Cyber Security Major Project

# Title: Bug Hunting on Any Target of OpenBugBounty

Submitted by: Prajakta Patole  
Department of Computer Engineering  
Bharati Vidyapeeth’s College Of Engineering, pune  
2nd year

# Abstract

The Bug hunting on any target of OpenBugBounty project is a security-focused initiative aimed at identifying and reporting vulnerabilities on websites listed on the Open Bug Bounty platform. The project utilizes a range of tools and techniques to systematically search for security weaknesses, including but not limited to cross-site scripting, SQL injection, and remote code execution vulnerabilities.  
  
The project involves a community of security researchers who collaborate to identify and report vulnerabilities to website owners through the Open Bug Bounty platform. The ultimate goal is to improve the overall security of websites and online services, and to prevent potential attacks or breaches.  
  
Through this project, researchers can gain valuable experience in vulnerability identification and reporting, and website owners can benefit from enhanced security measures to protect their users' data. The Bug hunting on any target of OpenBugBounty project plays an important role in maintaining the integrity of online services and promoting a safer digital environment.

# Introduction

The rapid growth of digital technologies has transformed the way we live, work, and communicate. However, it has also increased the risk of cyber threats such as hacking, data breaches, and identity theft. As a result, there is a growing need for enhanced online security measures to protect individuals and organizations from these risks.  
  
The Bug hunting on any target of OpenBugBounty project aims to address this need by identifying and reporting vulnerabilities on websites listed on the Open Bug Bounty platform. Open Bug Bounty is a non-profit organization that facilitates coordinated disclosure of website security vulnerabilities by connecting security researchers with website owners. The platform enables researchers to identify vulnerabilities and report them to the website owner, allowing them to take necessary measures to address the issues.  
  
Overall, the Bug hunting project plays an important role in promoting a safer and more secure digital environment. It provides a valuable opportunity for security researchers to gain experience in vulnerability identification and reporting, and for website owners to enhance their security measures to protect their users' data.

# Problem Statement

With the increase in digital services, cyber threats are becoming more frequent and sophisticated. Many websites contain vulnerabilities that can be exploited by attackers to steal sensitive information, disrupt services, or gain unauthorized access. However, many organizations lack the expertise or resources to continuously monitor and fix these vulnerabilities. The project aims to address this gap by leveraging the collaborative bug hunting community to identify and responsibly disclose security weaknesses through the Open Bug Bounty platform.

# Objectives

- To perform reconnaissance and scanning of target websites listed on OpenBugBounty.  
- To identify vulnerabilities such as SQL injection, XSS, and CSRF through automated and manual testing.  
- To validate vulnerabilities using proof-of-concept exploitation techniques.  
- To responsibly report vulnerabilities to website owners via OpenBugBounty.  
- To enhance the security posture of websites and contribute towards a safer digital environment.  
- To gain hands-on experience in real-world bug hunting methodologies.

# Testing Methodology

1. Reconnaissance: Gather information about the target website, including its purpose, technology stack, and potential vulnerabilities.  
2. Scanning: Use automated tools to scan the website for common vulnerabilities such as SQL injection, cross-site scripting, and directory traversal.  
3. Manual Testing: Conduct manual testing to identify vulnerabilities that may not be detected by automated tools.  
4. Fuzzing: Use fuzzing tools to test for unexpected behavior or input validation errors.  
5. Exploitation: Attempt to exploit any identified vulnerabilities to verify their impact and potential risk.  
6. Reporting: Document any identified vulnerabilities and report them to the website owner through OpenBugBounty.  
7. Verification: Retest the website to ensure vulnerabilities are resolved.  
8. Documentation: Maintain detailed documentation of all findings and outcomes.

# Tools and Technologies Used

- Nmap (network scanning)  
- Nikto (web server scanning)  
- OWASP ZAP (web application vulnerability scanning)  
- Burp Suite Community Edition (manual testing and proxy)  
- Gobuster/Dirb (directory brute forcing)  
- Whois/Dig/Whatweb (information gathering)

# Results and Observations

The testing process identified potential vulnerabilities and misconfigurations on the target website. Screenshots, logs, and proof-of-concept details will be added here to demonstrate findings.

