Antonio Rocco Spataro

Summary

Penetration Tester & Bug Bounty Hunter with 5+ years of experience specializing in web application security and vulnerability research. Proven track record of identifying critical vulnerabilities, contributing to CVEs, and achieving top rankings in Bug Bounty programs. Passionate about offensive security and continuous learning.

Education

2017–2021 **Bachelor's Computer Science degree**, *Università della Calabria*, Rende (CS)
Graduated in April 2021 at University of Calabria

2022– **Master's Cyber Security degree**, *Università della Calabria*, Rende (CS)

Experience

2021– **Security Researcher**, *Full Remote*
Independent Security Researcher for private companies and Bug Bounty Hunter in various platforms including Hackerone, Intigriti, Cyberdart, Yeswehack, Bugcrowd, Hackenproof

2022– **Ethiack**, *Full Remote*
Penetration tester - Ethiack ethical hacker team

2024– **Unlock Security**, *Full Remote*
Penetration tester - Unlock ethical hacker team

2025– **Cyberdart**, *Full Remote*, Head of Triager
Led triage of bug bounty reports, ensuring accurate validation and prioritization. Acted as main contact for researchers and clients, while mentoring junior triagers and improving internal workflows

Skills

- Knowledge of information security frameworks and standards.
- Application development using Java, C++, Python, PHP, Perl, Autoit, HTML, Javascript, MySQL, SQL, PostgreSQL, ecc.
- Strong technical ability in security related architecture design and assessment (manual approach to penetration testing).
- Strong technical ability in current application and infrastructure testing methodologies.
- Strong attention to detail in conducting analysis combined with an ability to accurately record full documentation in support of their work

via crucicella n7 – 89025 – Rosarno, Italia
antonioroccospataro@gmail.com • *antoniospataro.github.io*
antoniospataro • *antonio-rocco-spataro-9007a6175*

Some Cyber Security achievements

2024 **CVE-2024-47873** - XXE via regex bypass by using UCS-4 and encoding guessing in PHPSpreadSheet

2025 **CVE-2025-5062** - Blind XSS leads to becoming Admin with full privileges on every website developed with Wordpress-Woocommerce (CVE Requested, fixed in the version 9.4.3)

2024 **CVE-2024-48917** - XXE in the new version by using a payload in the encoding UTF-7, and adding at end of the file a comment with the value encoding="UTF-8" to match the wrong regex in the code

2024 **CVE-2024-21627** - Bypassing the Validate::isCleanHTML method leads to obtaining XSS in every input sanitized with that method in PrestaShop CMS

2024 Binance Bug Bounty program top 10 researchers, reporting various critical vulnerabilities to their program

2023 Reported two O-Click Account Takeover in Booking bug bounty program.

2023 Reported a sensitive IDOR vulnerability to create infinite coupon in Dell Bug bounty program.

2022 **CVE-2022-4105** - Markup injection to Stored XSS in KiwiTCMS library leads to account takeover and exploitation of various endpoints. Possibility of wormable XSS to broke the system.

2023 **CVE-2023-27489** - Another Stored XSS in KiwiTCMS.

2023 **CVE-2023-32686** - Stored XSS with weak WAF and CSP bypass in KiwiTCMS

2021-2025 Reported Many other critical vulnerabilities in various companies and bug bounty brograms subject to non disclosure agreement

Projects

2021-2023 **antoniospataro.github.io** - My personal Blog about cybersecurity, where I share interesting vulnerabilities found during my work and solutions to ctf challenge

2020 Pokemon Blue Battle AI (for US Pokemon Blue) using Answer Set Programming system, based on disjunctive logic programming, and a mod for SameBoy GB emulator in C/C++ (for personal satisfaction)

2021-2025 Script and tool for automation recon and automation vulnerability in penetration testing and Bug Bounty.

Languages

Languages Proficient in English and native Italian speaker

via crucicella n7 – 89025 – Rosarno, Italia
antonioroccospataro@gmail.com • *antoniospataro.github.io*
antoniospataro • *antonio-rocco-spataro-9007a6175*