Chaofan Shou

5691 Stinson Way, Goleta, CA, 93117
805-284-7138 · scf@ieee.org · shou@ucsb.edu
https://github.com/shouc

Introduction

I am a second-year student majoring Computer Science at UC Santa Barbara. I am now open for job and research opportunities where I can apply my skills.

Education

UC Santa Barbara
BS in Computer Science
- Expected to graduate at Jan, 2022
- Related courses: OS, Automata, Network, Binary Security
- GPA: 4.0, Dean's Honor x 3

Online Education
- Machine Learning - Andrew Ng, 2016 Certificate ID: 5UAB2MXFLDCY
- Automated Reasoning: satisfiability - EIT Digital, 2020 Certificate ID: BKTPXS4CXXVS

Full-time Work Experience

Salesforce.com Inc. San Francisco, CA
Software Engineer Intern *06/2020 - 09/2020*
- Worked on an AWS EMR metrics collection library that publishes metrics to internal monitoring frameworks and helped instrumenting exisiting Hadoop/Spark jobs with it.
- Analyzed metrics from Spark clusters and determined under-provisioned / over-provisioned jobs.
- Created dashboards on Grafana & Splunk to provide detailed information regarding Spark job optimization.
- Patched a race-condition issue in Redshift metrics collection library that caused failures over AWS data pipelines.
- Rewrote SQL of a data pipeline to support a specific change in logic.
- Stack Used: Java, Scala, Python, AWS, Spark, Redshift, MySQL

Part-time / Contracting Work Experience

Faria Education Group Remote
Security & AI Consultant *10/2018 - 09/2019*
- Provided information security consulting including security assessment.
- Conducted two pentests and identified 8+ risks.

UCSB SexInfo Project Remote
DevOps Engineer *10/2019 - Present*
- Developed Wordpress plugins and customized themes to fulfill researchers' special request on QA section, UI, etc.
- Managed a Wordpress website with 500k+ MAUs and successfully handled two accidents in production system.

Bug Bounty Programs
External Pentestor
- Netease: Discovered 2 severe XSS & CSRF vulnerabilities that could lead to 1.1 billion accounts takeover.
- PingAn Insurance: Discovered 1 severe code injection vulnerability that leaks millions of lines of personal information.
- International Baccalaureate (IBO): Discovered 1 access control risk that leads to admin accounts takeover.
- Shanghai Government: Discovered 50+ access control, LFI, SQL Injection, XSS, etc. vulnerabilities on government infrastructures.

Selected Projects

DAudit
Main Contributor
DAudit provides Ops team an easier interface to evaluate risks in configuration of databases and big data toolkits.
Stack Used: Python, MySQL, Redis, ELK, Hadoop, Spark, MongoDB

Relier (Incubating)
SDE & Cofounder
Relier is a meetup App for adventurers and teenagers.
Stack Used: Golang, WebRTC, GKE, React Native, Swift, Kotlin, Hadoop Stack, HBase, gRPC.

IBKiller
Lead SDE & PM

IBKiller provides a platform for IB students to share notes and video, as well as practicing exam-style questions. The DAUs have once reached 200+. I am the lead engineer and PM of this project. I have overseen one major updates in infrastructure.

- Version 2 Stack Used: Golang, Vue.js, MySQL, Redis, Kubernetes
- Version 1 Stack Used: Laravel(PHP), MySQL, AWS Lambda, Heroku
- This project is no longer active due to policy issues. API has been removed yet frontend is still served for demo purposes. Full code / demo on request.

Baidu CUP
Contributor

CUP is a Python interface for system management. It is the most popular Python library inside Baidu. I have contributed the macOS module.

Selected Vulnerability Discoveries

CVE-2020-11709
cpp-httplib client has been discovered a Header Injection vulnerability, which allows attackers to conduct code execution on users of websites built on this library.

CVE-2020-9329
Gogs, a widely used Git platform, has been discovered a race condition vulnerability, which allows attackers to violate the admin-specified policies.

CVE-2020-7105
An official Redis client that is deployed to millions of servers has been discovered a null-pointer-dereferencing vulnerability, which allows attackers to conduct denial-of-service attack easily.

H/O#748835
[Undisclosed] This vulnerability allows attackers to visit CVS internal network, which has potential to leak users (patients) personal information.

Competitions

CTF (Capture the Flags) *Cybersecurity Competitions*
I usually work on CTFs with two of my classmates who are both undergraduates. Our team is called by7ch. I may also play with Shellphish. I mainly take care of challenges related to web applications and forensic.

Selected Participated Events:

- *UCSB iCTF 2020* - Ranked 23rd globally and 3rd among US teams.
- *m0leCon CTF 2020* - Ranked 53rd globally and 6th among US teams.
- *VolgaCTF 2020* - Ranked 78th globally and 6th among US teams.
- *PlaidCTF 2020* - Ranked 86th globally and 14th among US teams.

Organized Events:

- *WeCTF 2020* - I am the lead organizer, DevOps engineer, and author of the challenges. The event has attracted more than 700 teams from all over the world and been rated as one of the best web security oriented CTFs. Reviews from participants

Research Experience

UCSB VLab (PI: Tevfik Bultan) *10/2019 - Present*

- Conducted analysis on websites of medical industry and discovered side-channel vulnerabilities with the team, which lead to leakage of users' medical data and credentials.
- Created a large computing cluster to conduct real-world side channel quantification, leading to 90%+ reduction in experiment time.
- Created large benchmarks to evaluate the robustness of side channel evaluation tools.

Skills

- **Proficient: Python, PHP, C/C++, JavaScript/NodeJS, Golang, React Native, Pentest, Code Review**
- Familiar: Bash, Django, Laravel, Hadoop Stack, Kotlin, Vue, React, HTML5/*CSS, Assembly, LLVM
- Working Knowledge: Redis, (My)SQL, MongoDB, Docker, Kubernetes, WebRTC, AWS