Underdog’s Road to pwn2own

Pwn2Own Automotive 2026
해킹 대회 참가 후기

김동희

Chapter

01

소개

- 발표자 소개

01. 소개 – 발표자 소개

- 2019.06 ~ 2020.02 Best of The Best 8기 보안 컨설팅 트랙
- 2021.03 ~ 2022.05 Diffense
- 2022.05 ~ 2023.11 78리서치랩
- 2023.12 ~ 2025.11 그레이랩
- 2025.12 ~ 개인 연구 및 홈 프로텍터

Chapter

02

대회 소개

- PWN2OWN
- PWN2OWN Automotive 2026
- PWN2OWN Berlin 2026
- PWN2OWN Ireland 2025

02. 대회 소개 – PWN2OWN

주최 : ZDI(ZERO DAY INITIATIVE)

목표 : 제로데이 취약점 발견(Remote Code Execution) → 현장 시연 → 상금 획득💰

규정 : MITM 🚫 / ARP Spoofing 🚫 / DNS Spoofing 🚫

우승 : Master of Pwn

개최지

1. PWN2OWN 2026 Automotive (Tokyo)
2. PWN2OWN 2026 Berlin
3. PWN2OWN 2026 Ireland

02. 대회 소개 – PWN2OWN Automotive 2026

- **일시 :** 2026.01.21~2026.01.23 (2026년 기준 3번째로 여는 대회)
- **타겟** : 테슬라 / 차량용 인포테인먼트(IVI) / 전기차 충전기(EV Charger) / 자동차 운영체제
- **특이사항** : 테슬라의 경우 특정 목표 달성 시 상금 + **테슬라 차량 상품**

Tesla

Any Tesla ECU	Vehicle (VEH) CAN Control	$200,000	20	Vehicle Included
	Chassis (CH) CAN Control	$300,000	30	Vehicle Included
	Party CAN Control	$400,000	40	Vehicle Included
Autopilot	Diagnostic/ Infotainment Ethernet	$200,000	20	Vehicle Included Autopilot Root Persistence Add-on
	Full Remote	$400,000	40	Vehicle Included
	Full Remote with Unconfined Root	$500,000	50	Vehicle Included Autopilot Root Persistence Add-on

IVI

Target	Prize	Master of Pwn Points
Sony XAV-9500ES	$20,000 (USD)	2
Alpine iLX-F511	$20,000 (USD)	2
Kenwood DNR1007XR	$20,000 (USD)	2

EV Charger

Target	Cash Prize	Master of Pwn Points
ChargePoint Home Flex (Model CPH50-K)	$40,000	4
Phoenix Contact CHARX SEC-3150	$40,000	4
Ford Connected Charge Station	$40,000	4
Grizzl-E Smart Level 2	$40,000	4

02. 대회 소개 – PWN2OWN Berlin 2026

- **일시 :** 2026.05.07~2026.05.09 (2025년부터 베를린 OffensiveCon 컨퍼런스에서 개최)
- **타겟** : 웹 브라우저 / 엔터프라이즈 / 서버 / 컨테이너 / AI 등 다양한 분야
- **특이 사항** : AI 관련 카테고리 존재

Target	Vector	Cash Prize
Google Chrome	Renderer Only	$75,000
	Windows Kernel Escalation of Privilege	$125,000
	Sandbox Escape	$175,000
Microsoft Edge (Chromium)	Renderer Only	$75,000
	Windows Kernel Escalation of Privilege	$125,000
	Sandbox Escape	$175,000
Apple Safari	Renderer Only	$75,000
	Windows Kernel Escalation of Privilege	$125,000
	Sandbox Escape	$175,000
Mozilla Firefox	Renderer Only	$50,000
	Sandbox Escape or Windows Kernel Escalation of Privilege	$100,000

Target	Cash Prize	Master of Pwn Points
Adobe Reader	$50,000	5
Microsoft 365 Apps (Word/Excel/PowerPoint/Outlook)	$150,000	15

Target	Cash Prize	Master of Pwn Points
Anthropic Claude Code	$40,000	4
OpenAI Codex	$40,000	4
Cursor	$30,000	3

Target	Cash Prize	Master of Pwn Points
KVM	$50,000	5
VMware ESXi	$150,000	15
Microsoft Hyper-V Client	$250,000	25

02. 대회 소개 – PWN2OWN Ireland 2025

- 2026년 개최 정보 미공개
- **타겟** : WhatsApp / Samsung Galaxy / Apple iPhone / 공유기 / 프린터 / NAS 등
- **특이사항** : WhatsApp 상금 $1,000,000달러 (약 한화 15억)

Target	Vector	Cash Prize	Master of Pwn Points
Samsung Galaxy S25	Remote	$50,000 (USD)	5
	USB	$25,000 (USD)	2.5
Google Pixel 9	Remote	$300,000 (USD)	30
	USB	$75,000 (USD)	7.5
Apple iPhone 16	Remote	$300,000 (USD)	30
	USB	$75,000 (USD)	7.5

