



João Maria Campos Donato

📍 **Home** : Coimbra, Portugal

✉ **Email**: joaomariadonato@gmail.com

Date of birth: 2002 **Nationality**: Portuguese

WORK EXPERIENCE

Gray Swan AI

City: Remote | **Country**: United States

[2025 – Current] **Arena Engineer - Contract**

<https://www.grayswan.ai/>

CISUC (AI-SSD)

City: Coimbra | **Country**: Portugal

[06/2025 – 09/2025] **AI Security Researcher**

<https://ai-ssd.github.io/>

IToWin

City: Coimbra | **Country**: Portugal

Software developer

<https://www.ipn.pt/incubadora/empresa/399>

EDUCATION AND TRAINING

[2020 – 2023] **Bachelor's Degree in Informatics Engineering**

Universidade de Coimbra <https://www.uc.pt/en/fctuc/dei/education/bachelors/lei/>

City: Coimbra | **Country**: Portugal |

[2023 – 2025] **Master's Degree in Informatics Security**

University of Coimbra <https://www.uc.pt/en/fctuc/dei/education/masters/msi/>

City: Coimbra | **Country**: Portugal |

LANGUAGE SKILLS

Mother tongue(s): Portuguese

Other language(s):

English

LISTENING C1 **READING** B2 **WRITING** B2

SPOKEN PRODUCTION B2 **SPOKEN INTERACTION** B2

Levels: A1 and A2: Basic user; B1 and B2: Independent user; C1 and C2: Proficient user

PROJECTS

QueueR

Queue virtualization web app with no collection of user data.

2nd place at "Shift Appens" 2023

Link: <https://taikai.network/shift-appens/hackathons/shiftappens2023/projects/clgi4zsi358241001yk8ii84wlq/idea>

AI-SSD Website

Developed the website for the AI-SDD research group at my University.

Link: <https://ai-ssd.github.io/>

hotlapmode.app

Helped develop a website for f1 driver/team comparisons.

Link to website: <https://www.hotlapmode.app/>

Link to repository: <https://github.com/jose-donato/hotlapmode.app>

CONFERENCES AND SEMINARS

[2025] Short paper presented at the 20th European Dependable Computing Conference (EDCC) Student Forum

Lisbon

The short paper was titled: "Benchmarking LLM Robustness Against Prompt-based Adversarial Attacks"

Link: https://joaodonato.pages.dev/blog/edcc_2025/

COMPETITIONS

[2025] 6th place at Gray Swan AI's Agent Red-Teaming Arena

Ranked 6th in an AI security competition with 2000+ global participants earning over \$7000 in prizes.

Link: <https://app.grayswan.ai/arena/challenge/agent-red-teaming/leaderboard?tab=1>

[2025] 3rd place at LLMail-Inject: Adaptive Prompt Injection Challenge

Got 3rd place with my team RainaResearch, in the LLMail-Inject challenge, a competition at bypassing prompt injection defenses in a simulated LLM-integrated email client. Collectively winning \$1000 in prizes and the opportunity of being featured in the paper: <https://openreview.net/pdf?id=FhXoETzdfs>.

Link: <https://llmailinject.azurewebsites.net/>.

[2024] 3rd place at SplxAI's Christmas CTF

Got 3rd place in the SplxAI's Christmas CTF, a competition at bypassing prompt injection defenses by extracting a secret from the LLM.

Link: https://www.linkedin.com/posts/splx-ai_airedteaming-splxai-christmasctf-activity-7272911071059849216-Eydk/

[2023] 2nd place at ShiftAppens 2023

Secured second place with my team at the ShiftAppens 2023 hackathon with the queueR project, a tool for helping manage queues.

Link: <https://taikai.network/shift-appens/hackathons/shiftappens2023/projects/clgi4zsi358241001yk8ii84wlq/idea>