contact@yann.cam

+33 6 XX XX XX XX (email first)

RENNES, FRANCE, *Remote*

https://yann.cam

FORMATIONS

2009-2012 - **Polytech'Nantes I Engineer**
Engineer's degree in Computer Systems, Software, Networks and Security - Polytechnic School of the University of Nantes (Polytech'Nantes) 44000

2007-2009 – **University Diploma**
University Diploma in Computer Technology - University Institute of Technology of Nantes 44000

ACKNOWLEDGEMENTS

Google, Microsoft, Mozilla, Fortinet, eBay, Oracle, United Nations, NASA, EFF, CERN, Java, Synology, Cisco, CERT-EU, Hack4Values, redhat

Yann CAM (ycam)

ETHICAL HACKER / CYBERSECURITY CONSULTANT

AUDITOR / PENTESTER / TRAINER

« *Passionate about **CyberSecurity** and practising in this field since the early 2000s with **more than 15 years** of professional experience, I now work as an **Ethical Hacker** within the company **BZHunt**, as well as an **independent consultant, trainer and auditor** of information systems.*
*These experiences have allowed me to contribute to the security of **several hundred companies** through **audits** or **Bug Bounty** services, as well as to provide **training** to students (schools of engineers / company employees).* »

PROFESSIONAL EXPERIENCES

ETHICAL HACKER / CYBERSECURITY ENGINEER (PART-TIME) — 2024+
BZHUNT – BREST/RENNES, FRANCE, *Remote*

BZHunt is the **1st French company to participate in BugBounty competitions (LHE)**, where its ethical hackers have made their passion a profession!

- **Ethical Hacker / Cybersecurity Auditor:** performing offensive audits of intrusion tests (pentest) / Red Team (LAN/WAN, black/grey/white box) for web, mobile, thick client, LAN/DMZ/Wifi, Active Directory ecosystem targets…
- **Bug Hunter:** *Live Hacking Event* (LHE) and bug hunter on Bug Bounty platforms.

INDEPENDENT CYBERSECURITY CONSULTANT (PART-TIME) — 2018+
RENNES, FRANCE, *Remote*

With my past experiences and with versatility in the fields of CyberSecurity, I also work as a **Consultant Auditor** and **Independent Trainer**.

- **CyberSecurity auditor:** performing offensive penetration test audits (internal/external, black/grey/white box, OSINT) and configuration for web, mobile, heavy-client, LAN/DMZ/Wifi, Active Directory ecosystem, industrial (OT/IT) …
- **CyberSecurity trainer:** course of training (from 1 to 5 days) in awareness or offensive expertise accompanied by practical work in the form of riddles / challenges / CTFs.
- **Bug Hunter:** vulnerability hunter on Bug Bounty platforms.

SENIOR CYBERSECURITY CONSULTANT — 2012-2022
SYNETIS – RENNES, FRANCE

Leader of independent consulting firms in French Cybersecurity, SYNETIS offers a 360° service in the various areas of information system security: Governance, Risk, Compliance of authorizations, Identity and access management, Operational security, Audit (PASSI), SoC, CSIRT/CERT.
Senior CyberSecurity Consultant: Lead-Tech / Audit Manager / Trainer (2019-2022)

- Orchestration, follow-up and realization of technical audits of intrusion tests, architecture, configuration, source code, RedTeam, phishing, industrial, cryptanalysis & training.

Confirmed CyberSecurity Consultant: Pentester / Lead-Auditor / Analyst (2014-2019)

- Internal/external security audits, web, mobiles, heavy-clients, source codes, LAN, DMZ, wifi, infrastructure, Active Directory, etc. and post-incident forensic interventions.

CyberSecurity Consultant: Technical Expert / Security Architect (2012-2014)

- Expertise and integration of IAM solutions, SSO, MFA, DLP, centralized encryption, federation, SIEM, authorization compliance, password management, directories, etc.

