Another thing you can do with your notes is begin to **create custom wordlists**. Let's imagine we are testing "example.com" and we've discovered /admin /admin-new and /server_health, along with the parameters "debug" and "isTrue". We can create examplecom-endpoints.txt & params.txt so we know these endpoints work on the specific domain, and from there you can test ALL endpoints/parameters across multiple domains and create a "global-endpoints.txt" and begin create commonly found endpoints. Over time you will end up with lots of endpoints/parameters for specific domains and you will begin to map out a web application much easier.

Let's apply my methodology & hack!

Step One: Getting a feel for things

So as I mentioned before my intentions when choosing a bug bounty program is wanting to spend up to six months learning and poking at their in-scope domains & their functionality with the intention of wanting to dive as deep as possible overtime. With lots to play with it helps you learn quicker about common mistakes the program may be making. With that said, before I even open a program's in-scope domain I want to know something.

Has anyone else found anything and disclosed a writeup?

Remember I mentioned I want to be able to **create a lead** for myself and a starting point. **Before even hacking** I will search Google, HackerOne disclosed and