then expanding your attack surface as time goes on, **you realise you can continuously** switch between 5-6 wide-scoped programs and always have something to play with. (*Bigger the company the better, more likely to release changes more frequently!*). Make bug bounties work for you.

Two common things I suggest you look into automating which will help you with hunting and help create more time for you to do hands on hacking:

- **Scanning for subdomains, files, directories & leaks**
You should look to automate the entire process of scanning for subdomains, files, directories and even leaks on sites such as GitHub. Hunting for these manually is time consuming and your time is better spent hands on hacking. You can use a service such as CertSpotter by SSLMate to keep up to date with new HTTPS certificates a company is creating and @NahamSec released LazyRecon to help automate your recon: https://github.com/nahamsec/lazyrecon.

- **Changes on a website**
Map out how a website works and then look to continuously check for any new functionality & features. Websites change all the time so staying up to date can help you stay ahead of the competition. Don't forget to also include .js files in those daily scans as they typically contain new code first before the feature goes live. At which point you can then think, "well, the code is here, but I don't see the feature enabled", and then you've started a new line of questioning that you may not have thought of, can you enable this feature somehow? (true/false?!)

As well as the above I recommend **staying up to date with new programs & program updates.** You can follow https://twitter.com/disclosedh1 to receive updates on new programs being launched and you can subscribe to receive program updates via their policy page. Programs will regularly introduce new scopes via Updates and when there's new functionality, there are new bugs.
