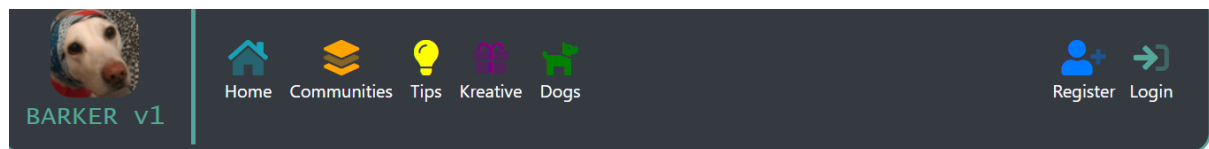



on signup to play with and could keep you busy for a few hours already. So let's break it down and figure out what we should be looking for.




 This web application has been made intentionally insecure. Please do not enter any personal information.

Register a new account

Basic account details

Appearance

Profile Picture



Display Name

Description

Uploading a photo: I mentioned above, we want to determine what type of files we can upload so we upload a normal jpeg image but change the extension to **.txt** **.xml** and **.svg** to see how it's handled. Now, this may depend on how the web application works but you may not see where your photo is uploaded until **after** you complete the registration process. Now can you see why re-testing features **multiple times** comes into action? (I mention more on this below).

Display name and profile description: Again these may not be seen until after you complete the signup process, but where are they reflected and what characters are allowed? Not only that but consider **where** this information is used. Imagine you can get < > through but it's not vulnerable when viewing your profile on desktop, but what about mobile apps, or what about when interacting with the site (making a post, adding someone). Did the developers only prevent XSS on your profile?

- **Can I register 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? What information do they trust from my social