on their main web application and finding issues & then expanding my attack surface as I scan for subdomains, files and directories. I can spend months going through features with a comb getting into the developers' head and the end result is a complete mind-map of this company and how everything works. Don’t rush the process, trust it.

Below is a good checklist for how to determine if you are participating in a well run bug bounty program.

- Does the team communicate directly with you or do they rely on the platform 100%? Being able to engage and communicate with the team results in a much better experience. If the program is using a managed service then make sure to proceed with caution.

- Does the program look active? When was the scope last updated? (usually you can check the “Updates” tab on bug bounty platforms).

- How does the team handle low hanging fruit bugs which are chained to create more impact? Does the team simply reward each XSS as the same, or do they recognise your work and reward more? This is where your risk vs reward will come into play. Some programs will pay the same for XSS and others will pay if you show impact. Sadly it’s the wild wild west but this is where I mentioned earlier, **get comfortable being in the driver's seat and making bug bounties work for you**, the results producer. **Don’t be afraid to walk away from bad experiences**.

- Response time across ~3-5 reports. If you are still waiting for a response **3 months+** after reporting then consider if it’s worth spending more time on this program. More than likely no.