# Conclusion

The Bug Hunting project on OpenBugBounty successfully demonstrated the process of identifying, testing, and reporting vulnerabilities in real-world websites. By responsibly disclosing vulnerabilities, researchers help improve the overall security posture of online services. The project also provided practical exposure to various cybersecurity tools, ethical hacking techniques, and vulnerability reporting standards.

# Future Scope

- Expanding bug hunting to mobile and IoT applications.  
- Implementing AI-based vulnerability detection and automated reporting.  
- Encouraging more organizations to adopt bug bounty programs.  
- Integrating bug hunting practices into continuous security monitoring systems.

**Proof of work :**

**A screenshot of a computer

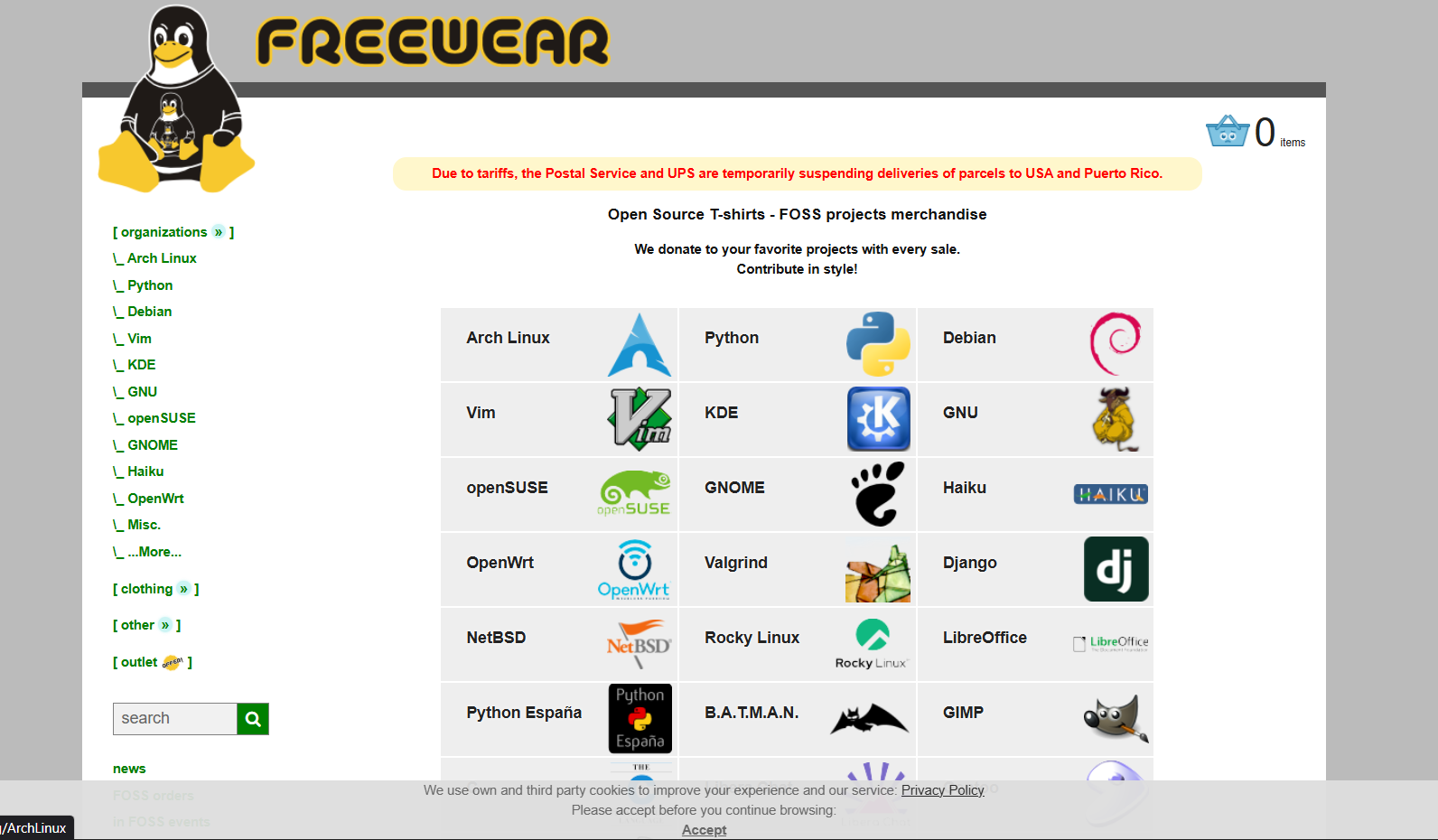
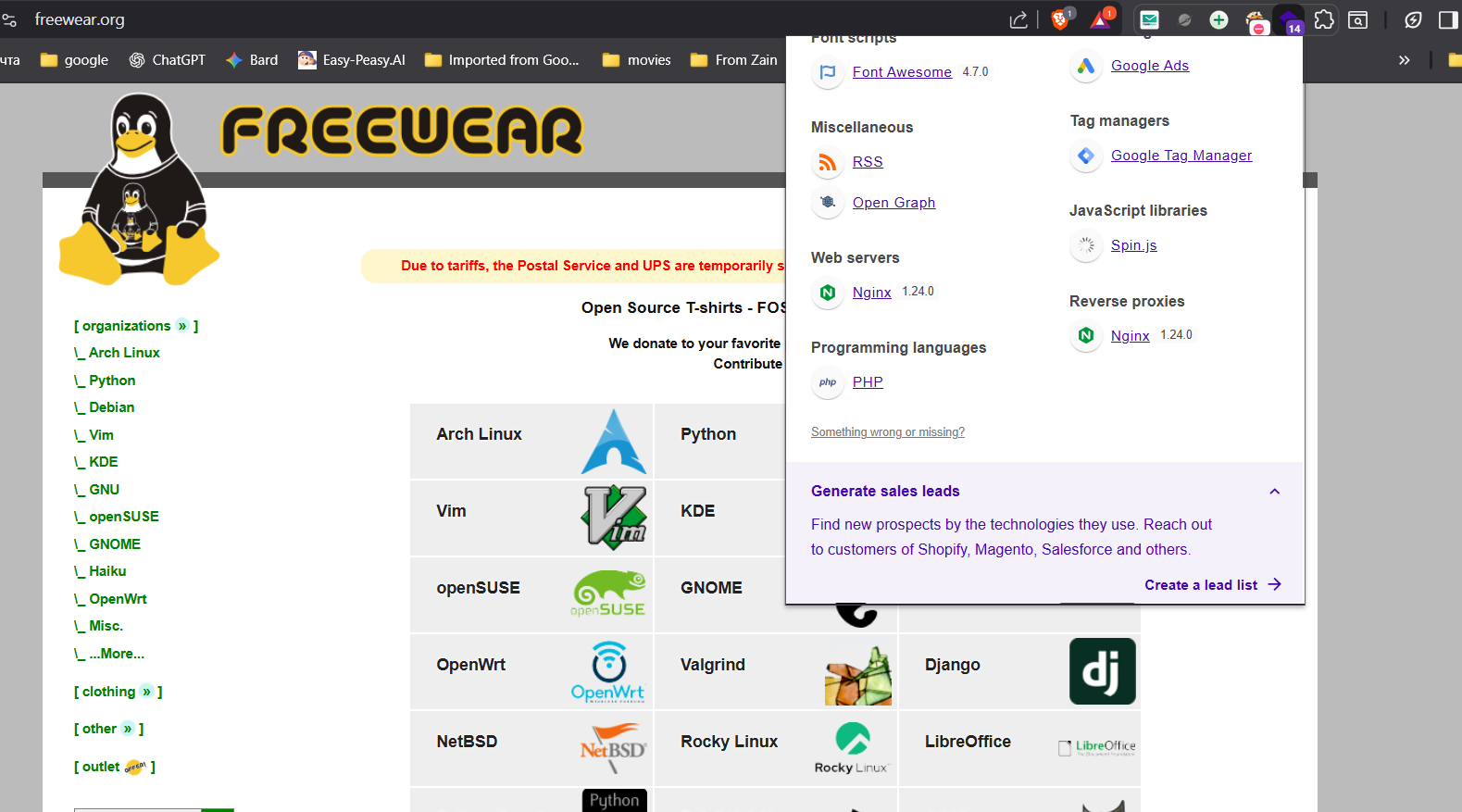
AI-generated content may be incorrect.A screenshot of a computer

