João C Buschinelli

Cyber Security & Software Engineer

+55 (11) 98964-9404

Github

buschinellijoao@gmail.com

LinkedIn

https://codigocaotico.com

Santa Cecília, São Paulo - Brazil

SUMMARY

Versatile Software Development Engineer with a strong background in Cybersecurity, Malware Research & Development, and Full Stack Web Development. Skilled in low-level programming (C and C++), with over four years of experience in designing and developing scalable software tools and automation processes using Python and C++. Experienced in system design, implementing secure coding practices, and integrating security measures into the software development life cycle. Proficient in PHP and Laravel for web development, with a track record of identifying and mitigating security vulnerabilities in Open Source projects. Known for leadership in incident response, mentoring junior engineers, and delivering reliable, secure, and maintainable code.

EXPERIENCE

Cyber Security Engineer & Software Developer 04/2024 - Present

Orbium

- **Led the establishment of the cybersecurity department**, driving compliance with LGPD, GDPR, and spearheading the acquisition of ISO 27001 certification, ensuring robust security standards across the organization.
- **Designed and delivered comprehensive security training programs** for the team, improving overall security awareness and best practices.
- **Developed advanced malware testing tools using C++**, applying SOLID principles and adhering to the Google C++ Style Guide, enhancing on-site threat detection capabilities.
- **Implemented secure coding practices** for software development in .NET, integrating security by design principles into the development life cycle.
- **Securing the entire software development lifecycle (SDLC) of Orbium's CRM software,** implementing automated vulnerability scanning and monitoring solutions. Ensured continuous security validation across cloud deployments, coding standards, code reviews, source control management, build processes, testing, and operational security.
- **Architected and optimized network designs** for Active Directory (AD) and AWS, ensuring secure, scalable, and efficient deployment, management, and scaling of resources.
- **Managed and configured AWS Firewall and IAM roles**, establishing secure access controls and maintaining robust cloud security environments.

Information Security Analyst 07/2023 - 04/2024

Orbium

- **Led threat intelligence initiatives**, gathering and analyzing market data to anticipate and mitigate emerging risks.
- **Conducted bimonthly security assessments, penetration tests, and risk evaluations**, identifying and remediating over 50 potential threats, enhancing the company’s security posture.
- **Utilized and customized security tools**, including Burp Suite and OWASP ZAP, while developing custom penetration testing tools to address specific vulnerabilities.
- **Developed a CRM web application using PHP and Laravel**, streamlining the management of internal employee performance metrics, including leads and sales phases, with intuitive data visualization capabilities.
- **Automated security testing and task processes using Python**, significantly improving the speed and accuracy of penetration testing workflows.
- **Oversaw the development, protection, and continuous maintenance of the company's central website and internal systems**, ensuring high availability and robust security.

Software Developer & Security Researcher 11/2022 - Present

Código Caótico

- **Developed a personal portfolio using Laravel**, following best coding and security practices, including designing a robust database architecture and building the application from scratch to ensure a secure, scalable structure.

- **Developing and integrating an .NET framework API for Hikvision UMobile** for parking lot barrier gates, enabling automated control through facial recognition, ensuring seamless integration with physical security systems.
- **Customized and integrated a Prestashop PHP module** to connect with the Sedex API, Brazil's official mailing system, automating shipping calculations for enhanced operational efficiency.
- **Leading the development of a scalable e-commerce platform** using PHP and custom PrestaShop themes for Dr. T Vitaminas e Suplementos, ensuring a seamless user experience and scalability for future growth.
- **Enhanced Dolibarr's security posture** by performing penetration testing, source code security assessments, and producing detailed vulnerability reports. Identified two critical vulnerabilities that were assigned CVEs, contributing to the community's security improvements.

Master Thesis Researcher 01/2019 - 08/2022
McGill University

- **Developed a set of estimators** based on the Fourier flat-sky approximation statistics to identify departures from statistical translation invariance, while contributing to the 21cmFAST project using Python and C. **Collaborated closely with a multidisciplinary research team**, sharing insights and ensuring smooth integration of new statistical methods.
- **Guided and mentored undergraduate researchers** involved in the Cosmic Dawn projects, providing training on data analysis techniques, simulation methods, and best practices in Python coding.
- **Contributed to the maintenance of Cosmic Dawn projects** during my Master thesis, implementing estimators and analyzing data from simulations to assess the impact of astrophysical and cosmological processes on early universe observations. **Fostered a collaborative environment** by facilitating discussions and brainstorming sessions, ensuring clear communication of complex concepts among team members.

E D U C A T I O N

Master of Science in Physics - Cosmology 01/2019 - 08/2022
McGill University, Montreal - Canada
Bachelor Degree in Physics 05/2015 - 12/2018
Universidade Federal do ABC, Santo André - Brasil
Bachelor Degree in Science & Technology 05/2015 - 12/2018
Universidade Federal do ABC, Santo André - Brasil

P R O J E C T S

Hikvision API Integration | .NET Framework 06/2024 - Present
Parking Lot Automation

- Developing and integrating a Hikvision API with the .NET framework to automate control of parking lot barrier gates through facial recognition, ensuring a seamless and secure user experience.
- Optimized the API for real-time performance, reducing latency to ensure quick response times and minimizing delays in access control operations.
- Designing a scalable system architecture for handling large volumes of data by utilizing data structures to queue and store user entries (regular users' faces) in the cloud.
- Implementing a mechanism that automatically offloads data from the Hikvision in-house database to the cloud, ensuring efficient storage management by deleting the oldest entries locally while maintaining backups.
- Applying best practices in API design and security, with a strong focus on data privacy, secure authentication, and encrypted data transmission to protect user information.

Worm Malware | C++ 08/2023 - Present
Parasyte

- Currently engaged on my own Open Source project, designed for educational purposes, intended to develop a Worm Malware with a toolset of different exploits to traverse and infect network security flaws.
- Adhered Google Style Guide for C++ and SOLID framework for easy maintenance of the project, as well as implementing rigorous documentation and testing protocols to ensure the project's integrity and educational value.
- The project aims to simulate how real worm malwares work under the hood and how one is able to gracefully detect and remove it with help of Firewalls and IDS.

PUBLICATIONS

CVE-2024-29477

Identified a code injection vulnerability in the Dolibarr ERP CRM Open Source project, leading to a potential Remote Code Execution (RCE). The vulnerability was rated with a CVSS v2 score of 8.4.

CVE-2024-31503

Together with another security researcher, discovered a vulnerability involving broken access control and session hijacking in the Dolibarr ERP CRM Open Source project. The vulnerability allows session cookies and anti-CSRF tokens to be stolen and used to access an account without needing a password.

CVE-2024-37821

Identified an arbitrary file upload vulnerability in the Upload Template function of Dolibarr ERP CRM up to v19.0.1 that allows attackers to inject maliciously crafted SQL statements and execute arbitrary code via uploading a crafted .SQL file.

LANGUAGES

Portuguese - - - - - - - - - - - - - - - - Native

English - Fluent

Russian - Basic

German - - - - - - - - - - - - - - - - - - - Basic