



SLIIT

Discover Your Future

Sri Lanka Institute of Information Technology

Bug Bounty Progress
SNP – IE2012

IT22921512

S.I.B. Jayawardhana

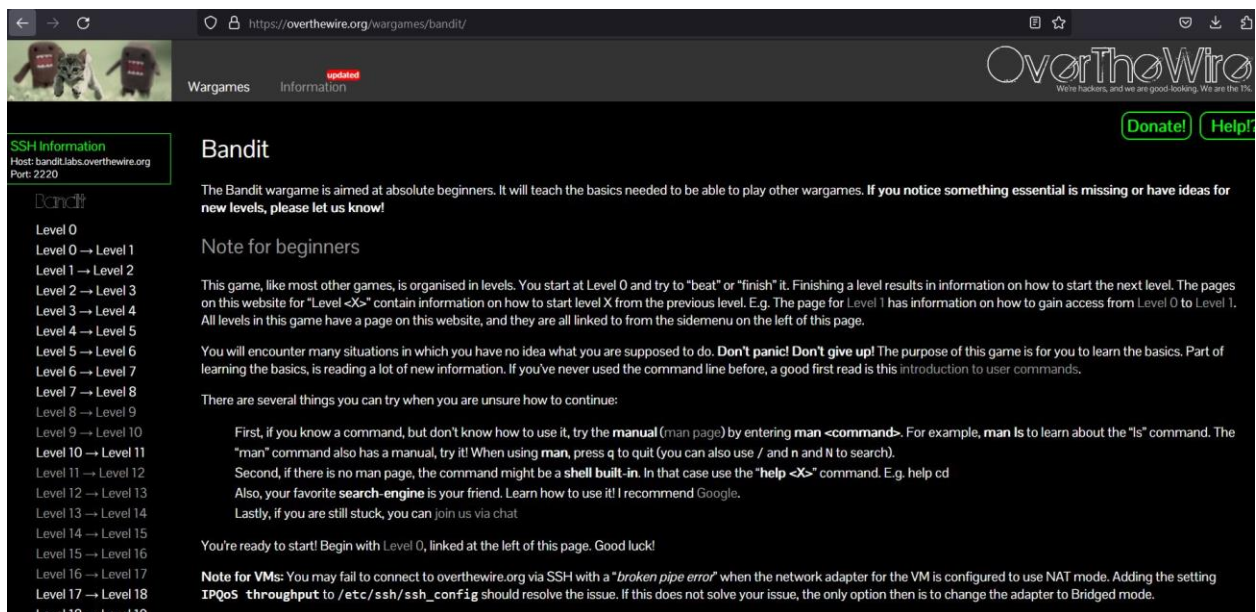
Acknowledgment

Writing, taking notes, or retaining information in our brains are not the only ways to learn. Particularly in a subject like System and Network Programming, everything revolves around application of learnt theories in the real world.

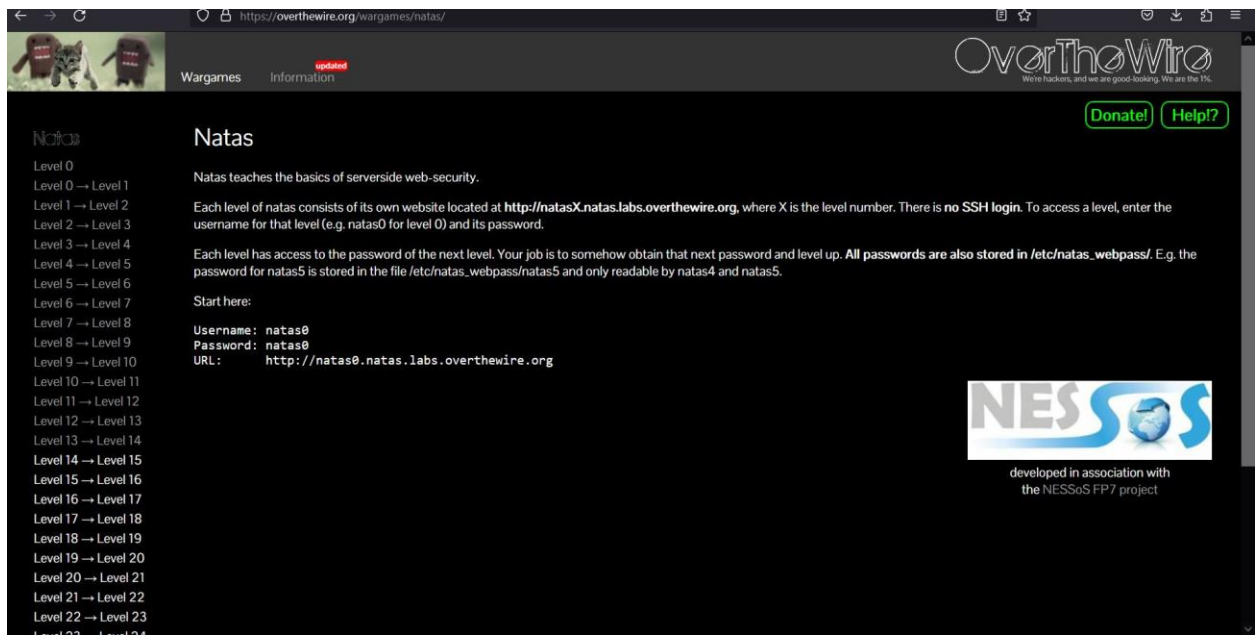
I want to express my sincere gratitude to Dr. Lakmal, Kolihan, and Thaniyawaram for guiding us successfully through the challenging conditions in this module.

