

PROFESSIONAL EXPERIENCE

Red Queen Tech

Web Security Engineer

📅 July 2021 – ongoing 📍 Contract

- Wrote various modules for a start-up that needed the automation framework for pentesting.
- Build out an infrastructure to support internal applications.
- Worked in an Agile methodology.

Hackerone / Bugcrowd / Intigriti

BugBounty

📅 Aug 2020 – ongoing 📍 Independent/Remote

- Listed on Hall of Fame for various companies, such as Google, GitHub, PayPal, US Department of Defense, DELL, Atlassian, Zynga.
- I am proficient at web and mobile application security testing.
- Performed static code analysis to identify various vulnerabilities in APK files.
- Performed zero-day research on open source software.
- **HackerOne**: <https://hackerone.com/mzfr>

The HoneyNet Project

🔗 Code

Developer

📅 May 2020 – August 2020 📍 Google Summer of Code

- 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.

Vulnhub / TryHackMe

Content Creator

📅 Aug 2019 – March 2020 📍 Independent/Remote

- Created various CaptureTheFlag (CTF) challenges for TryHackme.com that teaches about Web related vulnerabilities like XXE, XSS, JWT.
- Created a three potential Vulnerable machines for VulnHub.com
- Invited to perform beta tested various vulnerable virtual machines like TempusFugit series, DC8 for vulnhub.com.

XBMC Foundation

🔗 Code

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.

PROJECTS

• slicer

🔗 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.
 - Once exploited, it can also generate & provide reverse shell.

• takeover

🔗 Code

- Made a CLI tool to check subdomain takeover at a mass scale.
- Given output of amass/subfinder this tool can check if any of the subdomain is vulnerable to subdomain takeover.

ACHIEVEMENTS



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 C++ golang

Tools/Tech

Burp Suite Metasploit Zap Proxy
Docker WireShark

Misc

SQL PostgreSQL Git

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.