

# Zhekun Hu

✉ zhekunhu@gmail.com

☎ 904-515-6302

🔗 zhekunhu.dev

🌐 linkedin.com/in/zhekunhu

🐙 github.com/huzhekun

## Education

- **Computer Science at UC Davis (Bachelor's)**
  - Sep. 2017 - Dec. 2021

## Skills

- Kubernetes, Ansible, Terraform, AWS
- Kuberay, Karpenter, ArgoCD, Prometheus, Grafana
- C, C++, Python, SQL, Java, Bash, Go
- SSL/TLS, PKI, GCP, DNS, TCP/IP, Apache, Nginx, Linux & Windows System administration
- Metasploit, Nmap, DIRB, Burp Suite

## Work Experience

- **Zoox. (04/2022 - Present)**
  - **Position: Site Reliability Engineer**
  - Responsibilities and Experience:
    - Deploy and maintain Kubernetes clusters.
    - Configure, deploy and maintain supporting cluster components
      - ArgoCD, Karpenter, cert-manager, etc.
  - Design, maintain, and deploy services and applications on Kubernetes
    - Design and manage Ray clusters in Kubernetes with Kuberay operator to serve inference requests
    - Coordinate and design highly available software infrastructure with developer teams.
    - Manage and deploy Cloud resources via Terraform.
    - S3, IAM, RDS, EKS, Opensearch, etc.
    - Manage large fleet of on-prem compute with Ansible.
- **Thinvent Corp. (China) (08/2018 - 09/2018)**
  - Position: Systems administration Intern
  - Tasks performed:
    - Maintaining and supporting a custom database solution.
    - Working with a support team to coordinate access.
    - Deploying custom software solutions.

# Honors & Awards

- DOE Cyberforce Competition Regional Champion (Nov. 2019)

# Clubs

- **Davis Cyber Security Club (09/2018 - 12/2021)**

- Vice President
- Responsible for managing officers and coordinating club activities such as attending CTF's, events, and conferences.
  - Provide technical assistance at workshops for tools such as nmap and ssh, shell utilities for log analysis such as grep and piping, as well as writing bash scripts and deploying reverse shells.

- **Aggie Gaming (10/2019 - 12/2021)**

- President
  - Responsible for hosting, maintenance, and upkeep of club infrastructure, presently hosted on a VPC on GCP. Infrastructure includes web server and discord bot, both with over 4 months of continuous uptime.
  - Maintained and hosted Minecraft server with custom DNS records and 2 continuous months of uptime.
  - Responsible for managing officers and organizing community events.

# CTF Experience

- Reconnaissance
  - Used Nmap to identify running services that may hold vulnerabilities
  - Utilized Dirb to find hidden management interfaces and directories on webservers
  - Searched for common CVEs
- Webapp Enumeration
  - Burp Suite
    - Capture HTTP traffic to and from the backend
    - Enumerate, or fuzz webapp API calls to find potential code execution vulnerabilities
    - Manipulate POST requests to insert malicious parameters
  - Injection Attacks
    - Took advantage of XSS and CSRF vulnerabilities to extract credentials from other clients
    - Utilized SQLi to bypass authentication and exfiltrate secrets from databases
- DNS
  - DynDNS
    - Learned how to compromise a DynDNS server when given credentials

- Updated DNS records to register personal machine under organization domain
- Privilege escalation
  - Automated search with LinPEAS to identify potential privilege escalation vectors
  - Manually searched to find credentials on the file system
  - Exploited SUID executables and sudo-allowed commands by manipulating input parameters to gain root access