



Bug Bounty Program

The crowdsourcing solution for information security

What is bug bounty?

버그바운티 프로그램이란, 여러 해커들에게 취약점 진단을 참여시켜 취약점을 발견하면 보상금을 주는 제도로, 집단 지성을 통해 보안 취약점 문제를 해결하는 솔루션입니다. 기존의 방식보다 훨씬 다양하고 많은 배경의 해커들이 취약점 진단에 참여하기 때문에 잠재적으로 발생할 수 있는 취약점에 대한 커버 범위가 매우 넓습니다. hackerone에 따르면, 전통적인 취약점과 비교하였을 때 동일비용으로 6배 많은 취약점이 발견된다고 합니다. 그리고 케이스의 77%에서 24시간 내에 첫번째 취약점이 발견된다고 합니다. 이와 같은 결과로 볼 때, 6개월이나 1년 단위로 수행하는 전통적인 취약점 진단 방식과 달리 버그바운티는 지속적으로 취약점을 제보 받을 수 있는 창구가 마련되기 때문에 패치가 빈번한 현대적인 애플리케이션 서비스의 보안 취약점 발생을 방지하는 데에 훨씬 더 유용한 모델입니다.

google과 microsoft, tencent, facebook과 같은 테크 기업들 뿐만 아니라 airbnb, starbucks도 이미 버그바운티를 진행하고 있습니다. 국내의 경우에는 네이버, 삼성과 같은 기업들, 그리고 리디북스와 같은 비교적 작은 기업들도 점차 버그바운티를 도입하고 있는 추세입니다.



버그바운티를 수행하고 있는 해외 기업들

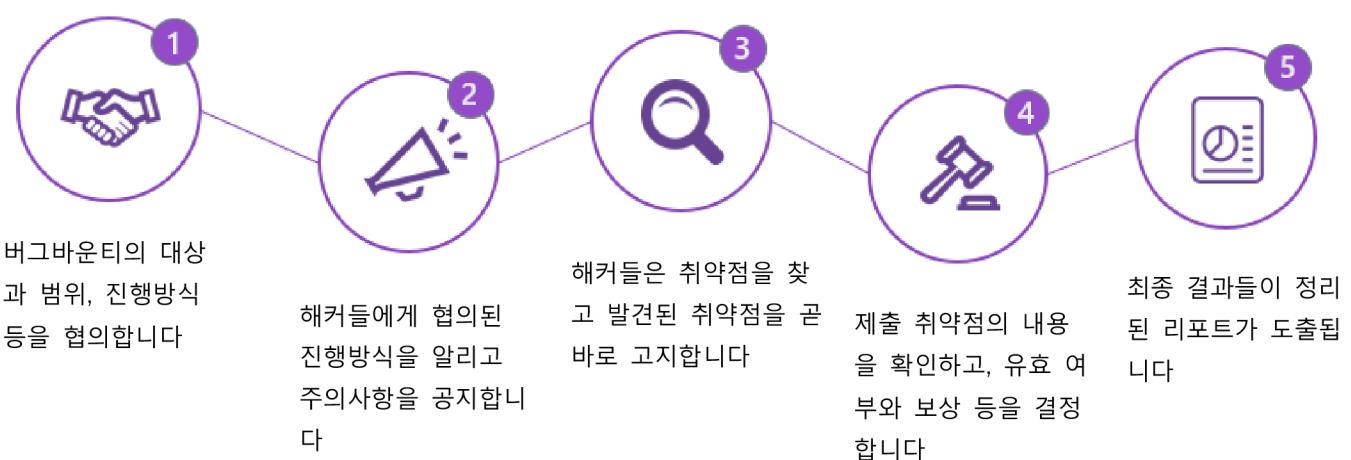
How to do?

규모가 큰 테크기업들은 충분한 보안 인력을 이미 고용하고 있기 때문에 자체적인 버그바운티를 수행하는 데에 큰 어려움이 없습니다. 그러나 모든 기업이 충분한 보안 인력을 확보하고 있는 것이 아니기 때문에 버그바운티 운영에 어려움이 있습니다. 그렇기 때문에 starbucks와 airbnb와 같은 경우, 다른 기업의 도움을 받아서 버그바운티를 운영하고 있습니다. 이처럼 저희 또한 버그바운티 운영을 원하는 기업을 위하여 다양한 형태의 프로그램을 제공하고 있습니다.

Public bug bounty란 서비스에 접근 가능한 모든 이용자가 취약점 진단에 참여할 수 있는 프로그램을 말합니다. 이와 같은 형태가 가장 버그바운티의 이점을 잘 살릴 수 있는 버그바운티의 형태이며, 많은 참여자들이 넓은 커버 범위를 다양하게 진단하기 때문에, 실제의 공격 방식과 유사하므로 발생할 수 있는 취약점을 아주 잘 찾아낼 수 있습니다.

Private bug Bounty란 일반 대중에게 공개하지 않고 진행하는 버그바운티를 말합니다. 여기서 진단에 참여하는 인력은 숙련도나 참여 이력 등으로 일정부분 필터링하여 참가시킵니다. Public 방식은 이미 오랜 세월 검증되어 문제가 없지만, 그럼에도 불구하고 기업에서 우려하는 점들을 역시 간과할 수 없기 때문에, 민감한 부분에 대하여 다소 합의된 형태의 버그바운티라고 할 수 있습니다.

버그바운티 프로세스



Forget about old-fashioned pentest !

전통적인 취약점 진단은 현대적인 어플리케이션과 서비스들의 취약점을 찾아내는 데에 뚜렷한 한계점이 존재합니다. 대부분의 취약점 진단은 범용적인 체크리스트 방식으로 이루어지며, 수행 인원 또한 1~2명 정도의 소수로 수행되기 때문에 실제 해커들의 창의적이고 다양한 공격으로 발견되는 취약점들을 발견하지 못하는 경우가 많습니다. 반면 버그바운티는 보다 많은 해커들이 다양한 방식으로 진단을 수행하게 되어, 실제 공격으로 이어질 수 있는 취약점들이 잘 발견됩니다.

	Traditional Pentest	Bug Bounty Platform
수행 인원	주로 1~2명의 인원이 수행합니다	훨씬 더 많은 인원들이 다양한 방식으로 취약점을 찾습니다
조치 과정	진단 도중의 소통이 적고, 결과보고서 도출에 집중하여 진행됩니다	실시간으로 진단 결과들이 전달되고, 결과의 유효성을 판단합니다
발견 속도	약 6개월 ~ 1년 단위로 수행되어 다양한 패치로 발생할 수 있는 취약점을 빠르게 발견할 수 없습니다	지속적인 취약점 제보 창구가 마련되어 패치와 기능개선으로 발생하는 취약점을 빠른 시간 내에 제거할 수 있습니다
수행 시간	계약에 따라 업무시간이 결정됩니다	시간제약 없이 취약점 진단이 수행됩니다
비용	시간과 업무량에 비례하여 비용이 증가합니다	실제 취약점이 도출될 때만 비용이 증가합니다