Target	Cash Prize	Master of Pwn Points
HP DeskJet 2855e	$20,000 (USD)	2
Lexmark CX532adwe	$20,000 (USD)	2
Canon imageCLASS MF654Cdw	$20,000 (USD)	2
Brother MFC-J1010DW	$20,000 (USD)	2

Target	Options	Cash Prize	Master of Pwn Points
WhatsApp	0-Click Remote Code Execution	$1,000,000 (USD)	100
	1-Click Remote Code Execution	$500,000 (USD)	50
	Remote 0-Click Account Take-over	$150,000 (USD)	15
	Remote 0-Click Access to Microphone or Video Feed	$130,000 (USD)	13
	Remote 0-Click Access to User Sensitive Data	$130,000 (USD)	13
	Remote One-Click Access to User Sensitive Data	$130,000 (USD)	13
	Zero-Click Impersonation of Other Users in Chats	$50,000 (USD)	5

Target	Cash Prize	Master of Pwn Points
Synology DiskStation DS925+	$40,000 (USD)	4
Synology BeeStation Plus	$40,000 (USD)	4
Synology ActiveProtect Appliance DP320	$50,000 (USD)	5
QNAP TS-453E	$40,000 (USD)	4

Chapter

03

초기 환경 세팅

- 장비 선정
- 분석 환경 세팅

03. 초기 환경 세팅 - 장비 선정

Alpine

Kenwood

Charx

Grizzl-E

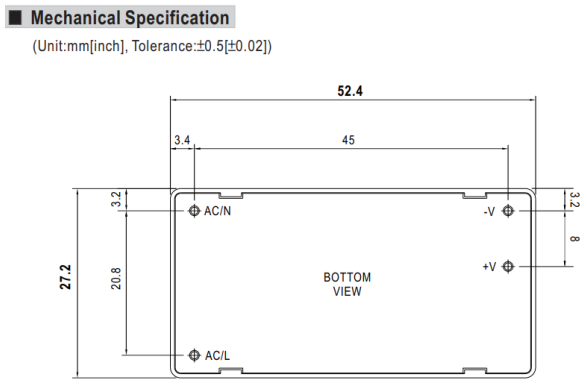
Ford

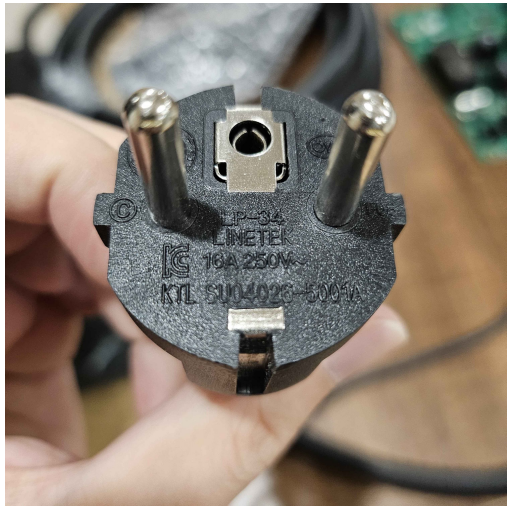
- 작년도에 나온 타겟인가 ?
- 펌웨어가 공개된 타겟 인가?
- 배송에 걸리는 시간은?
- 해당 장비의 가격은?
- 한국에서 사용가능 한지?
- 차량용 인포테인먼트 시스템(IVI) 2개
  - Alpine iLX-F511 / Kenwood DRN1007XR
- 전기차 충전기 3개
  - CHARX SEC-3150
  - Ford Connected Charge Station
  - Grizzle-E Smart Level 2

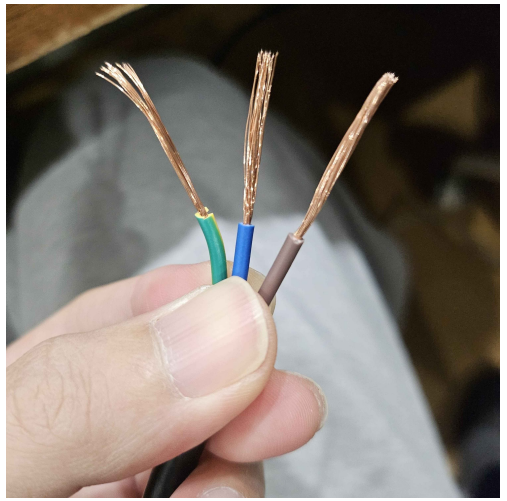
03. 초기 환경 세팅 – 분석 환경 세팅(EV Charger)

