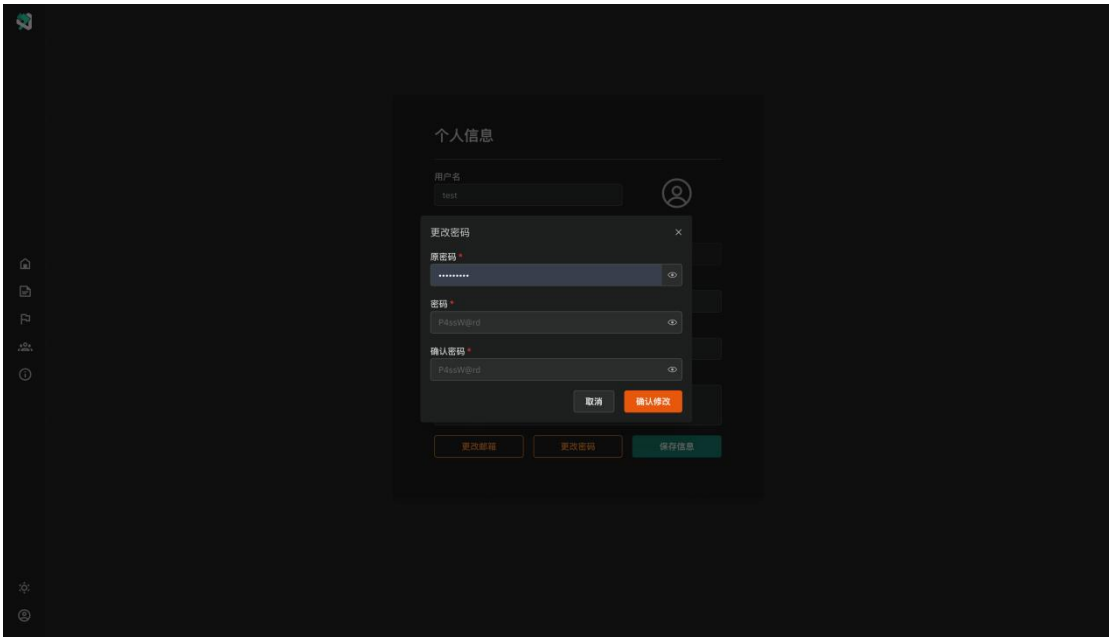
为 Aatest!1，如果登陆异常，请联系助教/管理员。



登陆成功后，我们点击左下角用户信息，进行个人信息的完善和修改，**强烈建议同学们登陆成功后立即修改密码。**



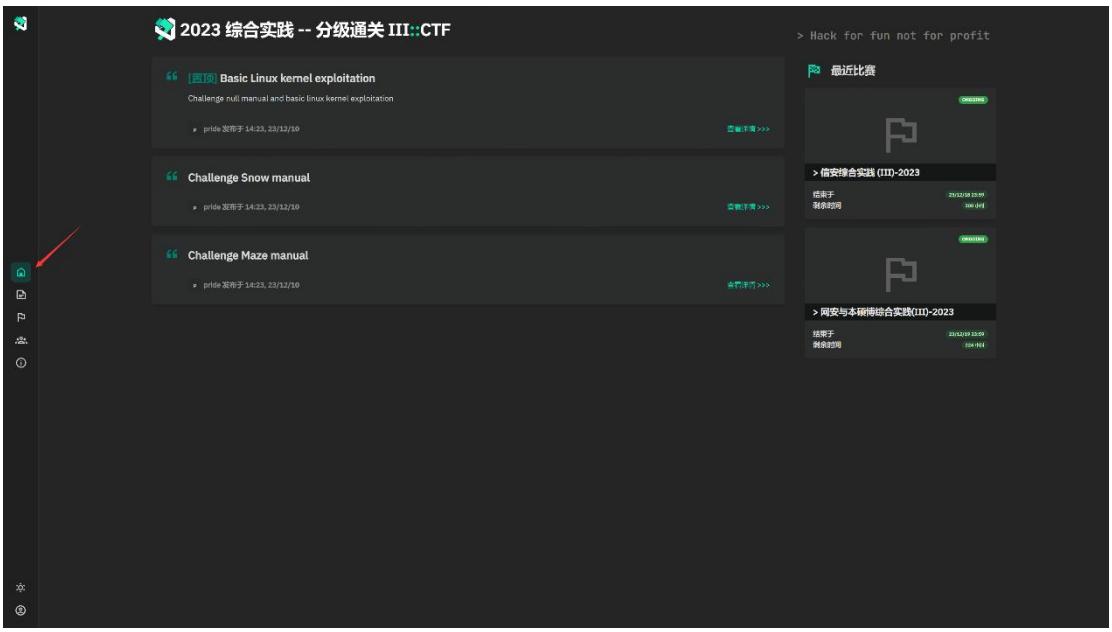
在用户信息界面，我们点击**更新密码**，把密码修改为想要的内容，点击确认修改即可。



