

Chanin Kim

lourcode@gmail.com | github.com/lourc0d3 | lourcode.kr

Updated : 2026.04.26

EDUCATION

Soonchunhyang University

Undergraduate Student

B.S. in Cybersecurity, GPA 3.55/4.5

Asan, South Korea

March 2022 – March 2027

Korea Game Science High School

High School, Graduated

Major in Computer Game Development

Wanju, South Korea

March 2019 – February 2022

Work EXPERIENCE

Research Team, ENKI Whitehat

Offensive Researcher

- Focused on iOS security research

Seoul, South Korea

September 2024 – present

Unreal (Offensive Research Team) , S2W Inc

Research Intern

- Developed an automated system for vulnerability detection in binary patching using IR and static analysis (based on BinaryNinja IR)
- N-day research & exploit developed

Seoul, South Korea

March 2024 – August 2024

HONORS & AWARD

- Finalist, DEF CON 33 | Team ColdFusion September 2025
- 2024 Synology Hall of Fame December 2024
- 4th place, WooriCon (Woori Bank Mock Hacking Competition) September 2024
- 2023 Synology Hall of Fame December 2023
- 4th place, KOSTA Mock Hacking Competition (한국교통신안전공단) December 2023
- 1st place, Chungcheong Cyber Security Competition November 2023
- Korea Convergence Security Society Fall Conference Outstanding Paper Award November 2023
- 5th place, Patchstack Monthly Bug Bounty April 2023

PUBLICATIONS

- Yeontae Ji, **Chanin Kim**, Seunghyeok Choi, Wochan Cha, Yusik Lee, CISC-W 2025 (한국정보보호학회), “Binary Static Analysis and Automatic Vulnerability Patch Detection System Using Intermediate Representation and LLM”
- Chaeyoung Kim, Minyoung Park, Arim Han, Jin Lee, Hoonhee Lee, Junwon Heo, **Chanin Kim**, Changseon Lee, and Gyeonggon Kim, CISC-W 2024 (한국정보보호학회), “A Study on Privacy Threats to LTE-Based Telephone Transmissions by Autonomous Robots”
- Chaeyoung Kim, Jin Lee, Hunhui Lee, Junwon Heo, Minyoung Park, Alim Han, **Chanin Kim**, Kyounggon Kim, Autumn Annual Conference of IEIE 2024 (대한전자공학회), “Security Requirements Derivation for Indoor Autonomous Driving Robots Based on STRIDE”
- Yu-Kyung Lee, **Chanin Kim**, Myeong-hun Pak, Myeong-jin Shin, Kangmin Yang and Minsu Kim, 2023 Korean Convergence Security Society Fall Conference (한국융합보안학회), "A Study on Bypassing Bootloader Security Techniques in Embedded Devices through Side-Channel Attacks"

EXTRACURRICULAR ACTIVITIES

FIESTA 2025 CTF Operation

Authored Forensics Challenges

Seoul, South Korea

Sep 2025

Codegate 2025 CTF Operation <i>Authored Pwnable Challenges</i>	Seoul, South Korea Mar 2025
CCE 2025 CTF Operation <i>Authored Pwnable Challenges</i>	Seoul, South Korea Jul 2025
Best of The Best @KITRI <i>12th. Vulnerability Analysis Track Trainee / Whitehat 10</i> Project Manager : “NVR Vulnerability Analysis”	Seoul, South Korea July 2023 – March 2024
TOOR @ TeamH4C <i>Member of Offensive Research group</i>	Asan, South Korea March 2022 – Present
K-Shied Jr. @ KISA <i>4th Security Incident Analysis and Response Track Trainee</i> Development lightweight WIPS using Raspberry Pi	Seoul, South Korea May 2020 – June 2020

TALKS & SPEECH

Invited Talk – Embedded Hacking Expert Lecturer, KISA <i>Lectures from UART connection to 0day hunting</i>	Naju, South Korea Sep 2025
CODEGATE 2024 Conference <i>“NVR: Pwning the Surveillance System and its Supply Chain”</i>	Seoul, South Korea Aug 2024
DEF CON 32 Conference Main Stage <i>“Watcher being watched: Exploiting the Surveillance System and its Supply Chain”</i>	Las Vegas, NV Aug 2024

CERTIFICATE

- Information Processing Technician August 2021

BUG REPORTS

With Team.ENVY

Hikvision

CVE-2023-28812, CVE-2023-28813, CVE-2024-29947, CVE-2024-29948, CVE-2024-29949

Synology

CVE-2024-29228, CVE-2024-29229, CVE-2024-29241, CVE-2024-29227, CVE-2024-29230, CVE-2024-29231, CVE-2024-29232, CVE-2024-29233, CVE-2024-29234, CVE-2024-29235, CVE-2024-29236, CVE-29237, CVE-2024-29238, CVE-2024-29239, CVE-2024-29240

Dahua

CVE-2024-39944, CVE-2024-39945, CVE-2024-39946, CVE-2024-39947, CVE-2024-39948, CVE-2024-39949, CVE-2024-39950

Hanwha Vision

CVE-2024-41882, CVE-2024-41883, CVE-2024-41884, CVE-2024-41885, CVE-2024-41886, CVE-2024-41887, CVE-2023,6116

By myself

CVE-2023-29439, CVE-2023-30491, CVE-2023-32961, CVE-2023-34190, CVE-2023-7224, KVE-2024-0073, CVE-2024-37885, CVE-2025-2848

TECHNICAL SKILLS

Programming: C/C++, Python, Java, C#, Obj-c, Swift, Assembly(ARM, ARM64, x64, x86, MIPS), LLVM toolchain, DevOps, USB Protocol / Packet

Fuzzing: AFL, libfuzzer, syzkaller, Jackalope, fuzzer development using LLVM

Exploit Dev: Linux Kernel Exploit, MacOS Exploit, iOS Exploit, Windows Kernel Exploit

Tools: Docker, qemu, IDA, IDA Plugin (self-made), Hopper, life, gdb, lldb, corellium, SRD, Xcode, Raspberry Pi

Language: Korean (Native), English(Intermediate)