Piotr Gaszczyński

Penetration Tester

Contact Information

Email: piotrek.gaszczynski@gmail.com
Phone / WhatsApp: +48 605 208 772
GitHub: https://github.com/PedroPLCode
Webpage: https://pedroplcode.github.io/portfolio/

Professional Summary

Detail-oriented **Penetration Tester** and **Backend Developer** with strong expertise in **Python, Flask, Django, SQL, REST APIs and cybersecurity tools**. Skilled in identifying and mitigating vulnerabilities, performing web application security testing, and automating analysis workflows. Experienced in using **Kali Linux, Metasploit, Burp Suite, and Nessus** for penetration testing and vulnerability assessment.
Proficient in AI-assisted coding (GitHub Copilot, ChatGPT) data analysis (Pandas, NumPy), and web application development with JavaScript, React.js, HTML5, and CSS3.
Fluent in English with extensive experience leading teams in international, multilingual environments.
Comfortable working on GNU/Linux and FreeBSD systems.

Technical Skills

Penetration Testing Tools: Kali Linux, Metasploit, Burp Suite, Nessus, Nikto, OWASP ZAP
Programming & Scripting: Python, JavaScript, Bash
Frameworks: Flask, Django, React.js, Redux
Cybersecurity & Web Security: SQL Injection, XSS, CSRF, Authentication/Authorization Testing, Secure Coding Practices, API Security
Data Analysis & Automation: Pandas, NumPy, Keras
Databases: MySQL, PostgreSQL, SQL
Operating Systems & DevOps: GNU/Linux (Debian, Kali), FreeBSD, Nginx, Gunicorn
Development Practices: Object-Oriented Programming (OOP), Test Driven Development (TDD), REST API Development, CI/CD
Version Control & Tools: Git, GitHub, Docker

Soft Skills

- Problem-solving
- Teamwork and Communication
- Time management
- Adaptability
- Leadership

Languages

Polish - Native, English - Advanced

Projects & Technical Achievements

BrutePedro - HTML POST Form Tester - 2025
- Python tool for ethical testing of web form security (HTTP POST)
- Configurable payloads, session handling, delays, and detailed result logging

Zen - Vulnerability Scanner - 2025
- Modular scanner detecting XSS, SQLi, and insecure headers
- Plugin-based design, async scanning, and JSON/CSV reporting

Freelance & Personal Open Source Projects - 2023-Present
- Personal GitHub Repository portfolio showcasing backend, cybersecurity, and data analysis projects
- Focus on clean code, maintainability, testing, and documentation

Cryptocurrency Trading Bot - Python, Binance API, Pandas, NumPy, Keras - 2024
- Developed automated trading bot with real-time data analysis
- Implemented algorithmic trading strategies and data-driven decision-making
- Applied AI-assisted coding and secure API integration
Tech Stack: Flask, SQLAlchemy, APScheduler, Binance API, Pandas, Numpy, Keras

Work Experience
Team Leader - Global Wind Service - 2017-Present
- Lead Rope Access Authorised Technicians for offshore wind turbine maintenance
- Supervise project progress, safety, and compliance
- Prepare reports and communicate with clients
- Skills applied: Leadership, Project Management, Safety Compliance, Teamwork, Communication

Owner - Optima Rope Access Solutions - 2011-Present
- Plan and manage Rope Access projects
- Coordinate teams and client interactions
- Skills applied: Project Planning, Client Management, Problem-Solving, Team Coordination,

Education & Certificates
Cyberium Masterclass - Cybersecurity Training - 10/2025
- Advanced penetration testing course with extensive labs
- Web application security, SQL injection, XSS, and other security topics

Kodilla Bootcamp Backend - Python, Flask, Django - 05/2024
- Backend development using Python and Flask
- REST API design, database integration, project deployment
Kodilla Bootcamp Frontend - React & JavaScript - 10/2023
- Frontend development with React.js and JavaScript
- HTML5, CSS3, SCSS, responsive web design, Redux state management

Adam Mickiewicz University - Master of Biology - 2010
- Analytical skills, scientific approach, problem-solving

Keywords: Penetration Testing, Ethical Hacking, Vulnerability Assessment, Python, Flask, Web Security, OWASP, Metasploit, Burp Suite, API Security, Linux, Docker