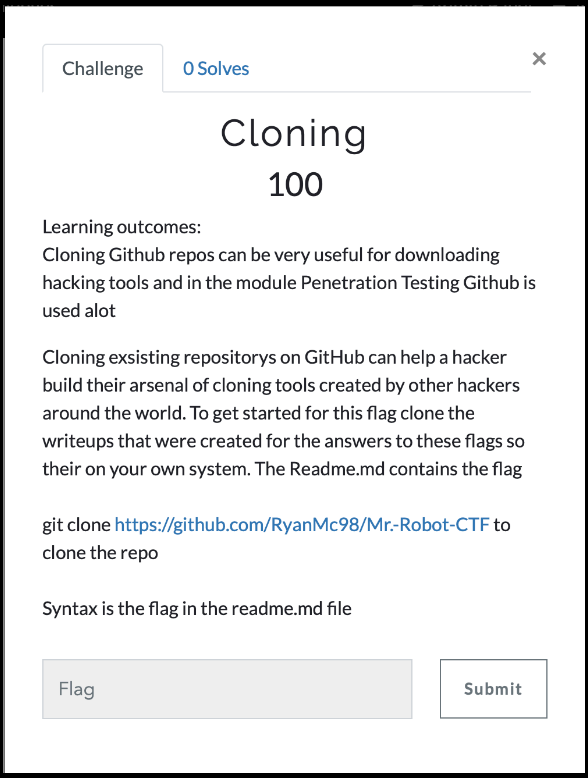
MR. ROBOT

1. In this challenge we have to clone the Mr-Robot-CTF repository from GitHub using the command provided. Within this repository there is a headmen.MD that contains the flag



Cloning

100

Learning outcomes:
Cloning Github repos can be very useful for downloading hacking tools and in the module Penetration Testing Github is used alot

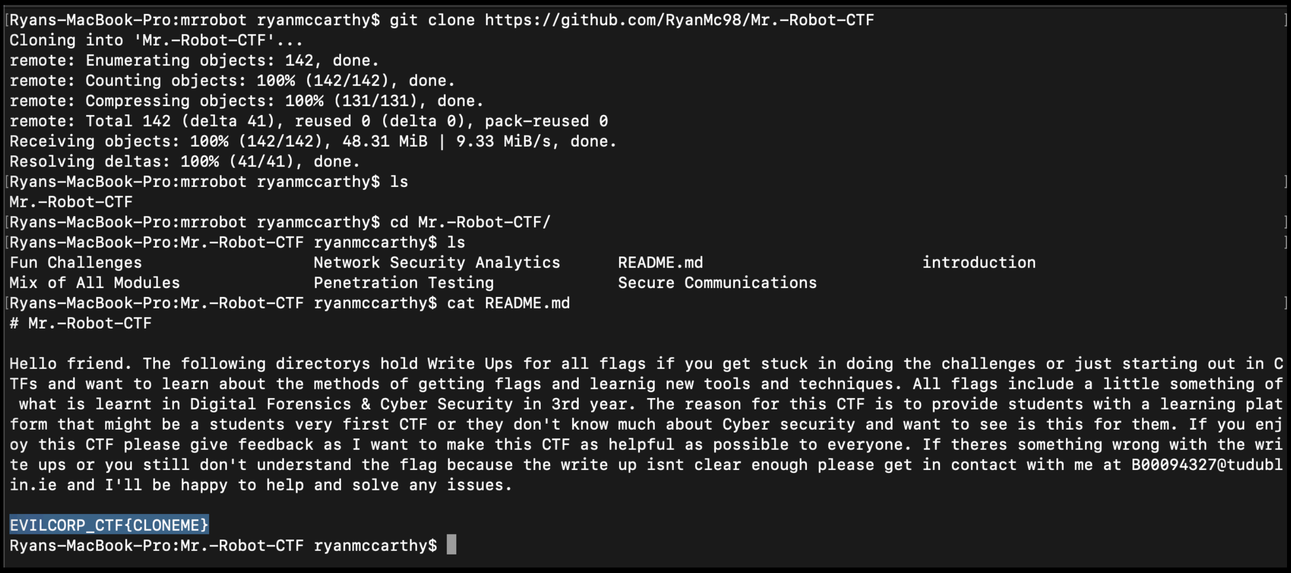
Cloning exsisting repositorys on GitHub can help a hacker build their arsenal of cloning tools created by other hackers around the world. To get started for this flag clone the writeups that were created for the answers to these flags so their on your own system. The Readme.md contains the flag

