Last update: Jan 12, 2025

## JAYACHANDRA YANAMANDALA

jayachandra.yanamandala@gmail.com (408) 460-5079 github.com/jayc279 linkedin.com/in/jayzee279

Since cybersecurity will be the main focus of almost everyone who uses internet via desktop, mobile, IoT, wireless etc., switched career paths to be an Ethical Hacker and Penetration Tester and help in efforts to keep us all safe from cyber threats. Currently looking for roles as a Penetration Testing Engineer.

During my certification courses study, due to the various infrastructure building and web applications testing I had done, came to realize I was an Ethical Hacker & Penetration Tester. To elaborate, during my work on iOS app and web applications to support the app as well the real estate site, I tested and fixed vulnerabilities: specifically, login access, Cross Site Scripting, Cookies & session Management, and SQL manipulation.

For the past 25+ years had worked in Electronic Design Automation industry, focused on software testing, risk analysis, infrastructure, and web application development, and now combined with penetration testing skills using cybersecurity tools, and experiences in pretraining GenAI LLM models, am very confident I will be a good addition to penetration testing teams who work to keeping cyberspace safe. I am very dependable, adaptable, and flexible to the strains of penetration testing that occur at odd hours.

Completed certifications, training, research in Certified Ethical Hacking (V12) Specialization, Google Cloud Cybersecurity, GenAI LLM, Deep Learning Neural Networks, Machine Learning, and Data Sciences. Very passionate to continuously learn, working towards completing certifications from SANS, and EC-Council organizations.

### PROFESSIONAL SUMMARY

- Web application Vulnerability testing to prevent cybersecurity threats in mobile, and Real Estate web applications.
- Vulnerable home-lab setup in Oracle VirtualBox: Web Application Vulnerability assessment, penetration testing tools on Kali-Linux and Windows against Metasploitable2, and OWASP-Broken Web App.
- 25+ years software vulnerabilities testing, and full-stack infrastructure development engineer.
- Automation using shell and crontabs on Linux testing and logging trends and history across various software.
- Experienced in Pretraining, Finetuning, and Prompt Engineering GenAI LLMs.
- Continuously learning penetration testing methodologies, passionate to deploy AI solutions in field of cybersecurity.
- Attention to detail and ability to meet strict sign-off dates while maintaining acceptable level of accuracy.
- Reduced system crashes by 70+% in various EDA (Electronic Design Automation) companies, and start-up (early stage).
- Good communication and presentation skills. Dependable, adaptable, and flexible.

### TECHNICALSKILLS

- Cybersecurity Software: Metasploit, Burp Suite, OWASP-ZAP, Amass, Nmap, Wireshark, SQLmap, John the Ripper, Hydra, Sublist3r, dirbuster, goBuster, Nessus, Snort, recon-ng, Hydra, OpenVAS, BeEF, Nikto, Webscarab, Shodan
- Programming: Python, Perl, PHP, Shell, and TCL (good), MySQL, and SQL (intermediate), JavaScript, C, C++, Ruby, and PowerShell (basic)
- Operating Systems & Tools: Kali Linux, Windows, Linux, MacOS, AWS (Intermediate), GCP, and Git (Basic)
- GenAI LLM: Hugging Face, LangChain, Multimodal RAG, OpenAI, BERT, RoBERTa, Flan-T5, Salesforce BLIP, GCP Models
- ML Models: Keras, Sci-Kit learn, Pandas, Numpy, PyTorch, Tensorflow

### EDUCATION

- Certified Ethical Hacking (v12) Specialization
- Generative AI with Large Language Models
- Machine Learning (Stanford Univ)
- Google Cloud CyberSecurity
- Deep Learning Neural Networks (DLNN)
- Data Sciences (Johns Hopkins Univ)
- University of Wyoming, Laramie: M.S.E.E. & M.S. Finance (1992 - 1996)

### PROJECTS

**Penetration Testing against vulnerable apps on Oracle VirtualBox**

- Reconnaissance and Fingerprinting using OSINT tools; Shodan, Google Dorks, Burp & ZAP passive scanning.
- Network Ports mapping and scanning using Nmap, Masscan. Network data packets sniffing using Wireshark.
- Passive and Active scanning; manual & automated, spidering, directory brute-force, etc. (Burp Suite, OWASP-ZAP, Nessus)
- Injection techniques to exploit Web apps: XSS, CSRF, SSRF, SQL, brute-force passwords and users, HTML Headers, etc. (Burp)
- Analyzed system for potential vulnerabilities from improper system and network configuration – Automated and Manual
- Exploitation, and Post exploitation using Metasploit

