# MEHTAB ZAFAR **Product Security Engineer**

#### PROFESSIONAL EXPERIENCE

# **Red Queen Dynamics**

#### **Security Product Engineer**

July 2021 - Ongoing

- Remote
- Developed from scratch a security training product (using Diango/PostgreSQL) and created a CI/CD pipeline for automated deployments.
- Created and managed cloud infrastructure (AWS) to support internal applications.
- Performed ad-hoc penetration tests for various clients.

# Hackerone / Bugcrowd / Intigriti

**BugBounty** 

Aug 2020 - ongoing

- Independent/Remote
- Listed on Hall of Fame for various companies, such as Google, GitHub, Pay-Pal, US Department of Defense, DELL, Atlassian, Zynga.
- Performed static code analysis to identify various vulnerabilities in APK files.
- Performed zero-day research on open source software.

# The Honeynet Project



Developer

- Improved the speed and functionality of a high-interaction honeypot (Snare/Tanner)
- Added support for persistent storage using PostgreSQL and SQLAlchemy
- Improved the API functionality based on the new database structure
- Both the API and honeypot were written in Python and used libraries like asyncio, Redis, jinja, etc

### Vulnhub / TryHackMe

Devops

- **Aug** 2019 March 2020
- Independent/Remote
- Created various CaptureTheFlag (CTF) challenges for TryHackme.com that teach about Web-related vulnerabilities like XXE, XSS, JWT.
- Created potential Vulnerable machines for VulnHub.com
- All the virtual machines had custom applications made in Python & bash
- Invited to perform beta test various vulnerable virtual machines like TempusFugit series, DC8 for vulnhub.com.

#### XBMC Foundation



Developer

- **May 2018 Aug 2018**
- Google Summer of Code
- Worked on an Open source project under a student program by Google.
- Developed a tool for performing static code analysis on all addons for Kodi, written in Python.

#### **PROJECTS**

Code

- Wrote this tool to automate the bug hunting process on Android applications (APK).
- It can find possible vulnerable activities, receivers and services.

liffy

Code

• Wrote this tool to automate the process of discovering and exploiting Local file inclusion (LFI) attack which can then be leveraged to get a reverse shell.

#### **ACHIEVEMENTS**

Hall of Fame for companies such as Google, Github, PayPal

Offensive Security Certified Professional (OSCP) by Offensive Security

Google Summer Of Code - 2018, 2020

Certified Penetration tester by eLearnSecurity (eJPT)

#### **EDUCATION**

# Inderprastha Engineering College 📋

Jul 2017 - Aug 2021

**B.Tech - Computer Science** 

#### SKILLS

#### **Programming**

Python golang

# Tools/Tech

Burp Suite Metasploit Zap Proxy Docker WireShark

#### Misc

SQL PostgreSQL Redis Git Django

# CI/CD

Github Actions Bitbucket Pipeline Gitlab

# **EXTRA CURRICULARS**

- Participating in CaptureTheFlag competitions with Team OpenToAll.
- Pentest vulnerable virtual machines on platforms like TryHackMe, HackTheBox, Vulnhub.
- Writing technical blog posts on security & development related topics.
- Writing walkthroughs for boot2root machines of HackTheBox & Vulnhub.