Raphael Karger

rkarger@albany.edu

Last Updated on November 12, 2020

EXPERIENCE

ADVANCED COURSE IN ENGINEERING (ACE) | Intern

June 2020 - August 2020 | Assured Information Security (AIS), Rome, NY

- Contracted on behalf of AIS for the Air Force Research Laboratory.
- Engaged in rigorous cyber warfare boot camp through intense coursework, research, and multi-domain field operations.
- Solved graduate-level challenges for open-ended Air Force relevant problems in exploit development, hardware security, covert communication, reverse engineering, and redteam operations.
- Planned, lead, and executed a simulated cyber warfare campaign.

CYBER DEFENSE ORGANIZATION | Executive Board Member

September 2019 - Present | University at Albany, NY

- Head of University at Albany's Collegiate Red Team.
- Defended and operated a simulated corporate network against active professional attackers in several Red vs Blue competitions.
- Developed, contributed to, maintained, and optimized a full stack web application used in Red vs Blue Competitions. Built using custom Node.js workers, MongoDB and VUE.

OPENSOURCE CONTRIBUTOR | Repository Creator & Maintainer

May 2017 – Present

- mXtract - A C++ memory analysis program that parses current memory and environment files and extracts private keys, IPs, and passwords with regexes.
- DDoor - A cross platform backdoor written in C++ that utilizes DNS TXT records for command execution. It currently has encrypted communication, anti-debugging, and auto-privilege escalation.
- fireELF - A Python framework to generate fileless Linux malware payloads.

SECURITY RESEARCH

CVES | Discovered Vulnerabilities on Widely Used Webapps

I discovered one *Privilege-Escalation* and four *Stored XSS* vulnerabilities on software developed by BBPress and PHPJabbers. For my research I was assigned Mitre's Common Vulnerabilities and Exposures (CVE) IDs **12810, 12811, 12812, 12813,** and **13693**.

EXPLOIT DEVELOPMENT | WordPress Plugin Exploit PoCs

Researched, developed, and authored three *Authentication Bypass exploits* for a widely used *WordPress plugins* that affected at the time around a *quarter-million* websites each. Exploit-Database IDs: **47832**, **47939**, **48534**.

BUG BOUNTY | Freelance

Publicly acknowledged for finding web application vulnerabilities by **Adobe**, **Apple**, **European Union**, **Microsoft**, **Oracle**, **United Nations**, and many more, a full list can be found **Here**.

CERTIFICATIONS

OSCE

Offensive Security
October 2020

OSCP

Offensive Security
Feb 2020

OSWE

Offensive Security
May 2020

SKILLS

PROGRAMMING

Python • PHP • C
C++ • LaTeX • Javascript • Bash
MongoDB • MySQL • x86 Assembly

VIRTUALIZATION

Docker • Proxmox • VMWare

OTHER

Web Application Penetration Testing
Network Penetration Testing
Software Reverse Engineering
Linux Server Administration
System Automation

EDUCATION

UNIVERSITY AT ALBANY

BS, Informatics, Conc. Cybersecurity
GPA: 3.8/4.0
Tau Sigma Honor Society Member
Expected Summer 2022 | Albany, NY

LINKS

Github:// **rek7**
Personal Site:// **raphael.karger.is**
Blog:// **blog.raphael.karger.is**
LinkedIn:// **raphael-karger**