MEHTAB ZAFAR
Information Security

✉ hello@mzfr.me   🔗 linkedin.com/in/mzfr/

PROFESSIONAL EXPERIENCE

Hackerone / Bugcrowd / Intigriti   **BugBounty**

📅 Aug 2020 – ongoing   📍 Independent/Remote

- Reported bugs to several Fortune 500 companies.
- Focusing mostly on Web and Mobile application related vulnerabilities.
- Hall of Fame in companies like GitHub, PayPal, US Department of Defense, DELL, Atlassian, Zynga etc

The Honeynet Project   ⌗ Code   **Developer**

📅 May 2020 – August 2020   📍 Google Summer of Code

- Made improvement in 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
- Improved cloning functionality using Selenium/Chrome headless browser

MetaBrainz Foundation   **Mentor**

📅 Dec 2019 – Jan 2020   📍 Google Code-In

- Mentored students from all over the globe on various python projects under the MetaBrainz Foundation.

Vulnhub / TryHackMe   **Content Creator**

📅 Aug 2019 – March 2020   📍 Independent/Remote

- Created various CaptureTheFlag (CTF) challenges for TryHackme.com that teaches about Web related vulnerability like XXE, XSS, JWT etc
- Created a bunch of potential Vulnerable machines for VulnHub.com
- 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
  - A tool to automate the bug hunting process on Android applications(APK)
  - It can find possibly vulnerable activities, receivers and services.

- **liffy**   ⌗ Code
  - Wrote this tool to automate the process of discovering and exploiting Local file inclusion attack
  - once exploited, it can also generate & provide reverse shell

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

- **cowrie**   ⌗ Code
  - Added support for DNS reverse lookup and greynoise plugins.
  - Fixed various bugs related to SSH & FTP functionality of the Honeypot

ACHIEVEMENTS

- Offensive Security Certified Professional(**OSCP**) by Offensive Security
- Selected in **Google Summer Of Code** 2018 and 2020, among thousands of applicants from 67 different countries
- Certified Penetration tester by eLearnSecurity (**eJPT**)

EDUCATION

Inderprastha Engineering College 📅

Jul'17 - ongoing

🎓 **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.