About Bug Bounty Progress

- Up to today, I have completed numerous assignments involving vulnerability scanning, vulnerability practice games Sql and XXE injection, and lab exercises so far in this program. All of the assignments we completed serve as the foundation for bug bounty searching or, to put it another way, as the basics of the bug bounty program.
- Bandit



- Natash



SQL injection

- LAB
APPRENTICE
SQL injection vulnerability in WHERE clause allowing retrieval of hidden data →
✓ Solved
- LAB
APPRENTICE
SQL injection vulnerability allowing login bypass →
✓ Solved

XML external entity (XXE) injection

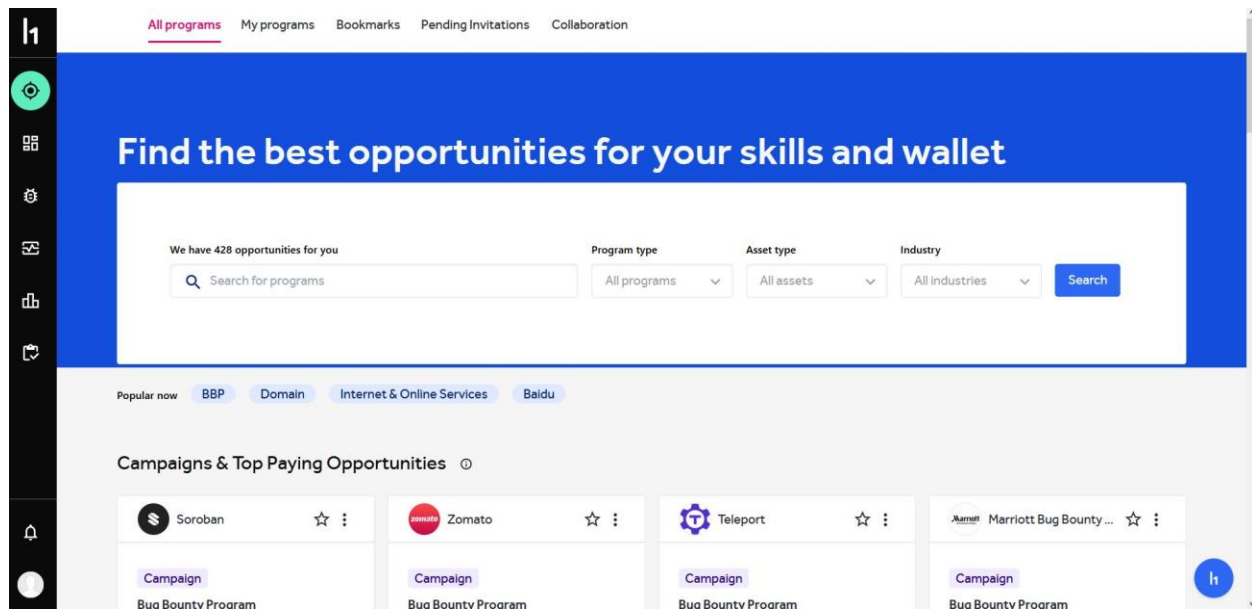
- LAB
APPRENTICE
Exploiting XXE using external entities to retrieve files →
Not solved
- LAB
APPRENTICE
Exploiting XXE to perform SSRF attacks →
Not solved