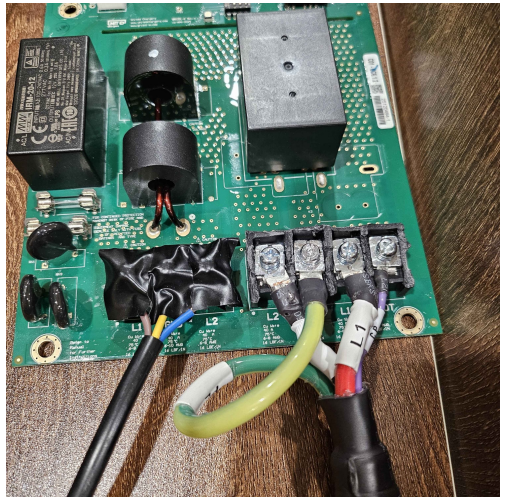
NEMA 14-50

- 미국식 240V 전원 규격으로 인해 국내 플러그 환경과 직접 호환되지 않음
- NEMA 14-50 전용 플러그만 호환가능한데 제조사 마다 구현 차이가 있었음
- 데이터시트 확인 후 직접 DC전원 인가를 시도했으나 **실패**
- 국내 220V 플러그를 개조해 장비에 전원 인가를 시도했으나 **실패**

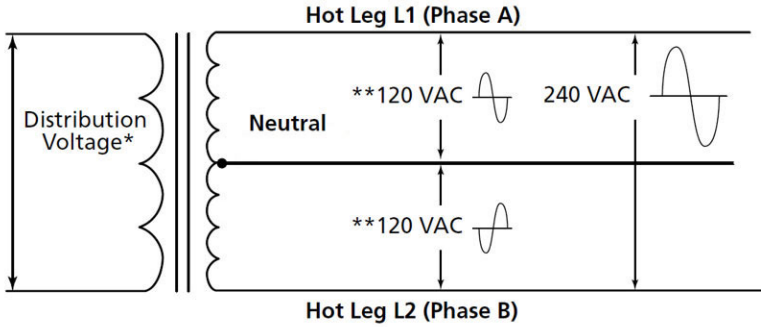


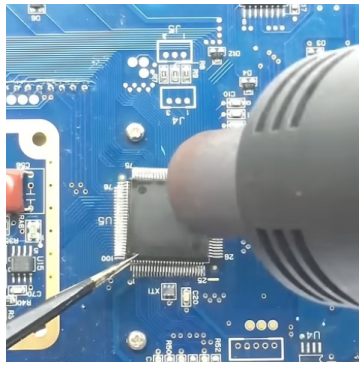






03. 초기 환경 세팅 – 분석 환경 세팅(EV Charger)





- 미국 240V 환경과 국내 220V 단상 환경의 차이로 인해 **문제 발생**
  - Split phase 장비 도입 고려 : 100만원 가량 및 배송 일정 문제
- 국내 전기 시공업체 약 30곳에 문의했으나, 적절한 해결 방안을 못 받음
- Ford는 칩 디솔더링 과정에서 장비 **고장**
- GRiZZL-E는 확인 결과 Wi-Fi 모델이 아닌 일반 모델 **오배송됨**
- **최종적으로 Charx에 집중 및 Alpine(IVI) 추가구매**

03. 초기 환경 세팅 – 분석 환경 세팅(IVI)

