**In recent times, bug bounties have gained considerable popularity and are considered as smart and reliable ways to test the vulnerabilities in your security code.**

**A recent survey by Veracode and Wakefield has concluded that businesses have become too reliant on bug bounties and don’t prefer the option of initial secure coding. However, 59% of respondents believed that the vulnerabilities discovered in bug bounty programs were costlier to fix as compared to secure coding during the development phase. As a result, 83% of survey respondents admitted to releasing the code without testing and subsequent fixing of bugs. Subsequently, many applications and software programs lack a proactive and layered security approach to battle security threats, despite the fact that their developers consider them to be secure.**

**The survey results also depict the insecurity of respondents in their code development process. About 44 percent of them were found to have expended more than one million dollars on bug bounties, even though 79% agreed upon lesser costs incurred in case of effective mobile application security testing program. Hence, one in every three of the respondents (approx. 36%) admitted to taking services from bug bounty programs.**

**Following the trend, tech giants like Apple and Google have also jumped into the bandwagon by announcing their personal programs. However, as much effective as these bug bounty programs are, we cannot deny the importance of mobile app security testing during the software development phase. Because these programs focus on those applications that are in use, they only expose risks encountered by users for months or years. Still, 77% professionals admitted to relying on such programs, even though 93% of them believed that majority of flaws discovered by these bug bounty programs could actually have been avoided during the development phase with mobile app security testing.**

**These survey results are a clear indication that businesses need help from security experts in devising their security strategies and securing software during the software development process.**