

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.

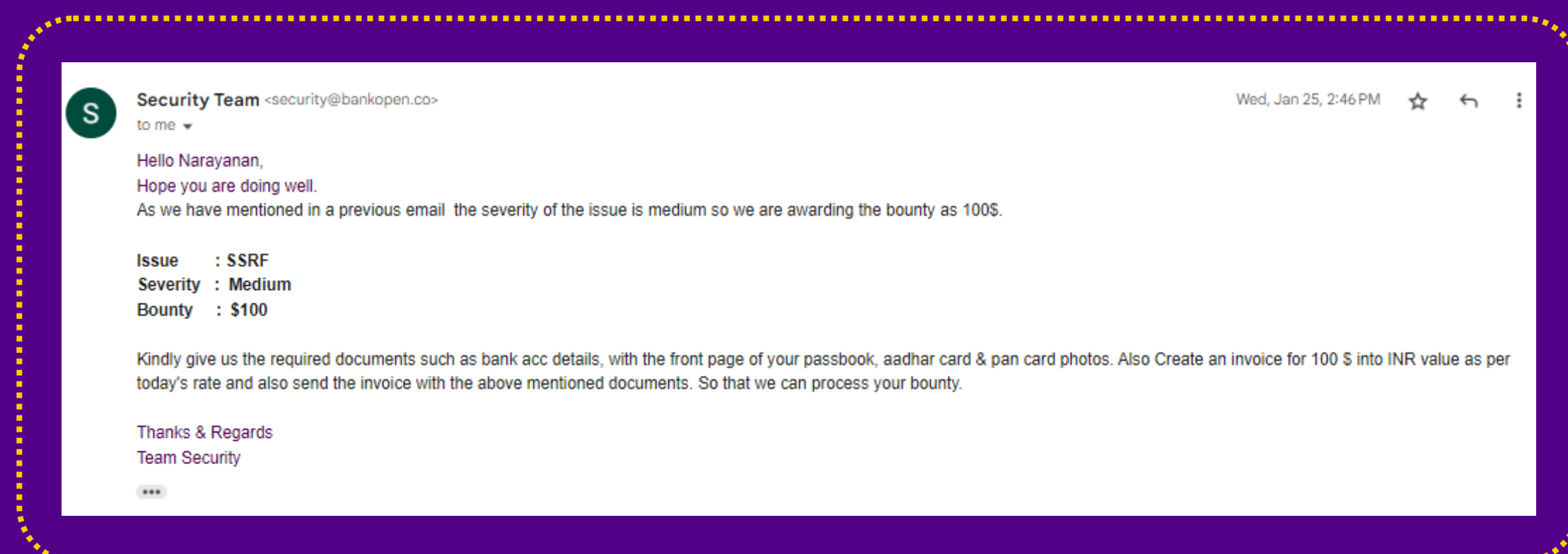
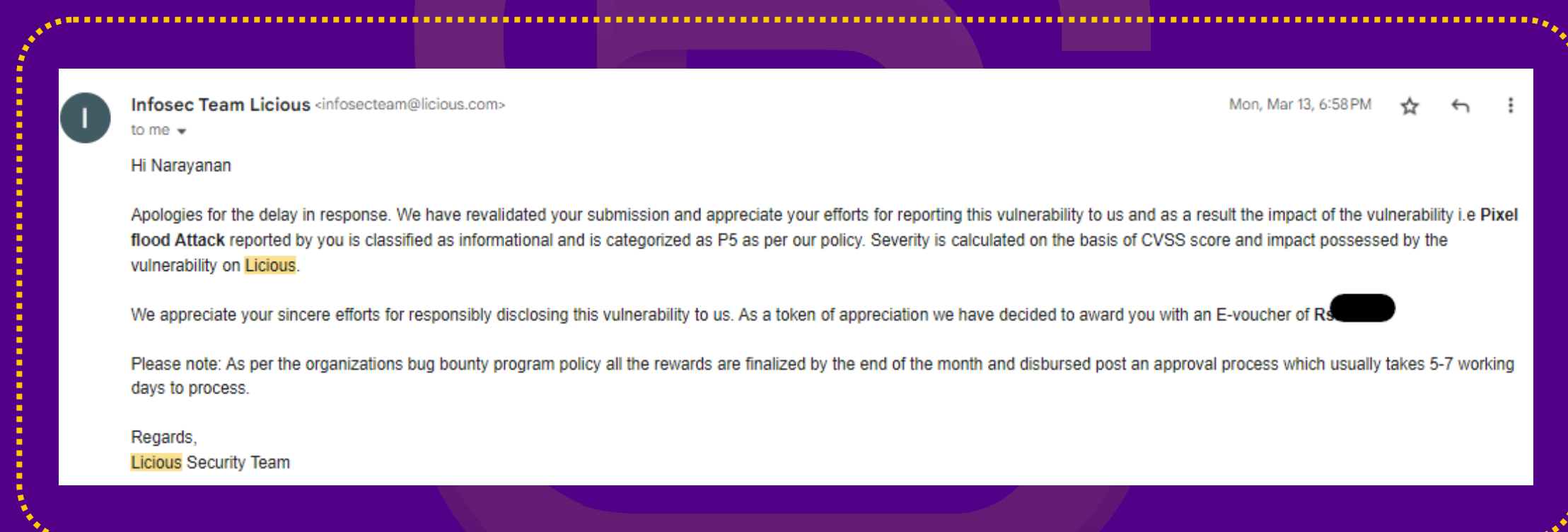
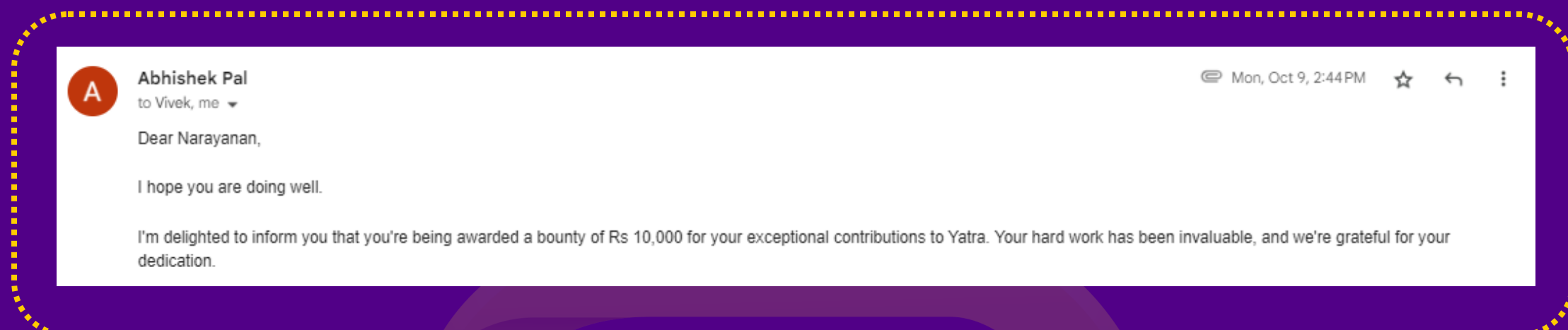
