ALEXANDR ROMANOV

Contact Info:
+49 152 23119282
downitch@proton.me
downitch.github.io

Current Location:
Germany

Work Authorization:
Germany
Kazakhstan

Languages:
- English (C1)
- German (C1)
- Russian (Native)
- Javascript
- PHP
- Golang
- Rust
- Python
- C/C++

Skills:
- Penetration Testing
- Reconnaissance
- Exploit Writing
- Threat Modeling
- SAST
- Methodology Writing
- Risk Mitigation
- Network Security
- Team Leading
- Blackbox/Whitebox Testing
- Security Assessments of AWS, AD, Azure, etc.

EXPERIENCE

Security Engineer, Mayflower — Jan, 2025-Present

- Conduct penetration testing of in-house and open-source systems to identify and mitigate vulnerabilities before exploitation by third parties.
- Perform static (SAST) and dynamic (DAST) analysis; validate automated findings through manual source code review and proof-of-concept exploit development.
- Triage and validate bug bounty submissions; assess severity, reproduce vulnerabilities, and collaborate with development teams to implement effective fixes.
- Research and assess open-source technologies in use, identifying potential security weaknesses and recommending secure configurations or alternatives.
- Provide security guidance and best-practice recommendations to cross-functional teams, tailoring mitigations to specific architectures and business needs.
- Conducted threat modeling and risk assessments for high-impact services, ensuring security requirements were considered during early design stages.
- Strengthened company-wide security awareness by sharing best practices and guiding developers through secure coding workshops.

As a Security Engineer at Mayflower, a service provider supporting diverse client organizations, I delivered comprehensive cybersecurity solutions tailored to varying business environments. My primary focus was on penetration testing across a broad range of projects and conducting static code analysis (SAST) to identify and mitigate threats before deployment. Leveraging my background as a software developer, I was able to rapidly understand complex systems and pivot my research to uncover hidden attack vectors. I also developed custom exploits to validate findings, ensuring products were secured against even edge-case scenarios.

Cybersecurity Researcher, Hackerone — 2022-2025

- Performed end-to-end penetration tests on web and mobile applications, from reconnaissance to exploitation and reporting, in alignment with OWASP methodologies
- Specialized in Web Application and Mobile Application security assessments, identifying vulnerabilities such as XSS, IDOR, SSRF, SQLi, and insecure storage
- Conducted reconnaissance and network monitoring to discover hidden attack surfaces, misconfigurations, and exposed assets across target infrastructures
- Delivered comprehensive vulnerability reports with reproducible proofs of concept, clear risk assessments, and actionable remediation steps for engineering teams
- Collaborated with bug bounty platforms like HackerOne, contributing to global security awareness and strengthening organizational security posture
- Applied advanced manual testing techniques beyond automated tools to uncover

complex, business-logic flaws not detected by scanners
- Actively researched new attack vectors and emerging security threats, applying cutting-edge exploitation methods to real-world systems

As a cybersecurity researcher I was conducting penetration tests in different products that were hosting their bug bounty programs at HackerOne. My interests during this time were mainly focused on Web-App penetration testing, Mobile Application penetration testing, Reconnaissance, Network monitoring and recon. I've conducted multiple penetration tests from recon to complete report on the infrastructure of the product, implementing methodologies that are aligned with OWASP guidelines. My impact to the industry made several companies more aware of their security situation and helped them enhance in fields they were lacking.

Lead Software Engineer, CIPHER LLC; USA — 2017-2022

- Led and mentored a cross-functional team of 5 software developers, fostering a strong security-first engineering culture
- Introduced Secure Software Development Life Cycle (SSDLC) methodology to standardize secure coding practices across all projects
- Designed and implemented CI/CD pipelines with integrated security gates, enabling automated testing and secure deployments
- Conducted regular SAST (Static Application Security Testing) and manual code reviews to identify and mitigate vulnerabilities early in the lifecycle
- Researched and integrated P2P networking protocols and TOR for privacy-preserving mobile communication
- Established internal R&D processes, leading investigations into novel cryptographic protocols, secure communication standards, and network hardening techniques
- Implemented threat modeling and risk assessment for new features, ensuring security considerations were embedded in design phases
- Championed secure coding guidelines and trained the team on OWASP standards, reducing security-related bugs in production
- Collaborated with product and business stakeholders to balance user privacy requirements with system performance and scalability

During my time at CIPHER I was tasked with leading a development and R&D departments, creating a privacy-oriented solution for mobile communications over p2p networks. I have conducted researches in fields of cybersecurity, network security, protocol communication, TOR adaptation and integration. My experience at CIPHER was deeply focused on securing the code, implementing best practices in both development and production. I was conducting regular SAST and CI/CD code and workflow analysis, ensuring the solutions provided by the company are robust and secure.

ABOUT ME

I'm a passionate programmer and cybersecurity professional with a strong foundation in privacy, secure software development, and ethical hacking. With almost a decade of experience in software engineering and several years in cybersecurity, my focus has always been on building secure, resilient, and privacy-preserving systems.

Throughout my career, I've held roles ranging from backend developer to team lead, where I was responsible for planning, task management, and delivering secure, high-quality products. This hands-on leadership experience sharpened my ability to translate security principles into practical development workflows.

I thrive on tackling complex security challenges and excel at communicating findings in a clear, actionable manner to both technical and non-technical stakeholders. Outside of work, I actively participate in bug bounty platforms to stay sharp and continuously evolve alongside the threat landscape.

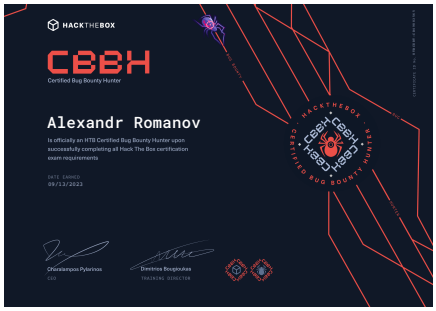
EDUCATION

University of Wollongong, Australia — BCompSc (Cybersecurity), 2025

Graduated with a strong focus on cybersecurity, network defense, and secure software development. Led multiple student projects, including the design and implementation of a custom IDS/IPS. Gained hands-on experience in threat detection, system hardening, and team leadership through collaborative, real-world-inspired challenges.

CERTIFICATIONS

Certified Bug Bounty Hunter (CBBH) @ HTB — 2023



Certified Web Exploitation Specialist (CWES) @ HTB — 2023

CompTIA Security+ @ CompTIA — 2025