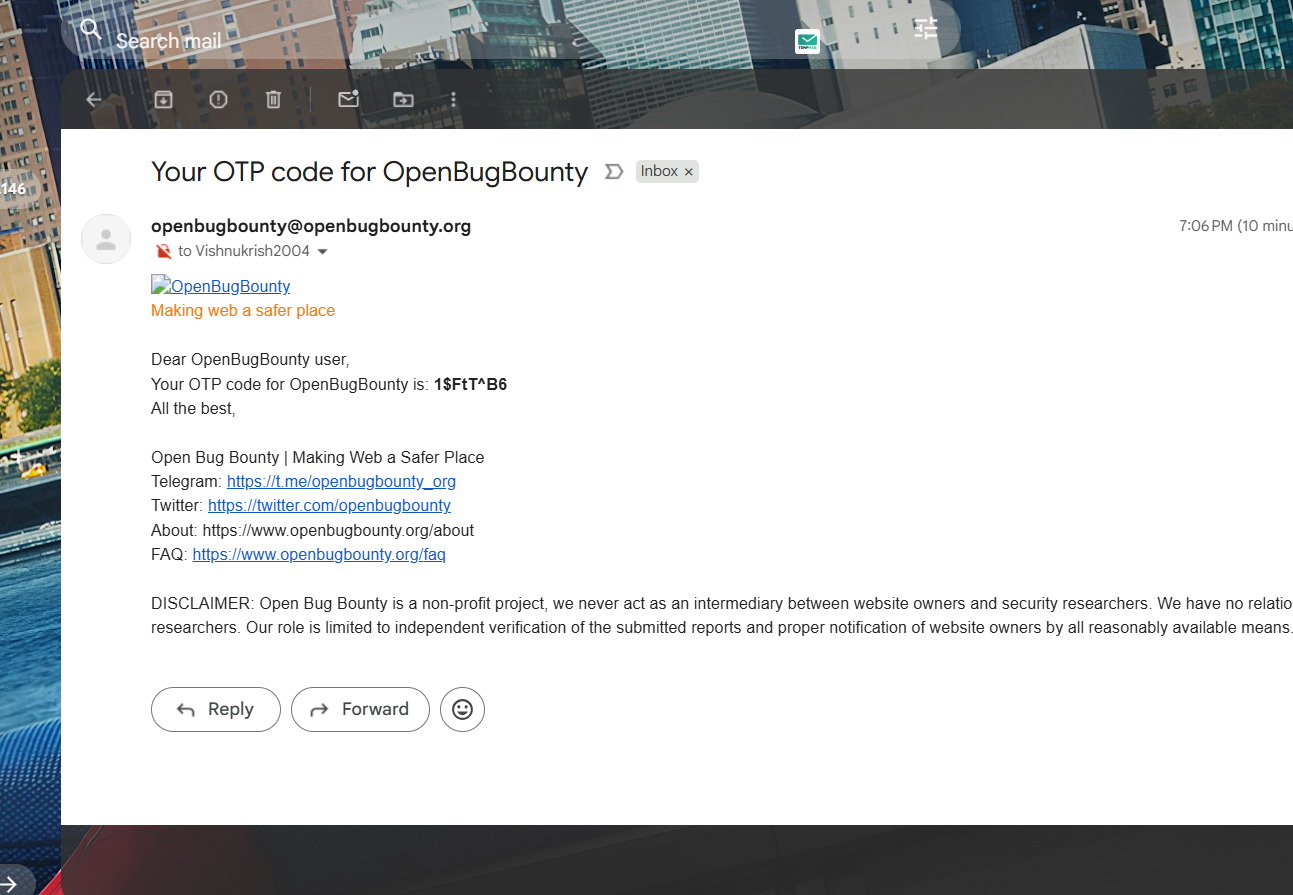
AI-generated content may be incorrect.A screenshot of a computer