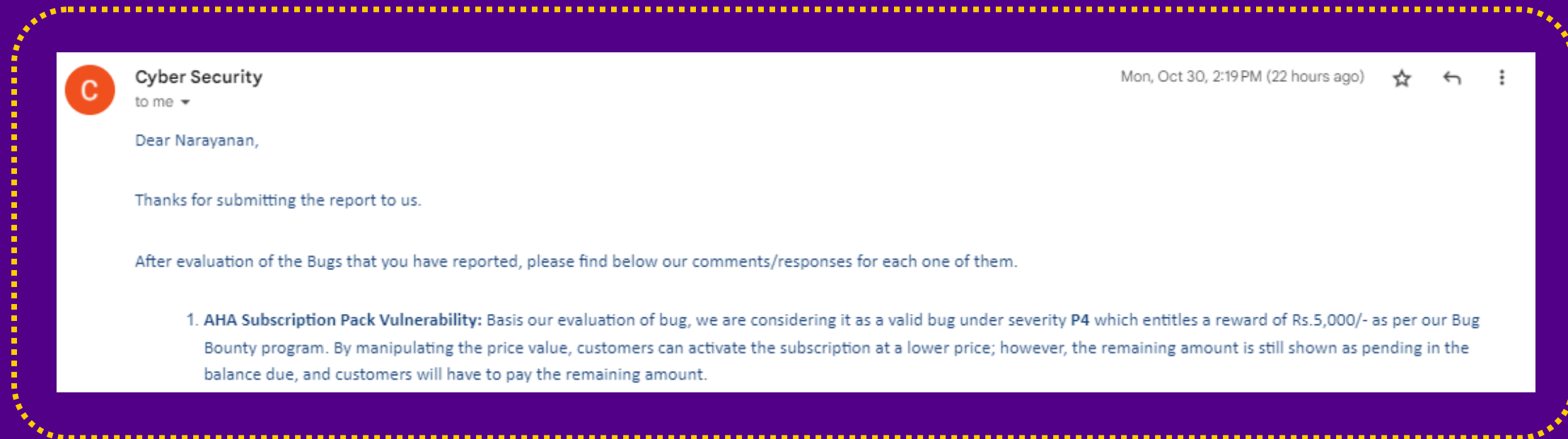
Flexibility and Independence

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!



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