LIM WANZHEN

lim.wanzhen.isme@gmail.com | +65 98587504 | cybrsucks.github.io

EDUCATION

NANYANG POLYTECHNIC *Apr 2019 – March 2022*

Diploma in Cybersecurity and Digital Forensics

- *Graduated with 3.0 CGPA*

CHIJ KATONG CONVENT *Jan 2015 – Dec 2018*

GCE 'O' Levels

EXPERIENCE

URBAN REDEVELOPMENT AUTHORITY (URA) *6 Sep 2021 to 20 Feb 2022*

Intern in Information Systems, Applications Department

- Ensuring security of applications that will be used by the public for general query and information, and other urban-planning-related responsibilities that falls under URA.
- Reviewing and evaluating source code on SonarQube done in Java language.
- Scans web applications using AppScan for security vulnerabilities and potential risks during the development process.

ACCENTURE / COLLABERA *TBC / Temporary arrangement*

Trainee Applications Support Engineer

- Currently training under Collabera on Programming in Java to prepare for Java/Jave EE Specialist role in Accenture
- Will automatically be posted to Accenture after assessment

CERTIFICATIONS

CERTIFIED ETHICAL HACKER *Jun 2020*

- Obtained from Diploma Plus Program at Nanyang Polytechnic

RECENT PROJECTS

WEBSITE DESIGN AND UI *Aug 2019*

- Designed a user-friendly interface for users to navigate through an ecommerce website
- Implemented multiple basic and complex functionalities to enhance user experience
- Coded using Python, HTML and CSS

E-COMMERCE WEBSITE DEVELOPMENT *Feb 2020*

- Designed and coded back-end and front-end operations of an e-commerce website with CRUD and with full validation and additional features to support business case

- Coded using Python, Flask, Jinja, MySQL Database, HTML and CSS

APPLICATIONS SECURITY PROJECT *Sep 2020*

- Designed and coded logging and monitoring features according the OWASP Top 10 vulnerabilities to secure an e-commerce website
- Designed and coded RESTful APIs according to website needs
- Coded using Python, Flask, Jinja, MySQL Database, HTML and CSS

CYBERSECURITY PROJECT *May 2021*

- Secure a server from an attacker by implementing a Fail2Ban SSH Server to log service uptime, Splunk Server to monitor fail2ban logs, and a ModSecurity Web Server logging potential attacks
- Secured server against website attacks like SQL injections, cross-site scripting and other OWASP attacks detected by ModSecurity
- Create web server backups and Redis rate-limiting based on IP address as part of resiliency solution and incident response

SKILLS

- Proficient in Python3, web design languages such as HTML5 and CSS
- Some knowledge on Javascript and Java
- Familiar with the use of software such as Wireshark, Packet Tracer, Tableau, FTK Imager tools, VMWare, SQL Workbench, AppScan Enterprise, SonarQube etc.
- Knowledge of Network Security – Firewall, IDS, IPS
- Worked with Security Information Event Management (SIEM) like Splunk Enterprise
- Knowledge on OWASP Top 10 vulnerabilities & Agile Methodology, Scrum Methodology
- Fluent in written and spoken English and Mandarin
- Hobbies include creating digital and traditional illustrations