ENKI

버그캠프 서비스 소개서

법률 자문 요청용

이재일 연구원
01041341638
jilee@enki.co.kr

2021.04.26

서비스 소개

본 서비스는 화이트해커 그룹과 정보자산을 보유한 기업을 연결하여 해킹 사고에 악용될 수 있는 **보안 취약점의 사전 발굴과 조치를 지원**하는 **크라우드 소싱 정보보안 문제 해결 플랫폼(버그바운티[1] 플랫폼)**이며, 이름은 버그캠프입니다.

플랫폼 참여자들(**웹·앱 서비스, IT 인프라를 보유한 기업 및 기관(파트너)**과 **국내외 화이트 해커(보안기술전문가)**)은 손쉽게 숨겨진 보안 문제를 확인하고, 관리할 수 있습니다. 또한, 해커와 소통하며 상세 침투 경로와 취약점의 근본 원인을 확인할 수 있습니다.

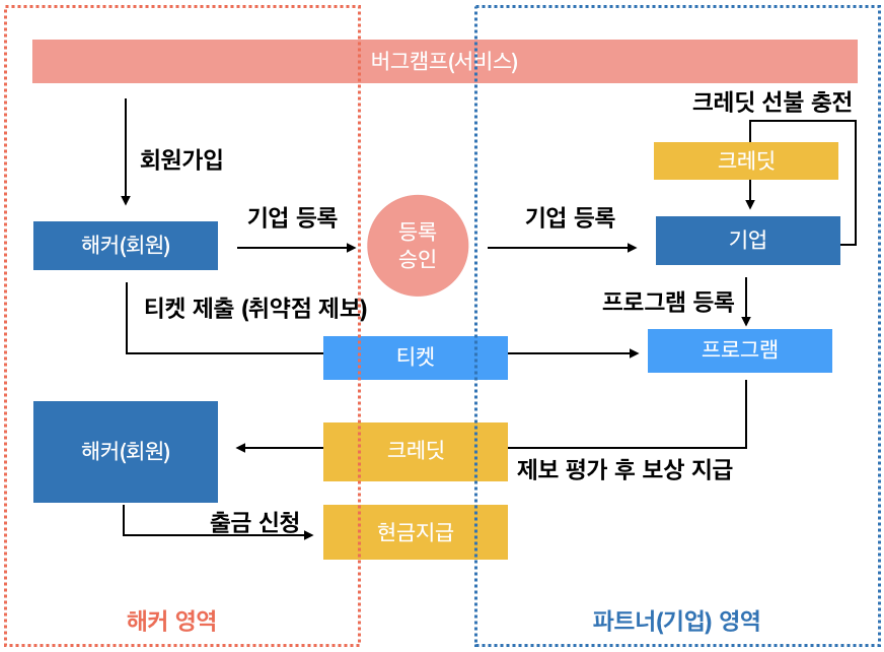
해외의 버그바운티 플랫폼은 이미 성공적인 비즈니스 모델로 정착하였으며, 글로벌 보안 생태계의 변화를 선도하고 있습니다.

- '20 년 2 월 기준, 해커원(Hackerone)은 170 개 국가, 1,700 개의 기관 및 기업에서 전 세계 약 60 만명의 해커를 통해 누적 15 만건의 유효 취약점을 처리하고, 2,500 만 달러 이상의 매출을 발생시켰습니다.
- 버그크라우드(Bugcrowd)는 크라우드 소싱 사이버 보안(Crowdsourced Cybersecurity) 플랫폼을 표방하며 사이버 해킹 공격을 막기 위한 "집단지성"의 힘을 강조하며 각종 통계 및 정기 리포트를 통해 **버그바운티 플랫폼의 효과성을 입증하였습니다.**

(마지막 장 'reference' 란에 국내외 버그바운티 운영사 및 버그바운티 플랫폼 링크를 첨부해 두었습니다. 해외 버그바운티 플랫폼과 서비스의 형태가 매우 유사하니 참고 부탁드립니다.)

[1] 버그바운티란 (https://www.bugbountyclub.com/beginning, https://www.itworld.co.kr/news/110223)

주요 기능



- 회원가입 및 로그인 (외 통상적인 웹서비스에서 제공하는 회원 관련 기능)
  '버그캠프' 서비스를 이용하기 위해서 사용자의 "이메일" 식별자로 회원가입을 해야 합니다. 회원은 '해커' 회원과 '파트너(기업)' 회원으로 나뉘며, 기업에 소속된 '해커' 회원을 '파트너' 회원으로 취급하여, 서비스 내 '파트너 영역' 의 기능을 추가로 이용할 수 있습니다.

