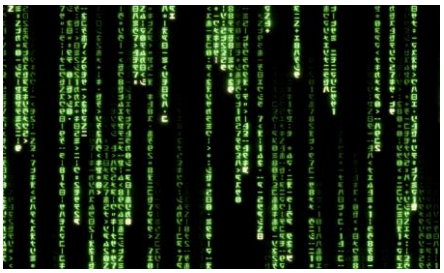
Hgame 2023 Week2 Writeup

Web

git leakage

直接点进链接，什么都看不到，查看网页源码也没有发现什么有用信息。



回到题目，git 泄露，使用 GitHack 获取 git 文件，就得到了 flag。

```
┌──(ke㉿ke)-[~]
└─$ GitHack

┌──(ke㉿ke)-[~/GitHack]
└─$ ls
data  dist  GitHack.py  lib  LICENSE  README.md

┌──(ke㉿ke)-[~/GitHack]
└─$ cd ./dist/week-2.hgame.lwsec.cn_30213

┌──(ke㉿ke)-[~/GitHack/dist/week-2.hgame.lwsec.cn_30213]
└─$ ls
Th1s_1s-flag

┌──(ke㉿ke)-[~/GitHack/dist/week-2.hgame.lwsec.cn_30213]
└─$ cat Th1s_1s-flag
hgame{Don't^put*Git-in_web_directory}

┌──(ke㉿ke)-[~/GitHack/dist/week-2.hgame.lwsec.cn_30213]
└─$
```

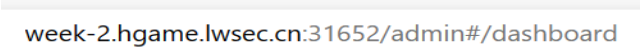
v2broad

利用搜索引擎，发现这是真实事件改编的题目。

根据网上的教程，首先注册普通用户，登陆，然后在响应里获取 auth_data，

```
▼ {data: {token: "ff870e9a73af54fef4d5e3c7dfa313a3",…}}
  ▼ data: {token: "ff870e9a73af54fef4d5e3c7dfa313a3",…}
      auth_data: "MTIzQHFxLmNvbTokMnkkMTAkVnZPRFUvVHMwbnNTQS5ybzk5REpEdUpQeEwzZE9BN1NlYWJkb0szWU9RaGlpTVlmVnRwYi4="
      token: "ff870e9a73af54fef4d5e3c7dfa313a3"
```

然后退出，利用 burpsuit，在再次登陆时将上述获得的 auth_data 作为 authorization 头，发送到/api/v1/user/login 接口，我们就有了管理员权限，可以修改 admin 用户密码了。



然后登陆 admin 用户，即可在响应头里找到 token，用 hgame{}包裹，就是 flag。


```
▼ {data: {token: "39d580e71705f6abac9a414def74c466",…}}
  ▼ data: {token: "39d580e71705f6abac9a414def74c466",…}
      auth_data: "YWRtaW5AZXhhbXBsZS5jb206JDJ5JDEwJGFlSUFLTnRzTFg4OW03c0pNTG5pbXVDQm4udUJuaFZNSTc3TlV1THRuNlVwclc0ay5xYkpt"
      is_admin: true
      token: "39d580e71705f6abac9a414def74c466"
```


Misc

Tetris Master（50pt）

```
Host 'week-2.hgame.lwsec.cn' resolved to 101.37.12.59.
Connecting to 101.37.12.59:31576...
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.

WARNING! The remote SSH server rejected X11 forwarding request.
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.15.0-53-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Are you tetris master?[y/n]
^Cctf@gamebox-3232-96-b21b6b360ae69e09:~$ cat flag
hgame{Bash_Game^Also*Can#Rce}
ctf@gamebox-3232-96-b21b6b360ae69e09:~$ ^C
ctf@gamebox-3232-96-b21b6b360ae69e09:~$
```

这题由于某些问题，有漏洞，连上 ssh 之后，直接 ctrl+c 退出当前程序就进了终端，直接 cat flag 就解决了。