git clone https://github.com/RyanMc98/Mr.-Robot-CTF to clone the repo

Syntax is the flag in the readme.md file

2. So open the terminal and do the following commands to get the flag. Each of these commands are broke down below:
   git clone https://github.com/RyanMc98/Mr.-Robot-CTF - download repository
   ls - list the directory to see did the repo download
   cd Mr-Robot-CTF - to change into the repository directory
   ls - list the contents in the repository
   cat README.md - to view the contents of this file and see the flag

As you can see the flag can be seen after viewing the contents of README.md which is EVILCORP_CTF{CLONEME}

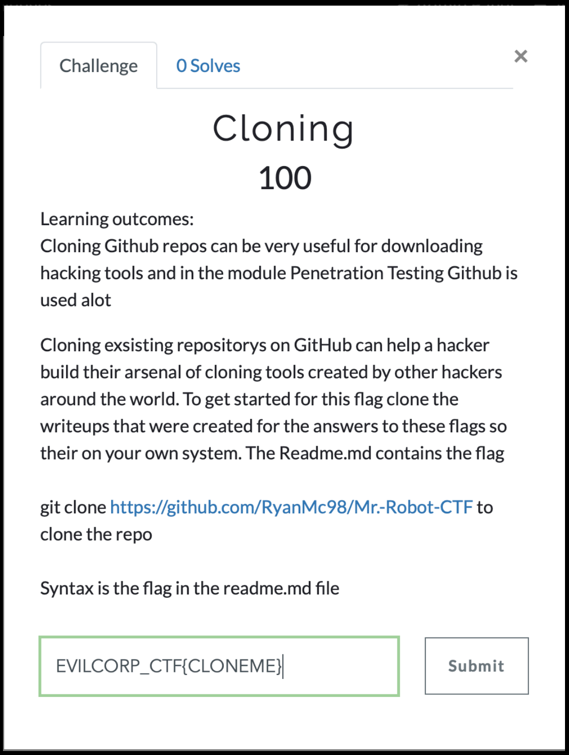


```
Ryans-MacBook-Pro:mrrobot ryanmccarthy$ git clone https://github.com/RyanMc98/Mr.-Robot-CTF
Cloning into 'Mr.-Robot-CTF'...
remote: Enumerating objects: 142, done.
remote: Counting objects: 100% (142/142), done.
remote: Compressing objects: 100% (131/131), done.
remote: Total 142 (delta 41), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (142/142), 48.31 MiB | 9.33 MiB/s, done.
Resolving deltas: 100% (41/41), done.
Ryans-MacBook-Pro:mrrobot ryanmccarthy$ ls
Mr.-Robot-CTF
Ryans-MacBook-Pro:mrrobot ryanmccarthy$ cd Mr.-Robot-CTF/
Ryans-MacBook-Pro:Mr.-Robot-CTF ryanmccarthy$ ls
Fun Challenges                  Network Security Analytics      README.md                       introduction
Mix of All Modules              Penetration Testing             Secure Communications
Ryans-MacBook-Pro:Mr.-Robot-CTF ryanmccarthy$ cat README.md
# Mr.-Robot-CTF

Hello friend. The following directorys hold Write Ups for all flags if you get stuck in doing the challenges or just starting out in C
TFs and want to learn about the methods of getting flags and learnig new tools and techniques. All flags include a little something of
 what is learnt in Digital Forensics & Cyber Security in 3rd year. The reason for this CTF is to provide students with a learning plat
form that might be a students very first CTF or they don't know much about Cyber security and want to see is this for them. If you enj
oy this CTF please give feedback as I want to make this CTF as helpful as possible to everyone. If theres something wrong with the wri
te ups or you still don't understand the flag because the write up isnt clear enough please get in contact with me at B00094327@tudubl
in.ie and I'll be happy to help and solve any issues.

EVILCORP_CTF{CLONEME}
Ryans-MacBook-Pro:Mr.-Robot-CTF ryanmccarthy$
```

