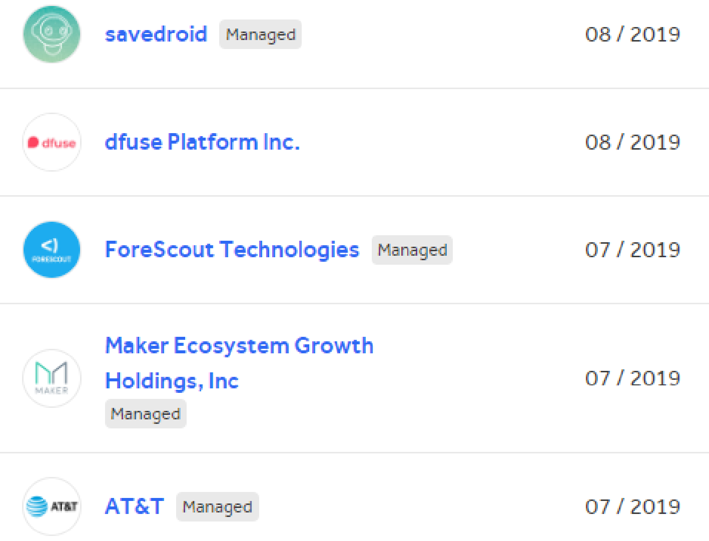
typically **choose wide scope** and **well known names**, it doesn't matter if it's private or public. From experience I know that the bigger a company the more teams they'll have for different jobs which equals to a higher chance of mistakes being made. Mistakes we want to find. The more I know already about the company (if it’s a popular well-used website), the better also.

By different teams I mean teams for creating the mobile app for example. Perhaps the company has headquarters across the world and certain TLD's like .CN contain a different codebase. The bigger a presence a company has across the internet, the more there is poke at. Perhaps a certain team spun up a server and forgot about it, maybe they were testing third party software without setting it up correctly. The list goes on creating headaches for security teams but happiness for hackers.



savedroid Managed	08 / 2019
dfuse Platform Inc.	08 / 2019
ForeScout Technologies Managed	07 / 2019
Maker Ecosystem Growth Holdings, Inc Managed	07 / 2019
AT&T Managed	07 / 2019

There is no right or wrong answer to choosing a bug bounty program if I'm honest. Each hacker has a different experience with companies and there is no holy grail, “*Go hack on xyz, there are definitely bugs there!*”. Sadly it **doesn't** work like that. Some people have good experiences on xyz, and others have bad experiences. **Focus on YOU**. I pick programs based on the names I recognise, the scope and how much there is to play with on the web application. If the first few reports go well then I will continue. My methodology is all about using the features available to me