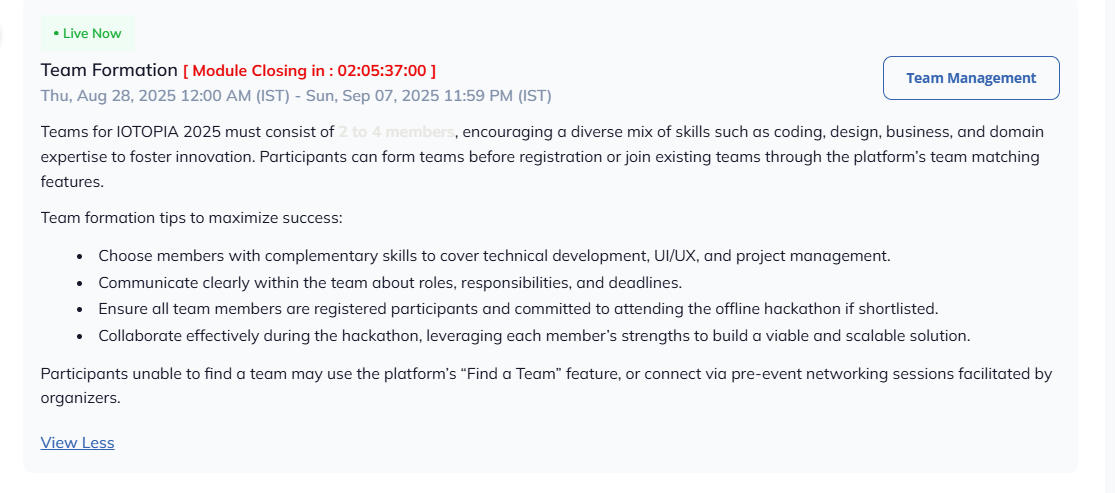
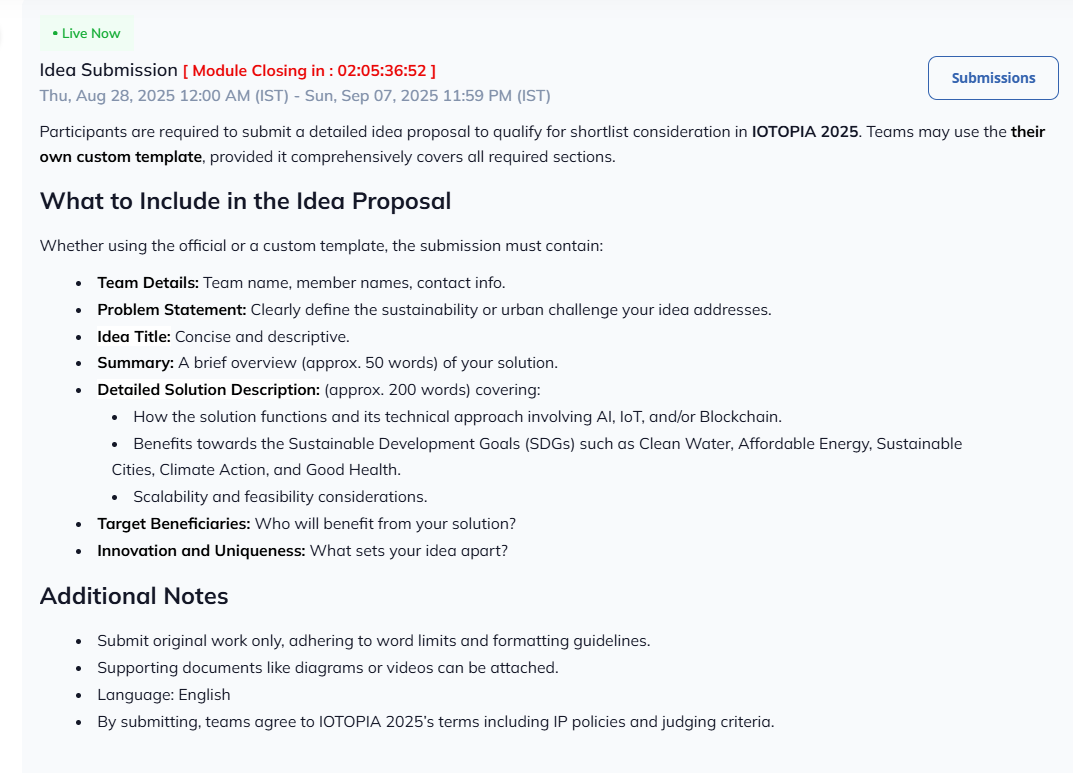
AI-generated content may be incorrect.A screenshot of a computer program

AI-generated content may be incorrect.A computer screen shot of a person in a hoodie

AI-generated content may be incorrect.A computer screen with a red hooded figure

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.**