



# 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

## Certificates

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

## Languages

mother tongue Italiano

B1 English

## 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

via crucicella n7 – 89025 – Rosarno, Italia

☎ (+39) 329 035 1118 • ✉ antonioroccospataro@gmail.com

📄 antoniospataro.github.io • 🌐 antoniospataro

📌 antonio-rocco-spataro-9007a6175

---

## Main 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.
- 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
- 2021-2023 Many other Private Bug Bounty Hall of Fame subject to non disclosure agreement

---

## Projects

- 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)
- 2021-2022 Script and tool for automation recon and automation vulnerability in penetration testing and Bug Bounty.

---

## Cyber Security

- 2012 I found and reported my first vulnerability in altervista.org (Stored XSS)
- 2021 I partecipate in CyberChallenge local finals (a Jeopardy capture the flag) getting the sixth position.
- 2021 I partecipate in CyberChallenge national finals (Attack and Defense ctf).
- 2021 Reported a domain takeover vulnerability in Acronis bug bounty program.
- 2021 Reported a domain takeover vulnerability in the context of a bug bounty program subject to non disclosure agreement.
- 2021 Reported Reflected XSS vulnerability in the context of a bug bounty program subject to non disclosure agreement.
- 2021 Reported sensitive data leak IDOR vulnerability in the context of a bug bounty program subject to non disclosure agreement.
- 2021 Reported Security Misconfiguration vulnerability in TIM Group vulnerability disclosure program.
- 2021 Reported missing rate limit in current password change settings leads to Account takeover in the context of a bug bounty program subject to non disclosure agreement.
- 2021 Reported Reflected XSS vulnerability in the context of a bug bounty program subject to non disclosure agreement.

*via crucicella n7 – 89025 – Rosarno, Italia*

☎ (+39) 329 035 1118 • ✉ [antonioroccospataro@gmail.com](mailto:antonioroccospataro@gmail.com)

📄 [antoniospataro.github.io](https://antoniospataro.github.io) • 🌐 [antoniospataro](https://antoniospataro.com)

📄 [antonio-rocco-spataro-9007a6175](https://antonio-rocco-spataro-9007a6175.github.io)

- 2022 Reported business logic vulnerability in Ubiquiti Inc. Bug bounty program
- 2022 Found business logic vulnerability that allows you to access a cloud administration panel in the context of a bug bounty program subject to non disclosure agreement
- 2022 Reported missing rate limit leads to ATO in the context of a bug bounty program subject to non disclosure agreement.
- 2022 Reported business logic vulnerability lead to ATO and mail flooding in the context of a bug bounty program subject to non disclosure agreement.
- 2022 Reported sensitive data leak IDOR vulnerability lead to disable other account in the context of a bug bounty program subject to non disclosure agreement.
- 2022 Reported sensitive data leak IDOR vulnerability lead to disclose information about private registered companies in the context of a bug bounty program subject to non disclosure agreement.
- 2022 Reported sensitive data leak IDOR vulnerability lead to disclose private information of users in the context of a bug bounty program subject to non disclosure agreement.
- 2022 Reported business logic vulnerability that allows you to access a cloud administration panel in the context of a vulnerability disclosure program subject to non disclosure agreement
- 2022 Reported sensitive data leak IDOR vulnerability lead to download private data of other users in the context of a bug bounty program subject to non disclosure agreement.
- 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 Logic business bug in forgot password leading to ATO in the context of a bug bounty program subject to non disclosure agreement.
- 2022 Reported TOCTOU vulnerability in a principal feature in the context of a bug bounty program subject to non disclosure agreement.
- 2022 Reported sensitive data leak IDOR vulnerability lead to view private photo and video of other users in the context of a bug bounty program subject to non disclosure agreement.
- 2022 Reported sensitive data leak IDOR vulnerability in email verification bypass leads to account takeover and account corruption of other user in the context of a bug bounty program subject to non disclosure agreement.
- 2022 Reported data leak IDOR vulnerability in share endpoint leads to view private data of other user 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.
- 2022 Reported Incorrect link sanitization in dashboards comments leads to clickjacking (HTML Injection/UI Redressing vuln) vulnerability in EazyBI bug bounty program

*via crucicella n7 – 89025 – Rosarno, Italia*

☎ (+39) 329 035 1118 • ✉ [antonioroccospataro@gmail.com](mailto:antonioroccospataro@gmail.com)

📄 [antoniospataro.github.io](https://github.com/antoniospataro) • 🌐 [antoniospataro](https://antoniospataro.com)

📄 [antonio-rocco-spataro-9007a6175](https://antonio-rocco-spataro-9007a6175.github.io)

- 2022 Reported sensitive data leak IDOR vulnerability leads to disclose private data of users in the context of a bug bounty program subject to non disclosure agreement.
- 2022 Reported sensitive SSRF vulnerability (SSRF attacks against the server itself) leads to use various API endpoint without admin permission in the context of a bug bounty program subject to non disclosure agreement.
- 2022 Reported sensitive data leak IDOR vulnerability leads to disclose private data of users in the context of a bug bounty program subject to non disclosure agreement.
- 2022 Reported sensitive IDOR vulnerability in email verification bypass leads to account takeover in the context of a bug bounty program subject to non disclosure agreement.
- 2022 Reported another sensitive IDOR vulnerability in email verification bypass in the context of a bug bounty program subject to non disclosure agreement.
- 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 stored XSS in KiwiTCMS library leads to account takeover and exploitation of various endpoints. Possibility of wormable XSS to broke the system. - CVE-2022-4105
- 2023 Reported Race Condition vulnerability (TOCTOU vuln) leads to using a free feature without limitation as if it were a premium account 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.
- 2023 Reported another stored XSS in KiwiTCMS - CVE-2023-27489
- 2023 Reported sensitive IDOR vulnerability leads to generate Infinite Coupons in E-Commerce in the context of a bug bounty program subject to non disclosure agreement.
- 2023 Reported Reflected XSS vulnerability in Ford Vulnerability disclosure program
- 2023 Reported Stored XSS with weak WAF and CSP bypass in KiwiTCMS - CVE-2023-32686
- 2023 Reported 3 Stored XSS vulnerability with privilege escalation leads to Financial Loss (third-party dependency) in the context of 3 bug bounty program subject to non disclosure agreement.
- 2023 Reported a sensitive IDOR vulnerability to create infinite coupon in Dell Bug bounty program.
- 2023 Reported O-Click Mass Account Takeover in Booking bug bounty program.
- 2023 Reported O-Click Mass Account Takeover in Binance bug bounty program.
- 2021-2023 I enjoy playing in hacking and pentesting competitions (weekly CTF, TryHackMe, HackTheBox and other)

*via crucicella n7 – 89025 – Rosarno, Italia*

☎ (+39) 329 035 1118 • ✉ [antonioroccospataro@gmail.com](mailto:antonioroccospataro@gmail.com)

📄 [antoniospataro.github.io](https://github.com/antoniospataro) • 🌐 [antoniospataro](https://antoniospataro.com)

📌 [antonio-rocco-spataro-9007a6175](https://antonio-rocco-spataro-9007a6175)