- 기업
  버그바운티 프로그램 게시의 주체이자, 1명 이상의 회원이 소속될 수 있는 집단입니다.
  서비스에 가입한 회원은 기업 등록을 신청할 수 있고, 서비스 운영진에 의해 기업 등록이 승인된 경우 프로그램을 게시할 수 있습니다. 또, 기업은 결제 수단을 통해 서비스 내 화폐 단위인 "크레딧" 을 선불 충전할 수 있습니다.

- "프로그램" 을 통한 버그바운티 게시
  "프로그램"은 '기업'이 등록 및 관리하며, 이를 통해 자사의 에셋을 대상으로 한 취약점 점검 허용 범위 및 정책을 게시할 수 있습니다. 해커 회원은 프로그램을 통해 기업에게 보안 취약점 보고서를 제출(티켓 제출)할 수 있습니다.

- 티켓 제출 (보안 취약점 제보)
  회원은 버그캠프에 등록된 "프로그램"이 규정하는 범위 내에서 기업이 등록한 에셋(웹, 앱 또는 정보 인프라)을 대상으로 보안 취약점 발견을 위한 공격을 시도할 수 있습니다.
  이 과정에서 발견한 보안 취약점을 "티켓"의 형태로 기업에 제보할 수 있습니다.
  기업은 접수된 "티켓"을 분석, 평가 및 (티켓을 제출한) 해커 회원과 커뮤니케이션 할 수 있습니다. 접수된 모든 티켓의 지적 재산권은 "버그캠프"에 귀속됩니다.

- 크레딧
  서비스 내에서 대금 지급이 필요한 때(서비스 내 유료 컨텐츠, 유효한 보안 취약점을 제보한 해커 회원에게 보상 지급 등)에 사용할 수 있습니다. 기업은 서비스가 제공하는 결제 수단을 통해 크레딧을 충전할 수 있습니다. 해커는 "출금 신청" 을 통해 크레딧을 현금으로 지급받을 수 있습니다.

중점적으로 고려해야 하는 부분

- □ 서비스 특성(버그바운티 참여가 곧 기업의 정보 자산 침해를 시도하는 행위임) 상 국내 정보통신망법 등을 침해할 우려가 다분하여, "버그캠프"의 책임과 역할이 참여 기업과 국내외 화이트 해커를 연결해 주는 플랫폼임을 명확히 하고, 두 참여자 간에 발생하는 불의의 사고에 대한 면책 사항을 견고히 검토 부탁드립니다.
- □ 서비스를 운영하면서 누적되는 데이터를 이용한 2차적인 산출물 활용을 기대하고 있는 바, 서비스를 통해 제출된 티켓(보안 취약점 제보)의 지적 재산권이 "버그캠프"에 귀속됨을 명확히 할 수 있는 방안을 검토 부탁드립니다.
- □ 당사의 매출매입 구조가 기업에서 "크레딧"을 선불 충전(자사 매출)하고, 취약점 제보 과정에서 해커 회원에게 지급된 "크레딧"을 현금 지급(자사 매입) 하는 형태인 바, 이 과정의 설명이 약관에 포함되도록 검토 부탁드립니다.

[용어정리]

- 버그캠프: 엔키에서 제공하는 서비스의 이름이며, 파트너는 프로그램을 버그캠프에 게시하고, 해커 회원은 파트너가 등록한 프로그램의 보안 취약점을 보고할 수 있는 플랫폼을 의미합니다.
- 해커: 서비스에 가입한 자로서 버그캠프에 있는 프로그램의 보안 취약점을 찾아 보고하고 바운티 보상을 받는 개인을 의미합니다.
- 파트너: 기업 서비스에 참여 및 계약한 기업에 소속된 회원으로서, 프로그램을 게시/운영하고, 티켓을 평가해 해커에게 보상을 지급할 수 있습니다.
- 버그바운티: "버그캠프" 에서 파트너가 게시한 제품의 보안 취약점을 해커 회원이 발견하여 티켓을 제출하면 유효 여부 및 보상 지급 기준에 따라 보상을 지급하는 제도를 의미합니다.
- 에셋: "파트너"가 소유한 웹, 앱, 정보인프라, 하드웨어 등을 식별하기 위해 "버그캠프"에 등록하는 자산 개념입니다.
- 프로그램: 파트너가 "에셋"으로 등록한 제품(들)의 버그바운티 정책을 게시하고, 해커가 프로그램에 게시된 정책을 확인할 수 있는 공간입니다.
- 티켓: 해커가 보안 취약점 제보를 제출하면 생성되는 "버그바운티" 행위의 단위이자, 제보별로 해커와 파트너가 소통하는 온라인 상 공간입니다.

[reference]

해외

해커원(https://www.hackerone.com/product/bug-bounty-program)

버그크라우드(https://www.bugcrowd.com/products/bug-bounty/)

국내

KISA 취약점신고포상제(https://www.krcert.or.kr/consult/software/vulnerability.do)

네이버 버그바운티(https://bugbounty.naver.com/ko/)