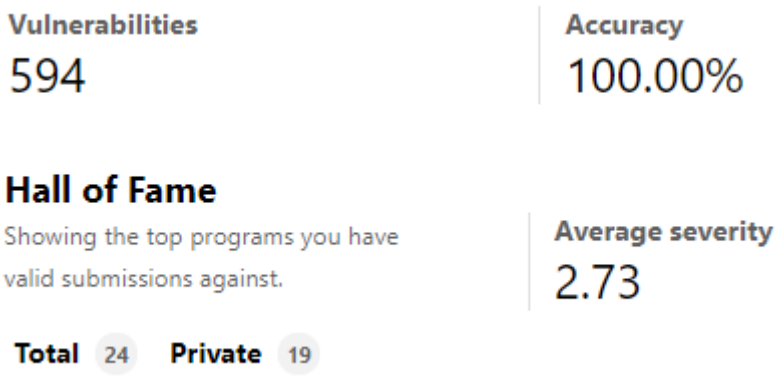
Time to automate! Step Three: Rinse & Repeat

At this point I would have spent months and months on the same program and should have a complete mental mind map about the target including all of my notes I wrote along the way. This will include all interesting functionality available, interesting subdomains, vulnerable parameters, bypasses used, bugs found. Over time this creates a **complete understanding** of their security as well as a starting point for me to jump into their program as I please. Welcome to the “bughunter” lifestyle. **This does not happen in days, so please be patient with the process.**



The last step is simply rinse & repeat. Keep a mental note of the fact developers are continuing to push new code daily and the same mistakes made 10 years ago are still being made today. Keep running tools to check for new changes, continue to play with interesting endpoints you listed in your notes, keep dorking, test new features as they come out, but most importantly you can now **start applying this methodology on another** program. Once you get your head around the fact that my methodology is all about just simply testing features in front of you, reverse engineering the developers' thoughts with any filters & how things were setup and