Last update: Jan 12, 2025

### Generative AI LLMs

- Hugging Face RoBERTa MLM 123+ million parameters, based on Google's BERT model (2018) was trained for 10 epochs against oscar.eo.txt file (approx. 1 million lines) using transformer pipeline.
- Trained and fine-tuned Salesforce BLIP (Unified Vision-Language) against tomytjandra/h-and-m-fashion-caption dataset on using Zero-Shot. Prediction was based on 11 images from test dataset. Bert F1 score ranges between 85% -to- 95%.
- Google Flan T5-small: Trained and fine-tuned using PEFT LoRA, and Prompt instructions against samsum dataset using transformer pipeline. Prediction was around 20% - model needs more training data to improve perplexity scores.

### Deep Neural Networks

- Kaggle: Participated in multiple competitions and documented research on DLNN hyperparameter search techniques: Neural Networks Deep Learning Hyperparameters search and Keras-Tuner-hyperparameters-search-for-Obesity-Risk-Prediction

## ENTERPRENEURIAL EXPERIENCE

### Hallowgram® iOS Meme App

- Designed and developed a features rich iOS app using Xcode and Objective-C enabled users to add text to personal images.
- Backend full stack development application to support the iOS app, built bottom up using PHP and MySQL on AWS EC2.
- Tested for password cracking, SQL injections, XSS, session & cookie stealing, and CSRF vulnerabilities.
- Implemented AWS RDS and S3 to archives greetings. CloudFront and Route53 to host web app in multiple regions & zones.

### SUV Realty Web Application

- Designed, developed a Real Estate web hosting application to target sellers and buyers – PHP, MySQL, JS with login access.
- Tested application for SQL injection, XSS, and PHP vulnerabilities.

## WORK EXPERIENCE

**Stealth Startup** Artificial Intelligence Consultant 03/2024 – 09/2024

- Implemented Prompt-Engineering pipeline for OpenAI GPT transformer model improve quality of completions.
- Documented, analyzed results using charts, various scores and made recommendations regarding choice of prompts.

**Synopsys** Solutions Staff 10/18 – 11/2023 (Sunnyvale, CA)

- Data Scientist, and Machine Learning: developed customized EDA workflows in Python to report design violations.
- Full-stack development project to select and build a Qik Package, using Next.js, Mui, FastAPI, and Python for IP Ecosystem
- Developed Ci/CD RM Flow regression infrastructure in Perl and TCL/Tk. Improved quality and adoption of RM flows by 30%.
- Account level project coordination to complete tasks in accordance with the project schedule.

**Mentor Graphics A Siemens Business** Architect 11/08 – 10/2018 (Fremont, CA)

- Trained offshore teams to implement software vulnerability checks for product releases. Reduced vulnerabilities by 80%
- Extended existing test infrastructure to be 90% automated. Alerts sent to development teams to warn of nightly build issues.
- Conducted post-mortem of product releases with design and development teams to improve stability and quality.
- Recognized for success in developing plans, and procedures to improve processes, quality & stability of software releases.

**Blaze DFM** *Operations* Lead 02/06 – 11/2008 (Sunnyvale, CA)

- Designed and developed a CI/CD architecture system to execute, and host results on web. Technologies used: CGI-PERL.
- Integrated Aprio's test infrastructure into Blaze for QA nightly suites and created 300+ QoR tests.
- Authored BlazeMO first User Manual, documented flows and functionalities of products.

**OKI Semiconductor** Staff CAD Engineer 11/03 – 02/2006 (Sunnyvale, CA)

- Software vulnerability testing & assessment of GGT GoPower power router before integration into Pegasus flow.
- Feasibility analysis on ReShape PDBuilder and identified value add to Pegasus flow.
- Drafted response to RFP (Request for Proposal) and prepared SOW (State of Work) documents on EDA CAD tools
- Integration testing of EDA tools (RedHawk, VoltageStorm, PT, NanRoute). Presented findings to executive staff.

**Cadence Design Systems** Product Engineer 04/96 – 07/2003 (San Jose, CA)

- Identified vulnerabilities in the Place & Route tools releases based on functional specs to improve stability and QoR.
- SDLC Reviews with design teams to address vulnerabilities. Revalidated the vulnerabilities to ensure closure.
- Proof of Concept (PoC) integration flows in Tcl & Shell to stitch various Cadence tools in the BGPKS/SOCE flow.
- Special achievement awards 1996, 1997 for writing 1500+ tests to verify functionality & stability in Timing Modules.