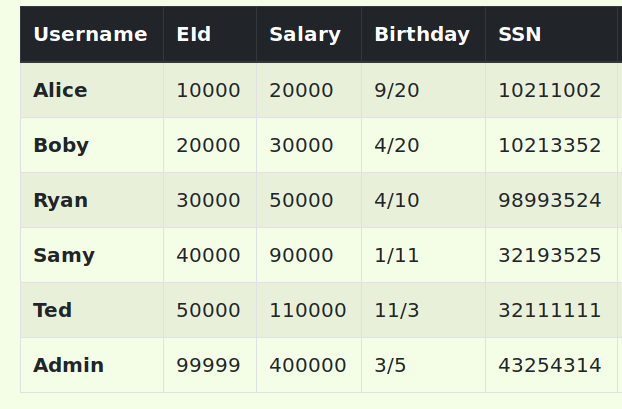
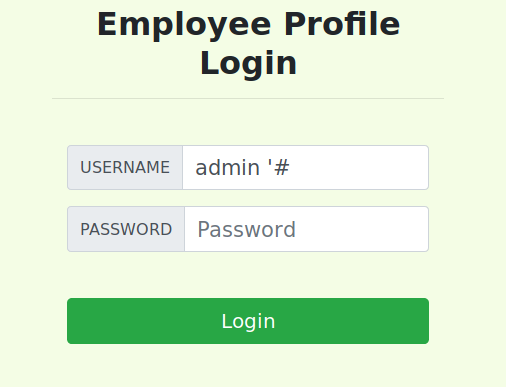
**TASK:**

1. 
2. cookie of boby received from samy’s profile
3. In task 1, I was able to log into the admin account with no knowledge of the admin password and with SQL I was able to get in and see all of the other EID, SSN, salary and other information. If this is allowed and can be exploited, the information of the employees at the company/ on the site are at risk and the safety of the user is also at risk.

Prevention: Always sanitize any input and making sure that the application never uses the input directly. This will prevent a user from getting in without knowing the proper credentials.

In task 2: I was able to get the cookie from boby’s action of clicking on samy’s profile. I would only need one account to start gaining access to other accounts such as boby’s and because I could insert the script in a place where others would click, the safety of the others on the site are compromised and the site is not to be trusted.

Prevention: Do not insert untrusted data except in allowed places, always HTML encode before inserting untrusted code into HTML element, encoding ‘ and “ is one way.