3. Put EVILCORP_CTF{CLONEME} to complete the challenge.



Cloning

100

Learning outcomes:
Cloning Github repos can be very useful for downloading hacking tools and in the module Penetration Testing Github is used alot

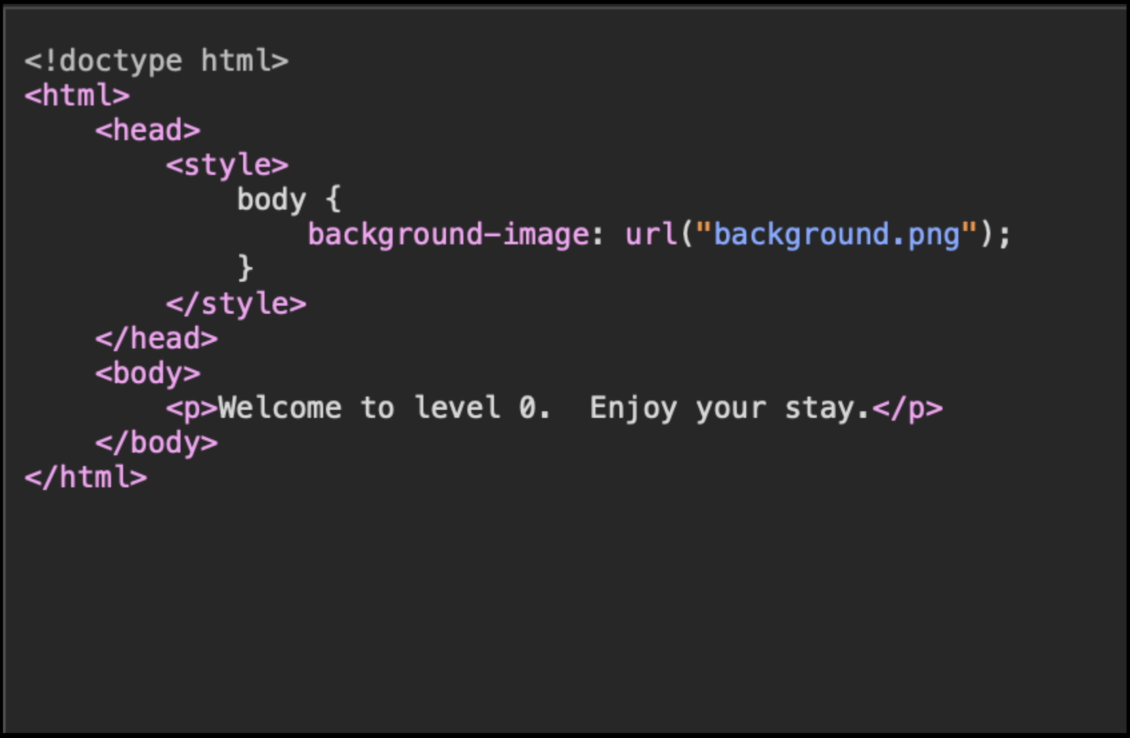
Cloning exsisting repositorys on GitHub can help a hacker build their arsenal of cloning tools created by other hackers around the world. To get started for this flag clone the writeups that were created for the answers to these flags so their on your own system. The Readme.md contains the flag

git clone https://github.com/RyanMc98/Mr.-Robot-CTF to clone the repo

Syntax is the flag in the readme.md file

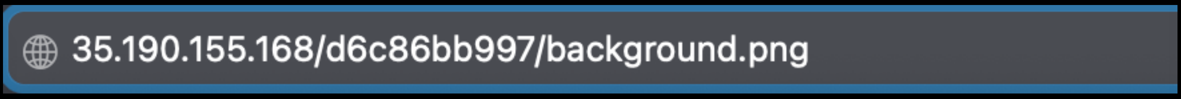
EVILCORP_CTF{CLONEME}

3. The page source shows what is showing below. Notice that there is a background.png as the image but we can't see anything. Its also in a URL bracket so this gives the hint to use the URL to redirect to see is there a page called background.png

