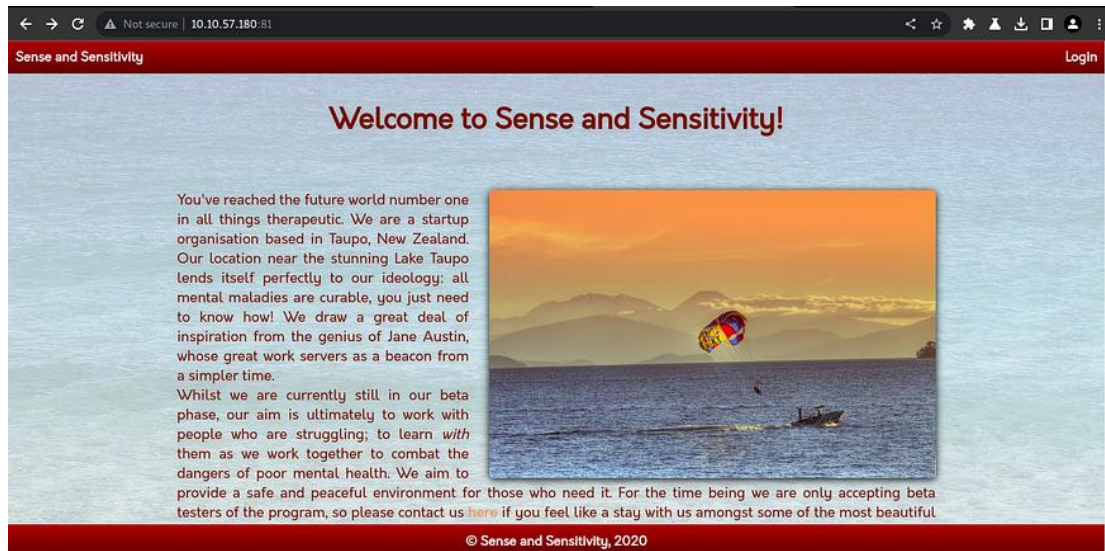


Task 8 : Cryptographic Failures (Challenge)

It's now time to put what you've learnt into practice! For this challenge, connect to the web application at <http://machine-ip:81/>.



Go to login page and view the source code to find the hidden directory.

```

1  <!DOCTYPE html>
2  <html>
3    <head>
4      <title>Login</title>
5      <meta name="viewport" content="width=device-width, user-scalable=no">
6      <meta charset="utf-8">
7      <link rel="shortcut icon" type="image/x-icon" href=" ../favicon.ico">
8      <link type="text/css" rel="stylesheet" href="assets/css/style.css">
9      <link type="text/css" rel="stylesheet" href="assets/css/loginStyle.css">
10     <link type="text/css" rel="stylesheet" href="assets/css/orkney.css">
11     <link type="text/css" rel="stylesheet" href="assets/css/icons.css">
12     <script src="assets/js/jquery-3.5.1.min.js"></script>
13   </head>
14   <body>
15     <header>
16       <a id="home" href="/">Sense and Sensitivity</a>
17       <a id="login" href="/login.php">Login</a>
18     </header>
19     <div class="background"></div>
20     <!-- Must remember to do something better with the database than store it in /assets... -->
21     <main>
22       <div class="content">
23         <form method="POST">
24           <input type="text" name="user" placeholder="Username"><br>
25           <input type="password" name="pass" placeholder="Password"><br>
26           <input id="loginBtnFunc" type="submit" value="Login!">
27         </form>
28       </div>
29     </main>
30     <footer><span>&copy; Sense and Sensitivity, 2022</span></footer>
31   </body>
32 </html>
33
34
```

Index of /assets

- [Parent Directory](#)
- [css/](#)
- [fonts/](#)
- [images/](#)
- [js/](#)
- [webapp.db](#)

Apache/2.4.54 (Unix) Server at 10.10.57.180 Port 81

Download the webapp.db to examine it

```
[lordofficial@parrot]~  
$sqlite3 webapp.db  
SQLite version 3.34.1 2021-01-20 14:10:07  
Enter ".help" for usage hints.  
sqlite> .tables  
sessions users  
sqlite> SELECT * FROM users;  
4413096d9c933359b898b6202288a650|admin|6eea9b7ef19179a06954edd0f6c05ceb|1  
23023b67a32488588db1e28579ced7ec|Bob|ad0234829205b9033196ba818f7a872b|1  
4e8423b514eef575394ff78caed3254d|Alice|268b38ca7b84f44fa0a6cdc86e6301e0|0  
sqlite>
```

CrackStation Password Hashing Security Defuse Security

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

6eea9b7ef19179a06954edd0f6c05ceb

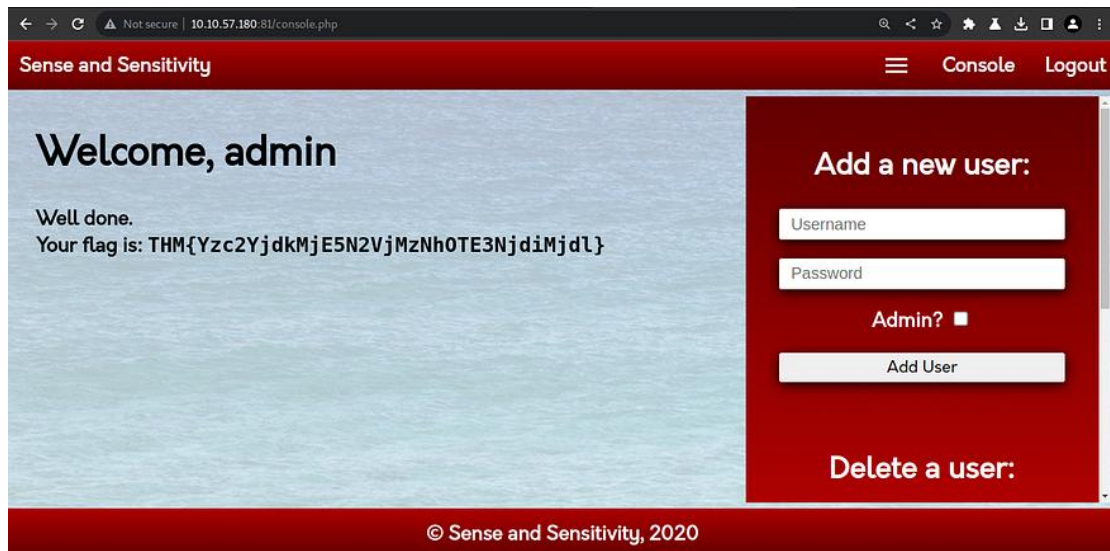
☐ I'm not a robot 
reCAPTCHA
Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-ha1f, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
6eea9b7ef19179a06954edd0f6c05ceb	md5	qwertyuiop

After Cracking the hash Now login as admin to get the flag.



Answer the questions below :

Have a look around the web app. The developer has left themselves a note indicating that there is sensitive data in a specific directory.

1. What is the name of the mentioned directory?

A. /assets

2. Navigate to the directory you found in question one. What file stands out as being likely to contain sensitive data?

A. webapp.db

3. Use the supporting material to access the sensitive data. What is the password hash of the admin user?

A. 6eea9b7ef19179a06954edd0f6c05ceb

4. Crack the hash.

What is the admin's plaintext password?

A. qwertyuiop

5. Log in as the admin. What is the flag?

A. THM{Yzc2YjdkMjE5N2VjMzNh0TE3NjdiMjdl}