interesting behaviour from these basic tests. I always go in with the assumption that the website **will be** secure & it should be working as intended.

Get your notepad out because this is where the notes start. As I'm hunting I mentioned I will regularly write down interesting behavior and endpoints to come back to after my first look. The word list is created from day one. How many custom wordlists do you have? More than 0 I hope. **Build a treasure map of your target**!

When testing a feature such as the register & login process I have a constant flow of questions going through my head, for example, can I login with my social media account? Is it the same on the mobile application? If I try another geolocation can I login with more options, such as WeChat (usually for china users). What characters aren't allowed? **I let my thoughts naturally go down the rabbit hole because that's what makes you a natural hacker.** What inputs can you control when you sign up? Where are these reflected? Again, does the mobile signup use a different codebase? I have found LOTS of stored XSS from simply signing up via the mobile app rather than desktop. No filtering done! **Have I ever mentioned that the possibilities to hacking are endless**?

Below is a list of key features I go for on my **first initial look** & questions I ask myself when looking for vulnerabilities in these areas. Follow this same approach and ask the same questions and you may very well end up with the same answer I get… a valid vulnerability!

Registration Process

- What's required to sign up? If there's a lot of information (Name, location, bio, etc), where is this then reflected after signup?

An example of this can be seen below when signing up for BARKER. It's asking you to input a **display name**, **profile description** and **upload a photo**. That's quite a lot