About Platform

I select HackerOne Platform for the assignment for the bug bounty program. In order to locate and fix vulnerabilities in the digital attack surface, HackerOne, a business that specializes in cybersecurity, especially attack resistance management, combines the security knowledge of ethical hackers with asset discovery, ongoing assessment, and process improvement..

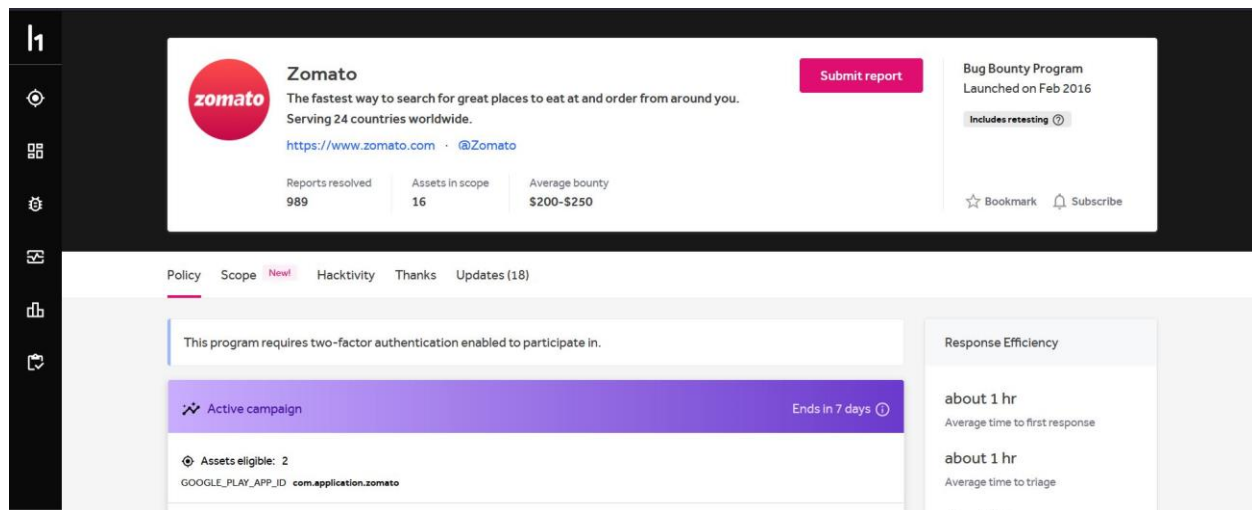
It's a well known and trusted platform for cybersecurity.

hackerone



About the target

1) Zomato



From all the programs offered from hackerone platform I choose *Zomato*. *Zomato* is an Indian multinational restaurant aggregator and food delivery company.

The reason why I select Zomato is because zomato uses mobile app advertising strategies to reach a wider audience and attract more downloads. This includes promoting its app through social media ads, search ads, Zomato's Digital Marketing Strategies. So, Protection is a must in this case.

2) Doppler

Doppler
Doppler is the multi-cloud SecretOps Platform developers and security teams trust to provide secrets management at enterprise scale.
<https://www.doppler.com> · @doppler

Reports resolved: 23 Assets in scope: 6 Average bounty: \$200

Bug Bounty Program
Launched on Dec 2022
Managed by **HackerOne**
Includes retesting ⓘ

☆ Bookmark 🔔 Subscribe

Policy Scope **New!** Hacktivity Thanks Updates (0)

This program requires two-factor authentication enabled to participate in.

Rewards

Low	Medium	High	Critical
\$250	\$750	\$2,500	\$10,000

Last updated on February 27, 2023. [View changes](#)

Response Efficiency

about 1 day
Average time to first response

2 days
Average time to triage

—
Average time to bounty

2 months
Average time to resolution

Doppler is the multi-cloud SecretOps Platform developers and security teams trust to provide secrets management at enterprise scale.