



CONTENT



INTRODUCTION TO BUG BOUNTY

Bug Bounty programs are an increasingly popular way for companies to outsource vulnerability discovery and patching.
Today We'll discuss about the Bug Bounty





THE IMPORTANCE OF BUG BOUNTY PROGRAMS

BUG BOUNTY REFERS TO A PROGRAM WHERE INDIVIDUALS, OFTEN CALLED ETHICAL HACKERS OR SECURITY RESEARCHERS, ARE REWARDED FOR DISCOVERING AND REPORTING VULNERABILITIES OR BUGS IN SOFTWARE, WEBSITES, OR DIGITAL SYSTEMS. IN SIMPLE TERMS, BUG BOUNTY IS A WAY FOR COMPANIES TO INCENTIVIZE PEOPLE TO FIND AND HELP FIX SECURITY FLAWS IN THEIR DIGITAL PLATFORMS.

ALBUS SECURITY





WHY BUG BOUNTY?

ANY COMPANY, BIG OR SMALL, CAN BENEFIT FROM THE EXPERTISE OF SECURITY RESEARCHERS (HACKERS) THROUGH A WELL-EXECUTED BUG BOUNTY PROGRAM.

BUG BOUNTY PROGRAMS PROVIDE AN AVENUE FOR ETHICAL HACKERS TO DISCOVER UNKNOWN VULNERABILITIES IN A COMPANY'S SYSTEMS THAT MIGHT HAVE GONE UNNOTICED OTHERWISE

BUG BOUNTIES PROVIDE AN INCENTIVE FOR RESEARCHERS TO REPORT SECURITY VULNERABILITIES TO COMPANIES RATHER THAN DISCLOSING THEM PUBLICLY, ALLOWING FOR MORE SECURE SYSTEMS OVERALL

ALBUS SECURITY





HOW BUG BOUNTY WORKS?

- COMPANIES DEFINE THE SCOPE OF THEIR BUG BOUNTY PROGRAM, OUTLINING THE TARGETS AND REWARDS AVAILABLE FOR FINDING SECURITY VULNERABILITIES.
- SECURITY RESEARCHERS OR "BUG HUNTERS" USE VARIOUS VULNERABILITY DISCOVERY TECHNIQUES TO TEST THE SYSTEMS DEFINED IN THE BUG BOUNTY PROGRAM. THEY SUBMIT THEIR FINDINGS TO THE COMPANY FOR VERIFICATION AND REWARD OR ATTRIBUTION.
- THE COMPANY VERIFIES THE SUBMITTED VULNERABILITIES, FIXES THEM, AND REWARDS OR ATTRIBUTES THE RESEARCHERS THAT DISCOVERED THEM BASED ON THE DEFINED RULES.

ALBUS SECURITY





TYPES OF BUG BOUNTY PROGRAM

BUG BOUNTY PROGRAMS COME IN DIFFERENT TYPES, INCLUDING PUBLIC, PRIVATE, TIME-BOUND, AND ONGOING. THESE PROGRAMS OFFER REWARDS, LIKE MONEY, RECOGNITION, OR SWAG ITEMS, TO INDIVIDUALS WHO FIND AND REPORT SECURITY VULNERABILITIES. UNDERSTANDING THE DIFFERENT TYPES HELPS RESEARCHERS DECIDE WHICH PROGRAMS TO JOIN, INCREASING THEIR CHANCES OF FINDING VULNERABILITIES.



COMPANY PROFIT

- BUG BOUNTY PROGRAMS OFFER A COST-EFFECTIVE WAY TO CROWDSOURCE SECURITY TESTING AND VULNERABILITY DISCOVERY, POTENTIALLY SAVING COMPANIES MONEY ON EXPENSIVE IN-HOUSE TESTING.
- BUG BOUNTY PROGRAMS PROVIDE ACCESS TO THE EXPERTISE OF THE CYBERSECURITY COMMUNITY, INCLUDING SOME OF THE MOST SKILLED AND EXPERIENCED SECURITY RESEARCHERS.
- BUG BOUNTY PROGRAMS CAN RESULT IN MORE SECURE SYSTEMS AND POSITIVE PRESS COVERAGE, HELPING TO BUILD CUSTOMER TRUST AND REPUTATION.
-

ALBUS SECURITY





CHALLENGES FACES BY HACKER

- COMPANIES MAY ONLY ALLOW TESTING ON CERTAIN SYSTEMS AND NOT PROVIDE ACCESS TO THE ENTIRE INFRASTRUCTURE FOR TESTING, LIMITING THE VULNERABILITIES THAT CAN BE DISCOVERED THROUGH THEIR PROGRAM.
- WITH HIGH REWARDS OFTEN AVAILABLE FOR FINDING VULNERABILITIES, THERE IS COMPETITION AMONG RESEARCHERS TO FIND AND REPORT VULNERABILITIES FASTER, EVEN TO THE POINT OF SELLING INFORMATION TO THIRD PARTIES.
- ONE CHALLENGE FOR BUG BOUNTY HUNTERS IS FINDING VULNERABILITIES IN WELL-STRUCTURED SYSTEMS. THESE SYSTEMS ARE OFTEN DESIGNED WITH STRONG SECURITY MEASURES IN PLACE, MAKING IT MORE DIFFICULT TO IDENTIFY POTENTIAL WEAKNESSES.



PLATFORMS AND RESOURCES

- MANY COMPANIES USE PLATFORMS TO RUN THEIR BUG BOUNTY PROGRAMS. THESE PLATFORMS PROVIDE A SECURE AND STREAMLINED PROCESS FOR RESEARCHERS TO REPORT VULNERABILITIES AND FOR COMPANIES TO MANAGE AND TRACK THEIR BUG BOUNTY PROGRAMS. SOME POPULAR PLATFORMS INCLUDE HACKERONE, BUGCROWD, YESWEHACK, YOGOASHA, INTIGRITI, AND SYNACK.
- MANY COMPANIES DO NOT USE THESE PLATFORMS AND INSTEAD RUN THEIR OWN BUG BOUNTY PROGRAMS FOR THEIR WEB APPLICATIONS, WHERE THEY HAVE ALL THE INFORMATION REGARDING THE PROGRAM.
- FOR RESOURCES SUCH AS ARTICLES, FREE LIVE SESSIONS, PDFS, AND FREE COURSES AND TRAINING, YOU CAN APPLY ALL THESE THINGS IN YOUR CYBERSECURITY JOURNEY.



ALBUS SECURITY



THANK YOU



+91 7983001181



INFO@ALBUSSEC.COM



@ALBUSSEC.COM