E.1.

Start Wireshark and open the provided file. Filter the messages in the query box using `frame contains "CS2107{"`.

E.2.

Run John the Ripper with the supplied file, which will output the password. `john --users=bob --format=crypt shadow.txt`

E.3.

There is a `/admin.html` route that was commented off in the HTML file. Follow that route to find the flag.

E.4.

Run nmap to scan for open TCP ports, then `nc` into the open port.

E.5.

The flag is in the application cookies storage of the browser.

M.3.

A `long` data type is 8 bytes long. The integer 31337 is then represented as `b'x69\x7A\x00\x00\x00\x00\x00\x00'` in hexadecimal. Supply a sequence of random 40 bytes to the input followed by the hexadecimal integer representation of 31337 to overflow the buffer and write into the `coolness` variable. `cat flag.txt` to reveal the flag.

M.4.

Just follow the instructions on the website.

H.2.

Upon inspection of the code, there's a `match_url_from_msg` function that is called by `send_msg`, which causes the recipient of the message to follow the url within the `<a></a>` tag. Craft a HTTP GET request such that the admin will send a message to me, i.e.: `<a>http://web:2776/message=helloworld&to_user_id=[my user id]</a>`, then send the payload as a message to admin. Check the "My Messages" tab for the flag.