

# Felix Billieres

## Offensive Security Researcher

Paris, France | [felix.billieres@ecole2600.com](mailto:felix.billieres@ecole2600.com)

GitHub: [felixbillieres](#) | LinkedIn: [felix-billieres](#) | HackTheBox: ElliotBelt | RootMe: Elliot\_Belt

## Professional Experience

### Purple Teamer

*Confidential*

September 2025 - Present

Paris, France

- Purple Team operations combining offensive and defensive security

- Security assessment, penetration testing, threat hunting, and incident response

### Pentester

*Galeries Lafayette*

September 2024 - September 2025

Paris, France

- Vulnerability identification, web services and Active Directory hardening supervision

- Blue Team training on advanced AD attacks, security assessment and penetration testing

### Analyste SOC N1 & N2

*ITrust*

September 2023 - September 2024

Toulouse & Paris, France

- SOC Analyst Level 1 & 2 with Blue Team & Red Team skill development

- Log analysis, incident report writing, pentest seminars, and internal penetration testing

## Education

### 4th Year Cybersecurity Student

2022 - 2026

*École 2600, Paris, France* - Specializing in offensive security with strong foundations from CTF competitions with Phreaks 2600

## Certifications & Achievements

### 2025

- **CRT0 Training Modules** - Zero-Point Security (Dec)
- **Mythical Mini Pro Lab** - HackTheBox (Dec)
- **Rastalabs Prolab** - HackTheBox (Oct)
- **CWES** - HackTheBox (Sept)
- **Zephyr Prolab** - HackTheBox (Aug)

### 2024

- **PNPT** - TCM Security (Nov)
- **Attacking & Defending AD** - Altered Security (Jun)

## Platform Statistics

- **HackTheBox**: 70+ machines
- **OffSec**: 60+ machines
- **RootMe**: 4000+ points
- **PortSwigger**: 60%+ completion

## Community Involvement

### Phreaks 2600 - Board Member

Project management, CTF creator (Web, Forensics, Pwn), workshop developer for advanced training labs.

### The Hacker Recipes - Contributor

[thehacker.recipes](https://thehacker.recipes) - Contributing to AD exploitation, web security, and pentest documentation.

### Bug Bounty Hunter

Active vulnerability research and reporting across various programs.

## Open Source Projects

### **AuditMapper v2** - [GitHub](#)

Security assessment suite presented at WineRump Bordeaux. Host management, AD mindmap renderer, config generators, Kanban & time tracking.

### **Exegol MCP** - [GitHub](#)

Model Context Protocol integration for Exegol. Custom pentest tools for reconnaissance, AD, and web security.

### **pySIDHistory** - [GitHub](#)

Python tool for SID History manipulation in Active Directory from Linux hosts.

### **pyGoldenGMSA** - [GitHub](#)

Python tool for gMSA exploitation in Active Directory.

## Technical Skills

**Specializations:** Active Directory Exploitation, Web Application Security, Bug Bounty Hunting, Red Team Operations

**Tools:** Cobalt Strike, BloodHound, Impacket, Burp Suite, Metasploit, NetExec

**Programming:** Python, PowerShell, Bash, JavaScript, TypeScript

**Platforms:** Linux, Windows, Active Directory, Cloud Security (AWS, Azure)

**Languages:** French (Native), English (Fluent)