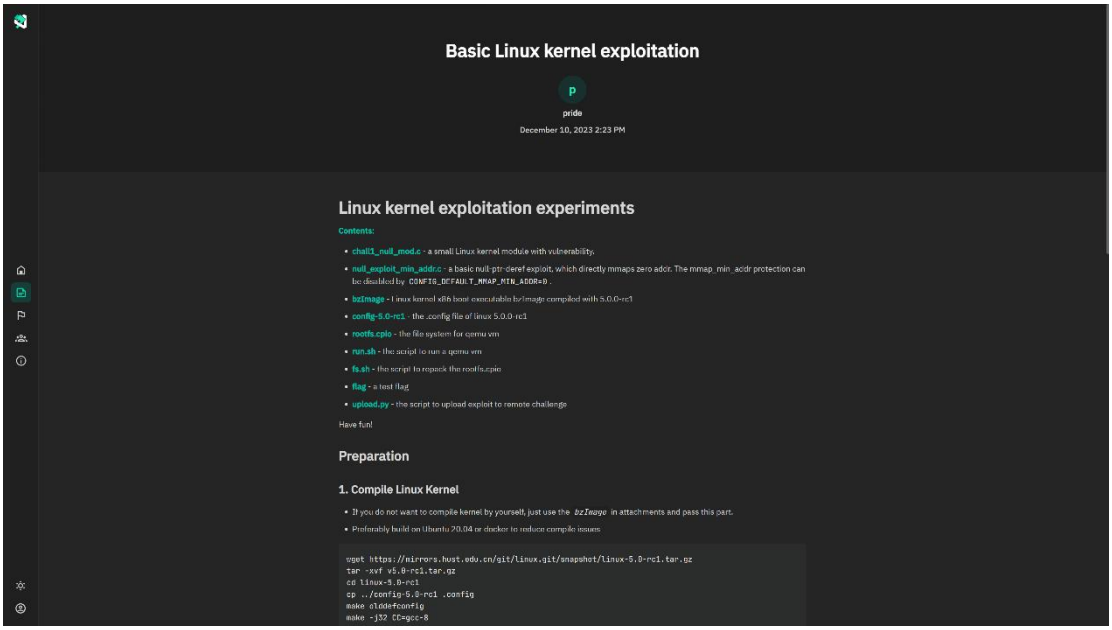
模块介绍

主页/文章

打开网页后，在主页中，有我们综合实践分级通关的必备阅读资料，需要同学们进行详细查看其内容，用来辅助完成分级通关。



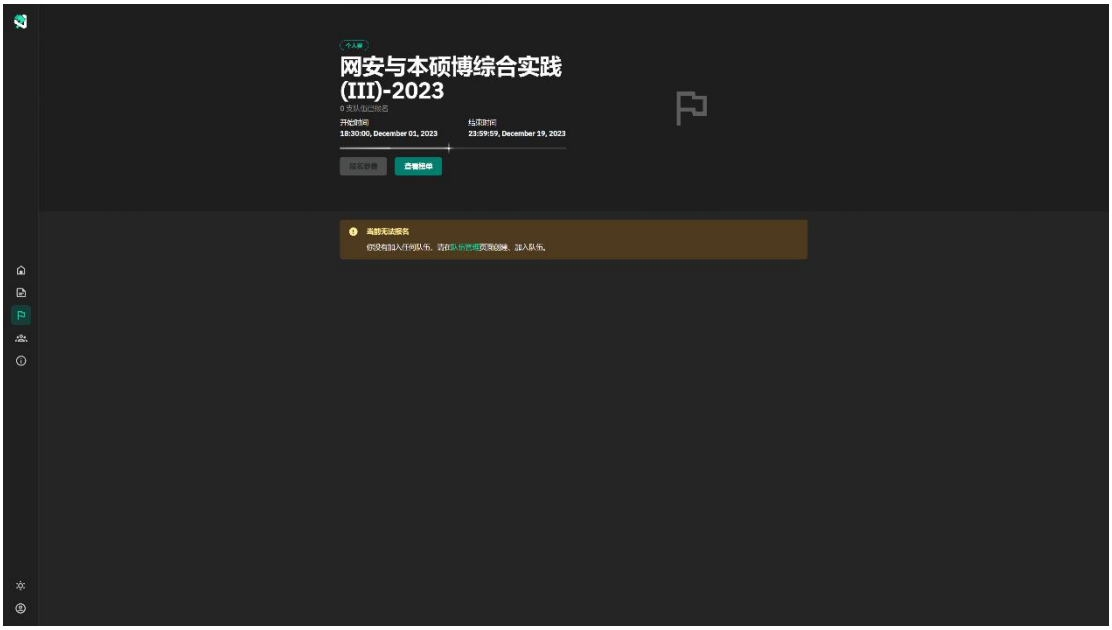
点击查看详情，即可查看对应题目的手册。



通关模块（网安）

点击赛事模块，选择对应实践的关卡。

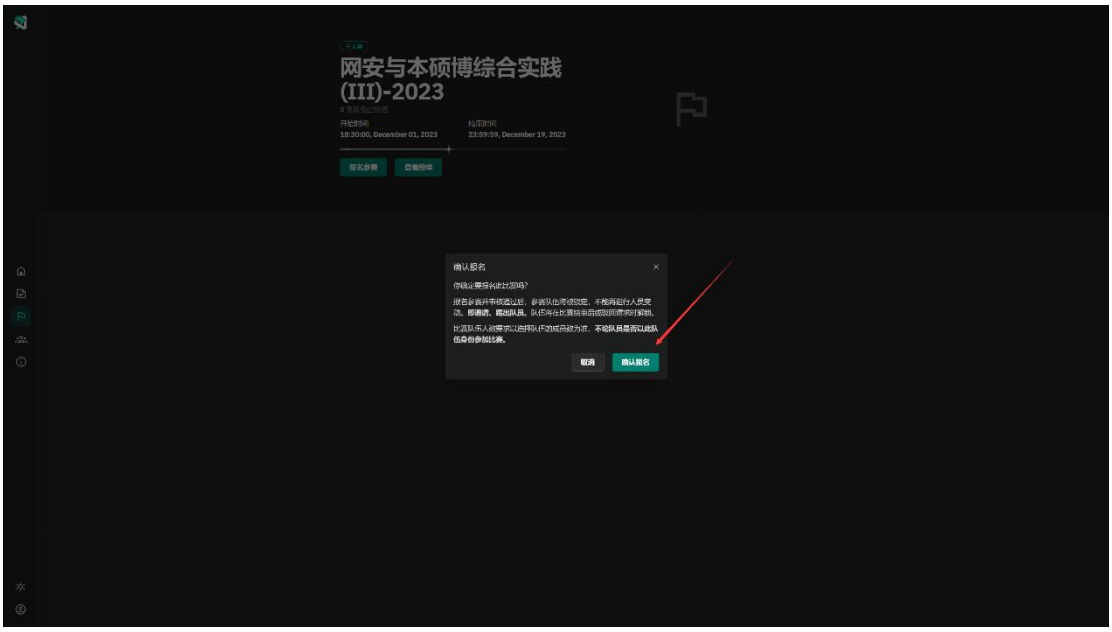
点击任意赛事，根据提示创建自己的队伍，点击**队伍管理。**



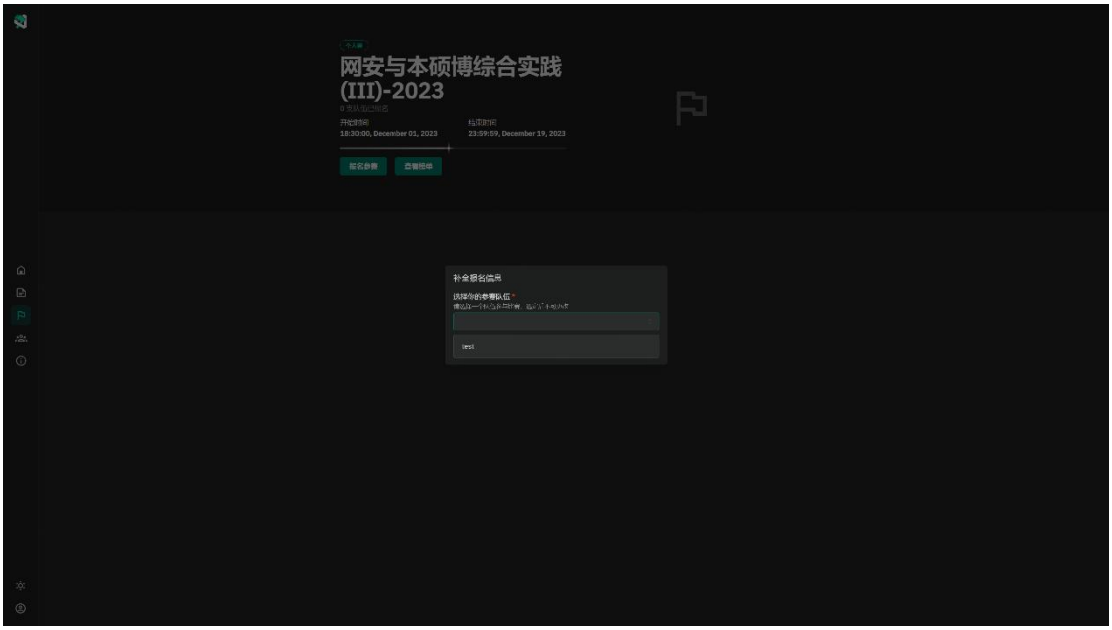
点击右上角，创建队伍，本次综合实践**一个人创建一个队伍**，无需组队邀请。

输入自己的队伍名称，以及队伍签名，点击创建队伍，即可完成。

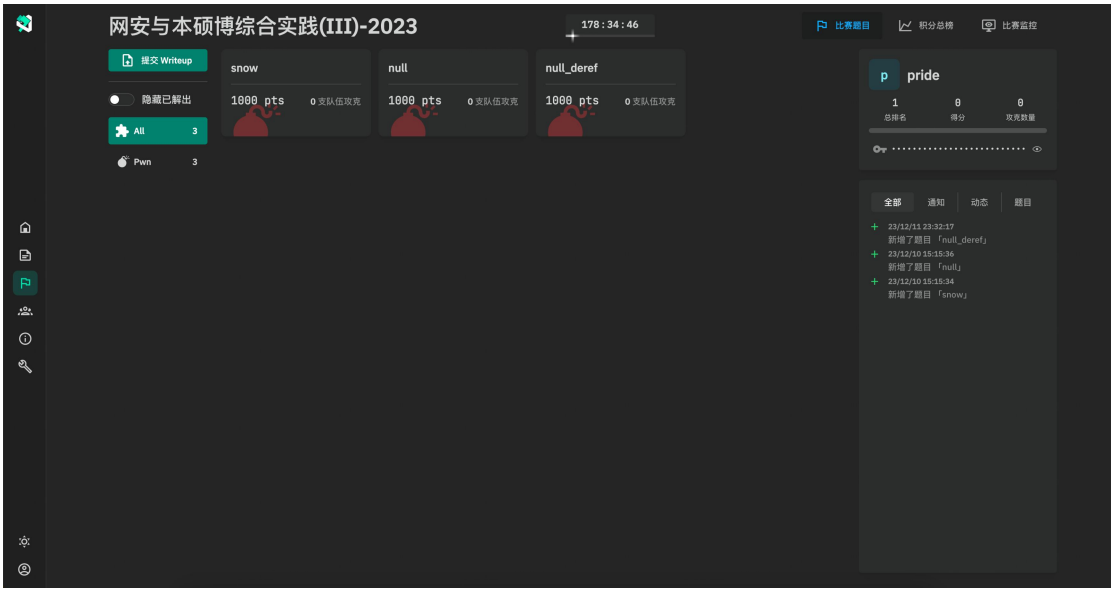
回到赛事界面，点击报名参赛，并确认报名。



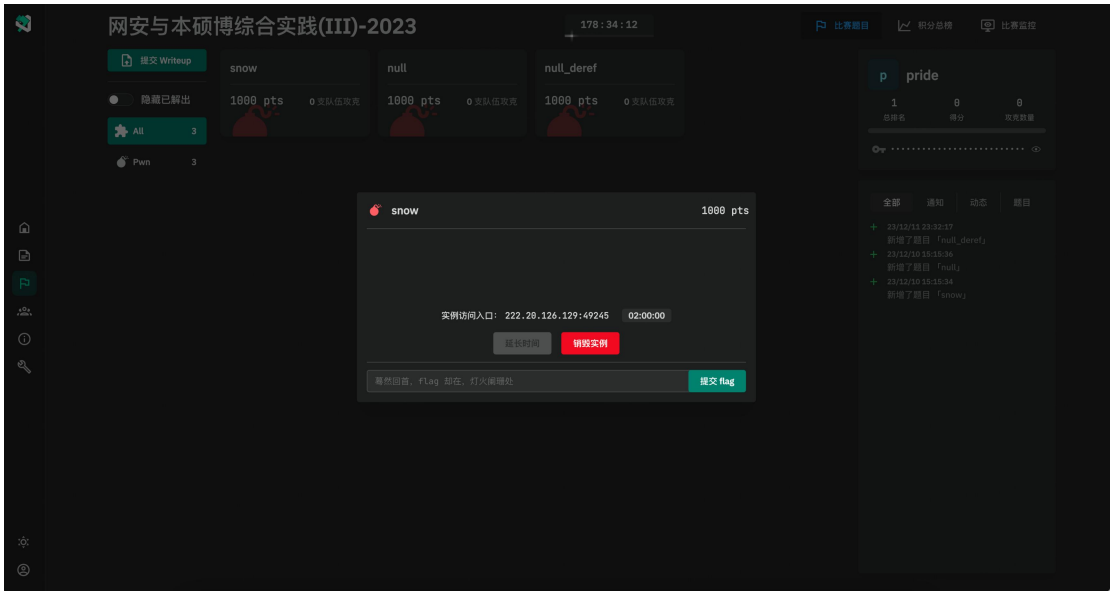
选择自己的队伍，并点击**报名参赛**。



点击进入比赛，选择我们的题目即可开始本次综合实践。



