

# MR. ROBOT

1. In this challenge involves using another platform to find the flag. The link to this platform is provided. Also the challenge is the flag that is found on a challenge called “A little something To get You Started”

Challenge

0 Solves

×

## 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 enthusiasts can get rewarded on finding bugs on companies like Tesla and Snapchat. Yes that's right you get paid if you can hack Tesla or Snapchat but be careful to read what's in Scope. This challenge introduces the platform to practice and also get started on the first challenge which shows the source code can reveal vulnerabilities and valuable information on a website

Getting paid for hacking, who would've taught this is where we'd be today? It's great isn't it.  
This flag follows this link and sign up:  
<https://ctf.hacker101.com/ctf>  
There's 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{TheNumbersBetweenTheFlagWords}`

Flag

Submit

2. By clicking the link, click login/sign up and the following will be shown below. If you don't already have an account to HackerOne, highly recommend creating one as this can benefit you in the future if you wish to learn more about web application hacking. So sign up and login to get access to the challenges.

Sign in to HackerOne

Email address

Using SAML? Email address only, no password needed.

Password

72

☐ Remember me for 2 weeks

[Forgot your password?](#)

Sign in

[Create a HackerOne account.](#)

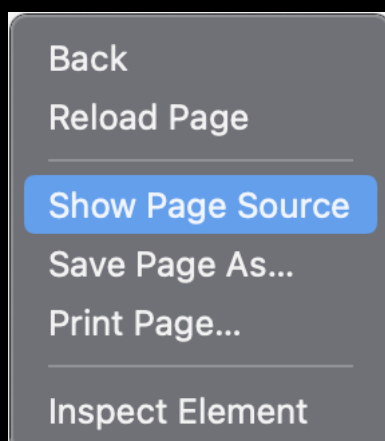
3. The challenge to this flag is the very first challenge and as you can see the name is the same name as the one in the challenge description. Click the go button and wait for the page to load.

Difficulty (Points)	Name	Skills	Completion	
Trivial (1 / flag)	A little something to get you started	Web	1 / 1	<a href="#">Go</a> <a href="#">Hints</a>   <a href="#">Restart</a>

3. The page will look like the page below. Nothing to interesting on the page.

Welcome to level 0. Enjoy your stay.

3. Right Click on your mouse and click on the option Show Page Source.



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}

Challenge

0 Solves

×

## 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 enthusiasts can get rewarded on finding bugs on companies like Tesla and Snapchat. Yes that's right you get paid if you can hack Tesla or Snapchat but be careful to read what's in Scope. This challenge introduces the platform to practice and also get started on the first challenge which shows the source code can reveal vulnerabilities and valuable information on a website

Getting paid for hacking, who would've taught this is where we'd be today? It's great isn't it.

This flag follows this link and sign up:  
<https://ctf.hacker101.com/ctf>

There's 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{TheNumbersBetweenTheFlagWords}

d731b22dc908a3ec2331b6efd1b1c61

Submit