media profile? I once discovered stored XSS via importing my facebook album conveniently named “<script>alert(0)</script>”.

- **What characters are allowed? Is <> “ ' allowed in my name?** (*at this stage, enter the XSS process testing. <script>Test may not work but <script does.*) What about unicode, %00, %0d. How will it react to me providing myemail%00@email.com? It may read it as myemail@email.com. Is it the same when signing up with their mobile app?

- **Can I sign up using @target.com or is it blacklisted?** If **yes** to being blacklisted, question *why*? Perhaps it has special privileges/features after signing up? Can you bypass this? Always sign up using your targets email address.

- **What happens if I revisit the register page after signing up?** Does it redirect, and can I control this with a parameter? (*Most likely yes!*) What happens if I re-sign up as an authenticated user? Think about it from a developers’ perspective: they want the user to have a good experience so revisiting the register page when authenticated should redirect you. Enter the need for parameters to control where to redirect the user!

- **What parameters are used on this endpoint?** Any listed in the source or javascript? Is it the same for every language type as well device? (Desktop vs mobile)

- **If applicable, what do the .js files do on this page?** Perhaps the login page has a specific “login.js” file which contains more URLs. **This also may give you an indication that the site relies on a .js file for each feature**! I have a video on hunting in .js files on YouTube which you can find here: Let’s be a dork and read .js files (https://www.youtube.com/watch?v=0jM8dDVifaI)