

버그바운티 도입 및 운영 101

홍성진

2025-04-29

LET'S START A BUG BOUNTY PROGRAM 🐛

홍성진 aka. nisam

- 샌드버드 Staff Security Engineer
- 前 네이버 Security Engineer
- AWS 한국 사용자모임 보안 소모임 운영진
- 비오비 4기 수료

#AppSec #DevSecOps #ThreatModeling
#BugBounty #CloudSec #SecureCoding
#☕ #🎾 #🏆



오늘 다루지 않을것

- 정보통신방법을 포함한 법령
- 플랫폼 소개
- 플랫폼 비용
- 회사 기밀

목차

1. 버그바운티란?
2. 버그바운티 목적
3. 버그바운티 장단점
4. 버그바운티 참여자 통계
5. 버그바운티 도입 프로세스
6. 자주 만나는 문제점
7. 요약

버그바운티란?

버그 바운티는 소프트웨어, 웹사이트 또는 시스템의 취약점이나 버그를 발견하고 신고한 윤리적 해커에게 기업이 금전적 보상을 제공하는 **클라우드 소싱** 제도입니다.





Get a bug if you find a bug.

Show us a bug in our VRTX® real-time operating system and we'll return the favor. With a bug of your own to show off in your driveway.

There's a catch, though.

Since VRTX is the only microprocessor operating system completely sealed in silicon, finding a bug won't be easy.

Because along with task management and communication, memory management, and character I/O, VRTX contains over 100,000 man-hours of design and testing.

And since it's delivered in 4K bytes of ROM, VRTX will perform for

you the way it's performing in hundreds of real-time applications from avionics to video games.

Bug free.


So, to save up to 12 months of development time, and maybe save a loveable little car from the junkyard, contact us. Call (415) 326-2950, or write Hunter & Ready, Inc., 445 Sherman Avenue, Palo Alto, California 94306.

Describe your application and the microprocessors you're using—Z8000, Z80, 68000, or 8086 family. We'll send you a VRTX evaluation package, including timings for system

calls and interrupts. And when you order a VRTX system for your application, we'll include instructions for reporting errors.*

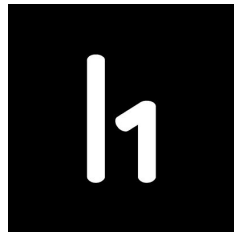
But don't feel bad if in a year from now there isn't a bug in your driveway.

There isn't one in your operating system either.

**HUNTER
♦ READY** 
VRTX
Operating Systems in Silicon.

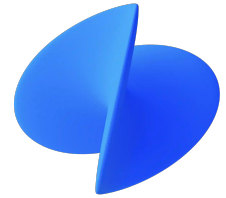
*Call or write for details. But, considering our taste in cars, you might want to accept our offer of \$1,000 cash instead. © 1983 Hunter & Ready, Inc.

f a  N G



THE GREAT BUG OUNTY ERA





버그바운티 목적

투자 대비 더 많은 보안 이점 확보하기 위함.





버그바운티 장점

- 비용
- 지속성
- 다양성
- 사회 기여
- 홍보
- 인재 유치
- 보험료 감소

버그바운티 단점

- 내부 리소스 증가
- 난이도 높은 취약점 상대적 부재
- 서비스 가용성 침해
- 법적·제도적 문제
- 평판




버그바운티 참여자 통계

Top 10 Countries Where Participating Hackers Live

 India

 Egypt

 Bangladesh

 Nigeria

 USA

 UK

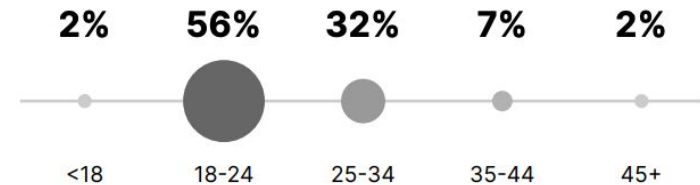
 Pakistan

 Vietnam

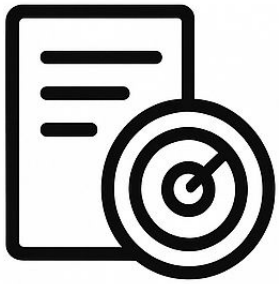
 Nepal

 Australia

Average Age



버그바운티 도입 프로세스



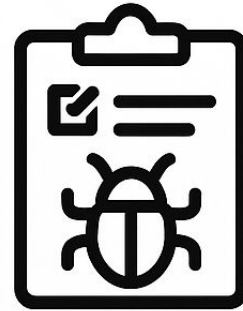
목표와 범위
확립



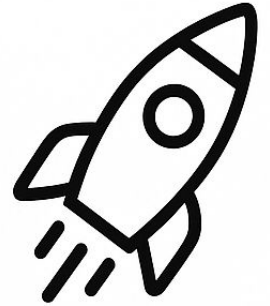
내부 자원
확보 및 동의



보상 구조 확립



취약점 처리
프로세스 설계



출시 및
홍보

목표와 범위 확립

- 조직의 버그바운티 목표
- 버그바운티 대상
- 제외할 취약점 종류
- 버그바운티 규칙 정의 - 테스트 계정, 헤더 등
- 운영 방식 - 이메일, 자체 플랫폼, 대행 플랫폼



내부 자원 확보 및 동의

- 버그바운티 운영에 필요한 예산 확보
- 내부 이해 관계자들의 동의
- 장애 대비 및 법적 문제 대비
- 취약점 공개 여부



보상 구조 확립

- 보상금 및 스웨그(Swag)
- 취약점 등급별 보상금
- 보상금 지급 프로세스
- 송금 프로세스 및 예상 소요 시간



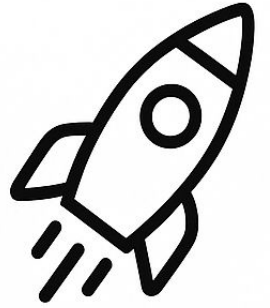
취약점 처리 프로세스 설계

- 버그바운티 처리 담당자 지정
- 버그바운티 런북
- 개발팀이 이해할 수 있는 문서로 변환
- 자동화
- 취약점 평가지 - 난이도, 위험도, 보고서 품질
- 답변지



출시 및 홍보

- 작게 시작하기 VS 크게 시작하기
- 출시전 내부 점검
- 홍보 - 국내/글로벌
- 효과 측정



자주 만나는 문제점

- 정보 비대칭성(투명성)
- 기대치 상이
- 송금 시간
- 취약점 공개 여부
- 온라인 비판
- 담당자도 사람이야
- 제보자도 고객이야





버그바운티
참... 좋다

요약

- 버그 바운티는 제보자에게 금전적 보상을 통해 기업의 보안성을 향상 시키는 제도입니다.
- 내부 팀 목표 명확화, 범위 설정, 보상 정책, 내부 처리 프로세스 등 철저한 내부 준비가 필요합니다.
- 확보된 예산 외에 내부에서 증가하는 리소스를 염두해야 합니다.
- 제보자와 담당자 둘다 만족할 수 있는 제도가 사전 준비되어야 합니다.

그림 출처

기업 로고를 제외한 장표의 모든 아이콘 및 그림은 dall·e (openai.com)로 생성되었습니다.

THANK YOU!

