Antonio Rocco Spataro

Education

2012–2017 **Maturità Scientifica**, *Liceo Scientifico R. Piria*, Rosarno (RC)
Graduated from high school in 2017 at Liceo Scientifico R. Piria

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, Bugcrowd and Google

2022– **Ethiack**, *Full Remote*
Member of the Ethiack ethical hacker team

Skills

- Knowledge of information security frameworks and standards.
- Application development using Java, C++, Python, PHP, Perl, Autoit, HTML, Javascript, MySQL, SQL, PostgreSQL, Answer Set Programming (DLV2).
- 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

Some Cyber Security achievements

2023 Reported O-Click Mass Account Takeover in Binance bug bounty program.

2023 Reported O-Click Mass 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.

via crucicella n7 – 89025 – Rosarno, Italia

(+39) 329 035 1118 • antonioroccospataro@gmail.com
antoniospataro.github.io • antoniospataro
in antonio-rocco-spataro-9007a6175

2023	**CVE-2023-27489** - Another Stored XSS in KiwiTCMS.
2023	**CVE-2023-32686** - Stored XSS with weak WAF and CSP bypass in KiwiTCMS
2021	Top 10 hacker in a famous cryptocurrency website with Private Bug Bounty Hall of Fame subject to non disclosure agreement
2021	Telecom Italia's Responsible Disclosure Hall of Fame
2022	Reported a sensitive IDOR vulnerability to see single pages of paid books in Studocu Bug bounty program and wrote a script in python to steal books entirely in pdf format
2022	Reported Incorrect link sanitization in dashboards comments leads to clickjacking (HTML Injection/UI Redressing vuln) vulnerability in EazyBI bug bounty program
2022	Reported business logic vulnerability in E-Commerce that allows you to buy thousands of products with a corrupt low price (it was possible also negative) in the context of a bug bounty program subject to non disclosure agreement.
2022	Reported Reflected XSS vulnerability bypassing the WAF leading to ATO in the context of a bug bounty program subject to non disclosure agreement.
2022	Reported chain of vuln: HTML Injection to Internal SSRF in the context of a bug bounty program subject to non disclosure agreement.
2023	Reported Pin Bypass in an Android Application via deeplink and weak regex in the context of a bug bounty program 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)
2021-2023	Script and tool for automation recon and automation vulnerability in penetration testing and Bug Bounty.

Certificates

2021	CyberChallenge.IT Local Contest
2021	CyberChallenge.IT National Contest

Languages

mother tongue	Italiano
B1	English

If you are interested in seeing a more complete resume **Look Here**.