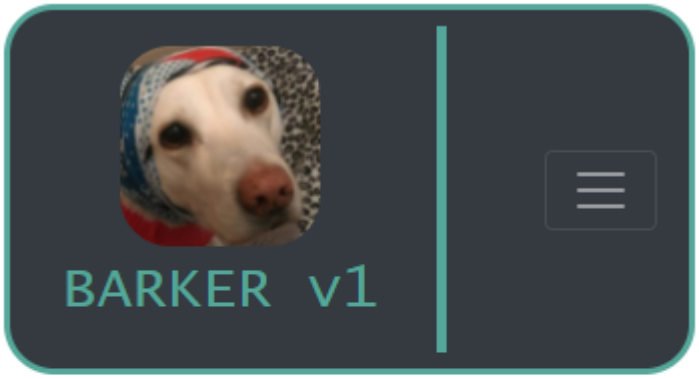
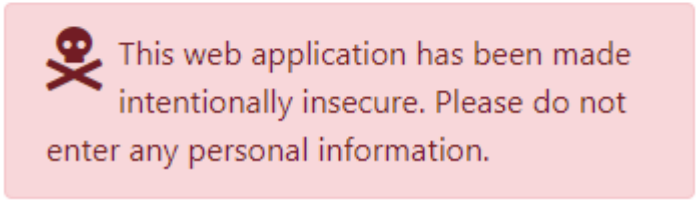
- **What happens if I try login with myemail%00@email.com** - does it recognise it as myemail@email.com and maybe log me in? If yes, try signup with my%00email@email.com and try for an account takeover. Think about the same when claiming a username too.

- **Can I login with my social media account?** If **yes**, is this implemented via some type of Oauth flow which contains tokens which I may be able to leak? What social media accounts are allowed? Is it the same for all countries? This would typically be related to the registration process however not always. Sometimes you can only login via social media and NOT register, and you connect it once logged in. (Which would be another process to test in itself!)



- **How does the mobile login flow differ from desktop?** Remember, user experience! Mobile websites are designed for the user to have the easiest flow as they don't have a mouse to easily navigate. "*Do you guys not have phones?*" - Blizzcon 2018



- **When resetting your password what parameters are used?** Perhaps it will be vulnerable to IDOR (try injecting an id parameter and testing for HPP!). Is the host header trusted? Imagine when resetting password you set the host to: Host: evil.com, will it then trust this value & send it in the email, leading to reset password token leak when the user clicks on the link (leading to evil.com/resetpassword?token=123)

Typically you can test the login/register/reset password for rate limiting (brute force attack) but often this is considered **informative/out of scope** so I don't usually