What is Bug Bounty and Why Should You Care?

Understanding

Bug bounty programs are initiatives offered by companies where they reward individuals for identifying and reporting security vulnerabilities in their software, websites, or applications.

Enhancing Cybersecurity

By participating in bug bounty programs, you contribute to strengthening the security infrastructure of companies, helping to protect sensitive data and maintain user trust.

Learning and Development

Engaging in bug bounty hunting allows you to develop and hone your cybersecurity skills, keeping you updated with the latest tools and techniques in the field.

Financial Rewards

Participants can earn substantial rewards for their findings. The compensation varies based on the severity of the vulnerability and the company’s budget, ranging from hundreds to thousands of dollars.

Career Opportunities

Successful bug bounty hunters often gain recognition in the cybersecurity community, which can lead to job offers, freelance opportunities, and collaborations with top tech companies.

Flexibility and Independence

Bug bounty hunting offers flexibility, allowing you to work from anywhere and at any time. It’s a great way to earn money on the side or even as a full-time endeavor.

Contribution to the Community

By reporting bugs, you contribute to a safer digital environment for everyone. Your work helps companies fix vulnerabilities before malicious hackers can exploit them.

Proof of Real Earnings from Bug Bounties!

Cyber Security Mon, Oct 30, 2:19 PM (22 hours ago)
to me

Dear Narayanan,

Thanks for submitting the report to us.

After evaluation of the Bugs that you have reported, please find below our comments/responses for each one of them.

1. **AHA Subscription Pack Vulnerability:** Basis our evaluation of bug, we are considering it as a valid bug under severity **P4** which entitles a reward of Rs.5,000/- as per our Bug Bounty program. By manipulating the price value, customers can activate the subscription at a lower price; however, the remaining amount is still shown as pending in the balance due, and customers will have to pay the remaining amount.

Abhishek Pal Mon, Oct 9, 2:44 PM
to Vivek, me

Dear Narayanan,

I hope you are doing well.

I'm delighted to inform you that you're being awarded a bounty of Rs 10,000 for your exceptional contributions to Yatra. Your hard work has been invaluable, and we're grateful for your dedication.

Infosec Team Licious <infosecteam@licious.com> Mon, Mar 13, 6:58 PM
to me

Hi Narayanan

Apologies for the delay in response. We have revalidated your submission and appreciate your efforts for reporting this vulnerability to us and as a result the impact of the vulnerability i.e **Pixel flood Attack** reported by you is classified as informational and is categorized as P5 as per our policy. Severity is calculated on the basis of CVSS score and impact possessed by the vulnerability on Licious.

We appreciate your sincere efforts for responsibly disclosing this vulnerability to us. As a token of appreciation we have decided to award you with an E-voucher of **Rs**[redacted]

Please note: As per the organizations bug bounty program policy all the rewards are finalized by the end of the month and disbursed post an approval process which usually takes 5-7 working days to process.

Regards,
Licious Security Team

Security Team <security@bankopen.co> Wed, Jan 25, 2:46 PM
to me

Hello Narayanan,
Hope you are doing well.
As we have mentioned in a previous email the severity of the issue is medium so we are awarding the bounty as 100$.

Issue : SSRF
Severity : Medium
Bounty : $100

Kindly give us the required documents such as bank acc details, with the front page of your passbook, aadhar card & pan card photos. Also Create an invoice for 100 $ into INR value as per today's rate and also send the invoice with the above mentioned documents. So that we can process your bounty.

Thanks & Regards
Team Security

Join Bug Seekers and Unlock Your Potential to Earn Big

Top 10 Highest-Paid Bug Bounty Reports Worldwide!

- Github access token exposure to Shopify - $50000, 1140 upvotes
- [Pre-Submission][H1-4420-2019] API access to Phabricator on code.uberinternal.com from leaked certificate in git repo to Uber - $39999, 326 upvotes
- Незащищённый экземпляр Zeppelin to Mail.ru - $35000, 164 upvotes
- Remote Command Execution via Github import to GitLab - $33510, 286 upvotes
- RCE via the DecompressedArchiveSizeValidator and Project BulkImports (behind feature flag) to GitLab - $33510, 278 upvotes
- RCE via npm misconfig -- installing internal libraries from the public registry to PayPal - $30000, 844 upvotes
- Arbitrary file read via the bulk imports UploadsPipeline to GitLab - $29000, 294 upvotes
- Exposed Kubernetes API - RCE/Exposed Creds to Snapchat - $25000, 1130 upvotes
- Server Side Request Forgery (SSRF) via Analytics Reports to HackerOne - $25000, 411 upvotes
- SQL Injection in report_xml.php through countryFilter[] parameter to Valve - $25000, 361 upvotes

Discover How Bug Seekers Can Help You Achieve Similar Success

COURSE CONTENT

- INTRODUCTION
- INTRODUCTION TO BURPSUITE
- FOOTPRINTING
- HTML INJECTION
- PATH TRAVERSAL
- CROSS SITE SCRIPTING
- WEB CACHE POISONING
- CROSS SITE REQUEST FORGERY
- SQL INJECTION
- PARAMETER TAMPERING
- SENDER POLICY FRAMEWORK
- WEB SHELLING
- RATE LIMITATIONS
- PASSWORD DOSING
- EXIF METADATA
- INSECURE DIRECT OBJECT REFERENCE
- WEB CACHE DECEPTION
- FILE INCLUSION
- REPORT WRITING
- BUG BOUNTY PLATFORM