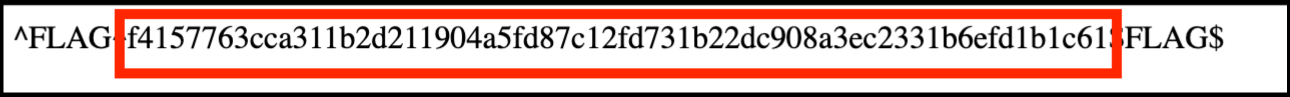


```
<!doctype html>
<html>
    <head>
        <style>
            body {
                background-image: url("background.png");
            }
        </style>
    </head>
    <body>
        <p>Welcome to level 0.  Enjoy your stay.</p>
    </body>
</html>
```

3. In the URL as shown below add background.png to be redirected to the hidden directory. When pressing enter another page pops up and the flag can be seen like below.

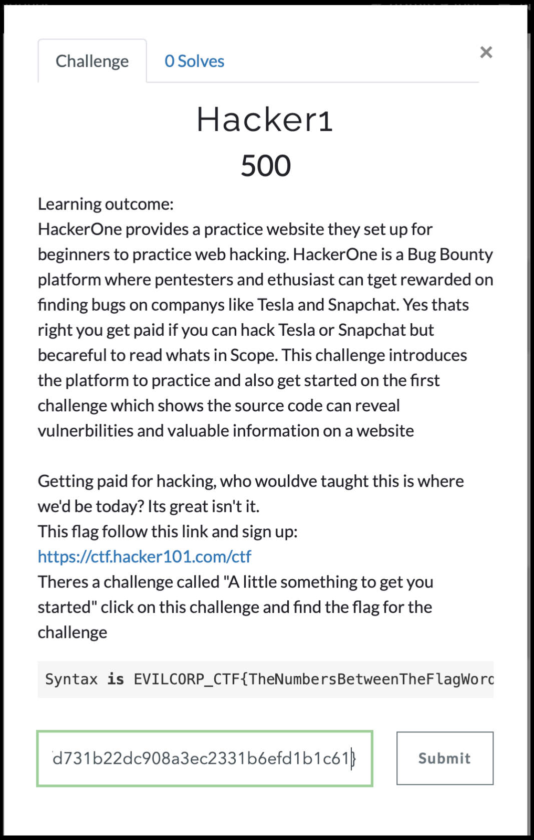


35.190.155.168/d6c86bb997/background.png



^FLAG^f4157763cca311b2d211904a5fd87c12fd731b22dc908a3ec2331b6efd1b1c61$FLAG$

The answer to this flag is
EVILCORP_CTF{f4157763cca311b2d211904a5fd87c12fd731b22dc908a3ec2331b6efd1b1c61}



Hacker1

500

Learning outcome:
HackerOne provides a practice website they set up for beginners to practice web hacking. HackerOne is a Bug Bounty platform where pentesters and ethusiast can tget rewarded on finding bugs on companys like Tesla and Snapchat. Yes thats right you get paid if you can hack Tesla or Snapchat but becareful to read whats in Scope. This challenge introduces the platform to practice and also get started on the first challenge which shows the source code can reveal vulnerbilities and valuable information on a website

Getting paid for hacking, who wouldve taught this is where we'd be today? Its great isn't it.
This flag follow this link and sign up:
https://ctf.hacker101.com/ctf
Theres a challenge called "A little something to get you started" click on this challenge and find the flag for the challenge

```
Syntax is EVILCORP_CTF{TheNumbersBetweenTheFlagWorc
```

d731b22dc908a3ec2331b6efd1b1c61}