点击题目，选择开启实例，即可获得我们的靶场环境，获取到题目的 flag 后，点击提交 flag 即可完成题目。请注意每个学生远程容器中的 flag 各不相同。



附录

提供文件上传脚本 upload.py

```
#!/usr/bin/env python3
from pwn import *
from sys import argv
import os

if len(sys.argv) <= 3:
        print("Usage: python3 upload.py [exploit file] ip port")
        exit(0)
else:
        ip = sys.argv[2]
        port = sys.argv[3]
# This file is used to upload exploit to remote and execute it
context.log_level = 'debug'

# Remember to replace `ip` and `port` of your docker container
io = remote(ip, port)

def exec_cmd(cmd):
        io.sendline(cmd)
```

```
    io.recvuntil(b"$ ")

def upload(file, remote_path):
    if os.path.exists(file) == False:
        log.info(f"[-]Error: File {file} not found")
        exit(0)

    p = log.progress("Upload")

    # config filename
    local_gzip_f = "./exp.gz"
    remote_base_f = remote_path + "/base_exp"
    remote_gzip_f = remote_path + "/exp.gz"
    remote_rexp_f = remote_path + "/exp"

    os.system(f'strip {file}')
    os.system(f'gzip -c {file} > {local_gzip_f}')
    with open(local_gzip_f, "rb") as f:
        data = f.read()
    encoded = base64.b64encode(data)
    io.recvuntil(b"$ ")

    for i in range(0, len(encoded), 600):
        p.status("%d / %d" % (i, len(encoded)))
        exec_cmd(f"echo \"%s\" >> {remote_base_f}" %
(encoded[i:i+600].decode()))

    exec_cmd(f"cat {remote_base_f} | base64 -d > {remote_gzip_f}")
    exec_cmd(f'gunzip -c {remote_gzip_f} > {remote_rexp_f}')
    exec_cmd(f"chmod +x {remote_rexp_f}")

    # trigger remote exploit
    io.sendline(f"{remote_rexp_f}")

upload(argv[1], "/home/ctf")
context.log_level = 'debug'
```

```
io.interactive()
```

我们需要通过执行 python3 upload_py3.py [exploit file] ip port 来上传我们编译完成的 exp，然后执行上传脚本。