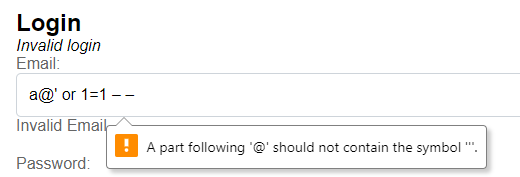
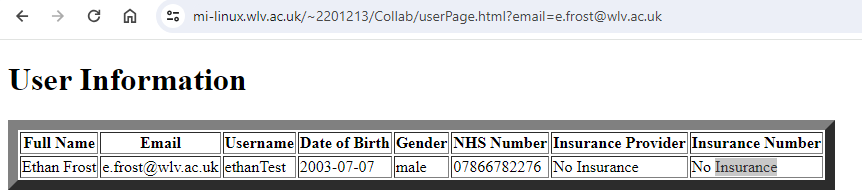
Testing: <https://mi-linux.wlv.ac.uk/~2201213/Collab/>

Results I have gained in testing the security of the website “Silver Sage Support”  
  
**Element Inspect:** after inspecting the elements of the login and register page, as well as the page of a user logged in there is no glaring vulnerability to exploit

**Login attempt (no known credentials):** not knowing the credentials prevents us from accessing the website or the sensitive information of users, the inspect terminal does not also bring up information or cookies transferring at this point

**Login attempt (known credentials):** after logging in we are presented with our own information that a user would give upon registering an account, using element inspect also revealed   
  
**Cyber Attack (SQL injection):** I attempted an SQL injection attack, and as shown below the website has precautions in place to prevent an SQL injection granting an attacker access to site, as apostrophes are not allowed to exist alongside an @ sign which is required to even make a login attempt, so it is safe to say the website is protected from attacks of this nature

  
  
**Cyber Attack (URL injection):** This is a large issue with the website. This is because you can access a page that contains an individual’s date of birth, NHS number, and their insurance provider + number by simply knowing their email and entering it into the search bar (example shown below). As such an attacker could attempt to brute force to guess the emails of website users, or perform footprinting on known users of the website to try and gain knowledge of their email in order to very easily gain access to this sensitive information.



**Fixes to implement:** the URL injection is the most glaring issue with the Silver Sage Support website, the URL of the page with user information should not contain the email of the user in future versions of the website to avoid this easily exploitable weakness. As the website stands now there are no other fixes that need to be implemented as there are no other large security risks.