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

Certificates

2017 Giovani e futuro comune business competition

2021 CyberChallenge.IT Local Contest

2021 CyberChallenge.IT National Contest

Languages

mother tongue Italiano

B1 English

Cyber Security

2012 I found and reported my first vulnerability in altervista.org (Stored XSS)

2021 I partecipated in CyberChallenge local finals (a Jeopardy capture the flag) getting the sixth position.

2021 I partecipated 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.

via crucicella n7 – 89025 – Rosarno, Italia
(+39) 329 035 1118 • *antonioroccospataro@gmail.com*
antoniospataro.github.io • *antoniospataro*
antonio-rocco-spataro-9007a6175

2021 Reported Reflected XSS vulnerability in the context of a bug bounty program subject to non disclosure agreement.

2022 Reported business logic vulnerability in Ubiquiti Inc.

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.

via crucicella n7 – 89025 – Rosarno, Italia
(+39) 329 035 1118 • antonioroccospataro@gmail.com
antoniospataro.github.io • antoniospataro
antonio-rocco-spataro-9007a6175

2021-2022 I enjoy playing in hacking and pentesting competitions (weekly CTF, TryHackMe, HackTheBox and other)

Projects

2019 Donkey Kong replica written in C++ using Allegro Game Library 5.0 (OOP exam; team working with a colleague)

2019 Pokemon mini-game written in Java using LibGDX game library ("Graphic Interfaces and Event Programming" exam; team working with a collegue)

2019 European Researchers Night, showcase of my game projects at University of Calabria

2020 IoT e-commerce demo powered by Bootstrap and Java servlets ("Web Computing and Software Engineering" exam; team working with collegues)

2020 AI for Five Card Draw poker powered by Answer Set Programming (DLV2; AI exam)

2020 Pokemon Blue Battle AI (for US Pokemon Blue) and mod for SameBoy GB emulator in C/C++ (for personal satisfaction)

Computer skills

Coding: Java, C++, Python, Perl, Autoit, Answer Set Programming (DLV2)

OS–Shells: Windows, Linux (bash, zsh, tmux)

Web: HTML, JSON, JavaScript, PHP

Tools: Git, Gradle

Database: MySQL, Postgres

Libs, Other: Design Pattern GOF, MVC,JUnit, LibGDX, Allegro Game Library

via crucicella n7 – 89025 – Rosarno, Italia
(+39) 329 035 1118 • *antonioroccospataro@gmail.com*
antoniospataro.github.io • *antoniospataro*
antonio-rocco-spataro-9007a6175