

“responsible disclosure program”

“vulnerability disclosure program”

“vulnerability program rewards”

“bugbounty reward program”

inurl: vulnerability disclosure

inurl: responsible disclosure

At the time of writing this bug bounty platform’s such as HackerOne will send “private” invites to researchers who regularly spend time on their platform and build “reputation”. A lot of researchers believe the most success is in these private invites but from experience a lot of the public-paying programs on platforms still contain bugs and some even pay more than privates! Yes, private invites are less-crowded, but don't rely on them. Should you spend time in a Vulnerability Disclosure Program (VDP)? In my opinion, yes, **but with limits**. I sometimes spend time in VDP's to practise and sharpen my skills because to **me** the end goal is about building relationships and becoming a better hacker (whilst helping secure the internet of course!). VDP's are a great way to practise new research, just **know your limits** and don't burn out giving companies a complete free test. Companies want our talent so even if they don't pay, show them you have the skills they want and should they “upgrade” their VDP to a paying-program, you may be at the top of their list to get invited. Perhaps there is some cool swag you want, or you just want a challenge on a sunday afternoon. Know your risk vs reward ratio when playing in VDP's.