TRAINER / TEMPORARY TEACHER - OFFENSIVE SECURITY — 2016+
POLYTECHNIC SCHOOL OF THE UNIVERSITY OF NANTES – FRANCE

Punctual and recurrent training and awareness-raising interventions in Offensive Security with **5th year students** (BAC+5) of the Computer Engineering cycle. Development and presentation of **Lectures**, animation and follow-up of **Practical Work** in the form of challenges / riddles / security CTF.

YANN CAM / HTTPS://YANN.CAM / CONTACT@YANN.CAM

ACCOMPLISHMENTS

MISC n°133 (2024)
JS Hoisting : exploit « unexploitable » XSS

MISC n°128 (2023)
Shuck Hash before trying to Crack it

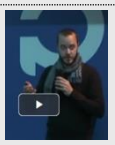
MISC n°125 (2023)
DisseXSSion of a generic payload

JavaScript for Hackers (2022)
Mention in the credits of Gareth Heyes' book

Interview Télégramme (2022)
Offensive security: Manipulative and blameless

Interview ZDNet (2020)
Bug bounty, can we live from it?

Conference Min2Rien (2018)
Adopt strong authentication!



Interview of Bug Bounty Yogosha platform (2018)

MISC n°98 (2018)
Web authN & Password reset / Strong Authentication (MFA) overview

MISC n°94 (2017)
pfSense : obtaining a root reverse-shell via an XSS

MISC n°89 (2017)
UnSHc: Decrypt shell scripts protected by SHc

GSMag n°34 (2016)
DarkWeb : Anti-indexing and camouflage techniques

The Browser Hacker's Handbook (2015)
Quotations from personal works in the book

PROFESSIONAL SKILLS

CyberSecurity:

- Seduced by the Bug Bounty model, while carrying out penetration testing missions, redteam, forensic, awareness (phishing / USB-dropping / training), I do intensive monitoring (MSF, BeEF, Kali, fuff, Sulley, Nessus, Responder, Burp, Hashcat, BloodHound…).

Pedagogy & writing:

- With a strong attraction for teaching and knowledge sharing, I give particular importance to the editorial quality of deliverables, to restitution speeches (managerial / technical) and to popularization / awareness through illustration.

Hardening & configuration:

- Following a constant security hardening approach, supported by recognized standards such as the CIS / ANSSI, I perform configuration audits for a multitude of technologies (Windows/Linux OS, web services, DBMS, software packages, VPN, firewall, etc.).

Development / Scripting:

- Bash, Powershell, Python, PHP, Ruby, Go, Java, C/C++… with very good bases in many languages, I adapt in a versatile way to various developments for the realization of source code audits and the search for vulnerabilities.

Identity & Access Management:

- My experiences led me to deploy, manipulate, compare and audit security software solutions such as PingIdentity, ForgeRock, Apereo, PWM, Prim'X, Brainwave, LDAP, Symantec, ILEX, OIM, Wallix, O365, GSuite, etc. allowing me to provide advice to clients.

Advisories & CVEs:

Development of exploits, PoC, tools, articles and vulnerability analyses:

- Jirafeau one-click-filesharing PHP project Stored-XSS (CVE-2024-12326, CVE-2025-7066)
- Stormshield Network Security firewalls Stored-XSS (CVE-2024-31946)
- pfSense 2.0.1 then 2.3.2 Remote root Command Execution (RCE)
- IPFire < 2.19 Update Core 101 XSS to CSRF to Remote Command Execution (RCE)
- IPCop 2.1.5 XSS and RCE (CVE-2013-7417, CVE-2013-7418)
- Smoothwall Express 3.1 (CVE-2014-9429, CVE-2014-9430, CVE-2014-9431)
- ZeroShell <=2.0.RC2 Local File Disclosure to Remote Command Execution (RCE)
- m0n0wall 1.33 CSRF to Remote root Command Execution (RCE)

Extra-professional activities:

- Active participation on Bug Bounty platforms (YogoSha, YesWeHack, BugCrowd), LHE/CTF/Wargame events and challenges (root-me : ycam).
- Circus arts: juggling (clubs, balls, rings), bolas, unicycle, contact ball.