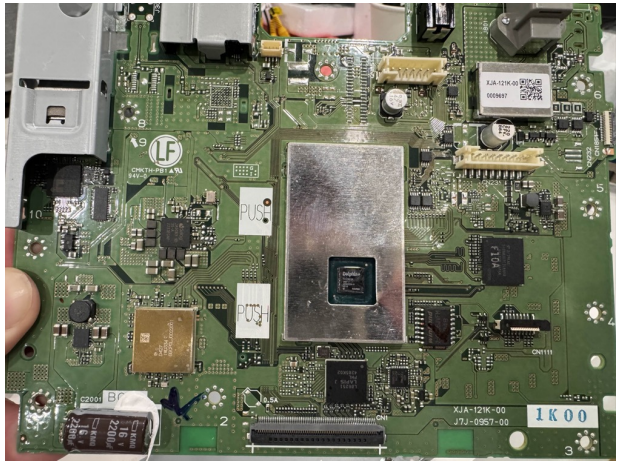
1. 공격 벡터 식별

2. IVI Wi-Fi 연결

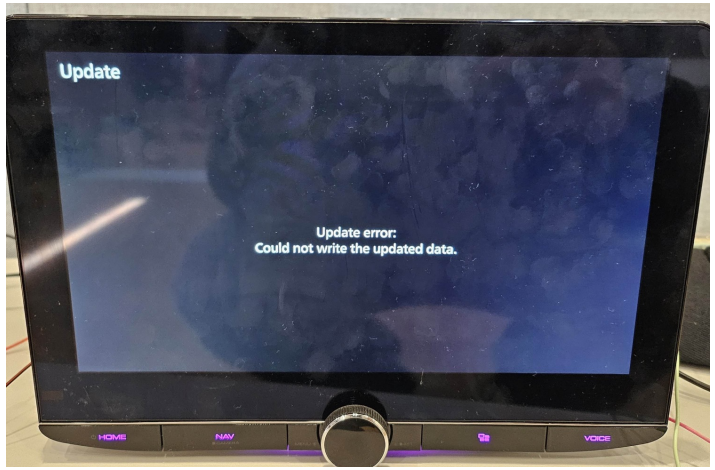
3. 포트 스캐닝

4. 1day 테스트

5. 칩 식별

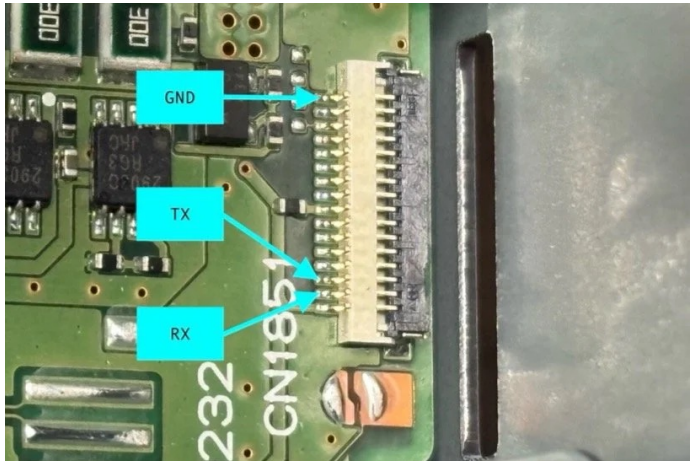


6. 동일 벤더 장비 분석



ls –al /mnt/usb* && sleep 1000;

7. UART 핀 식별



출처 : https://www.zerodayinitiative.com/blog/2026/1/6/breaking-down-the-attack-surface-of-the-kenwood-dnr1007xr-part-one

Chapter

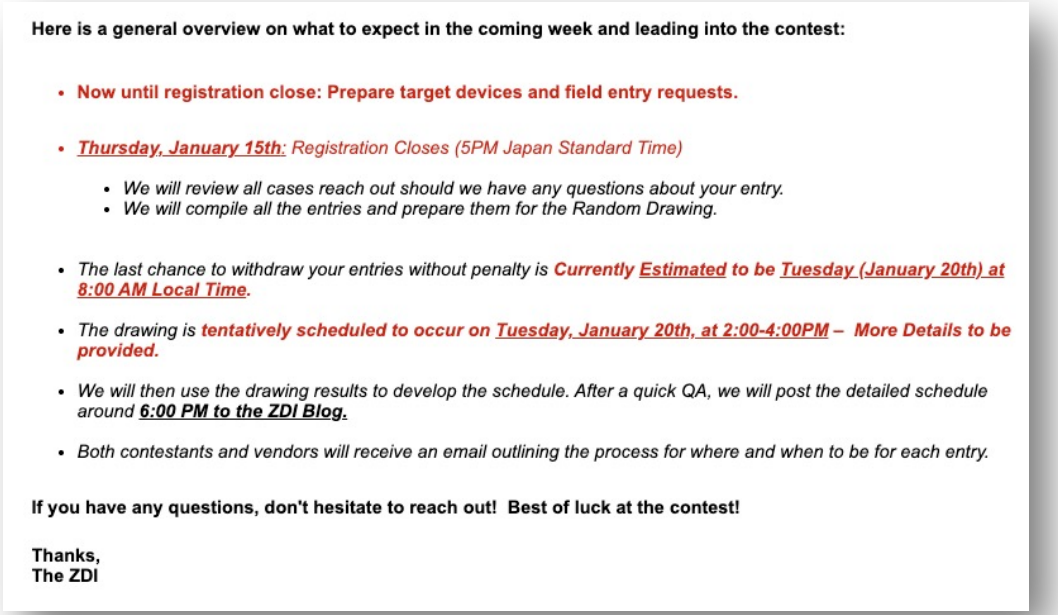
04

대회 참가

- 대회 등록
- 대회 현장
- 대회 결과
- 여담

04. 대회 참가 – 대회 등록

- **참가 등록 마감** : 2026년 1월 15일 오후 5시(일본 표준시)
- **등록 절차** : ZDI(pwn2own@trendmicro.com) 로 메일 발송 후 등록 안내 및 참가자 등록 양식 수신
- **유의사항** : 세부 취약점은 서술하지 않지만, 시연하기 위한 환경은 기술 해야함. (예. Wi-Fi 연결 / Bluetooth 페어링 등)
- **사전 확인 사항** : banned_cve_list에 해당 하지 않는 취약점인지도 확인

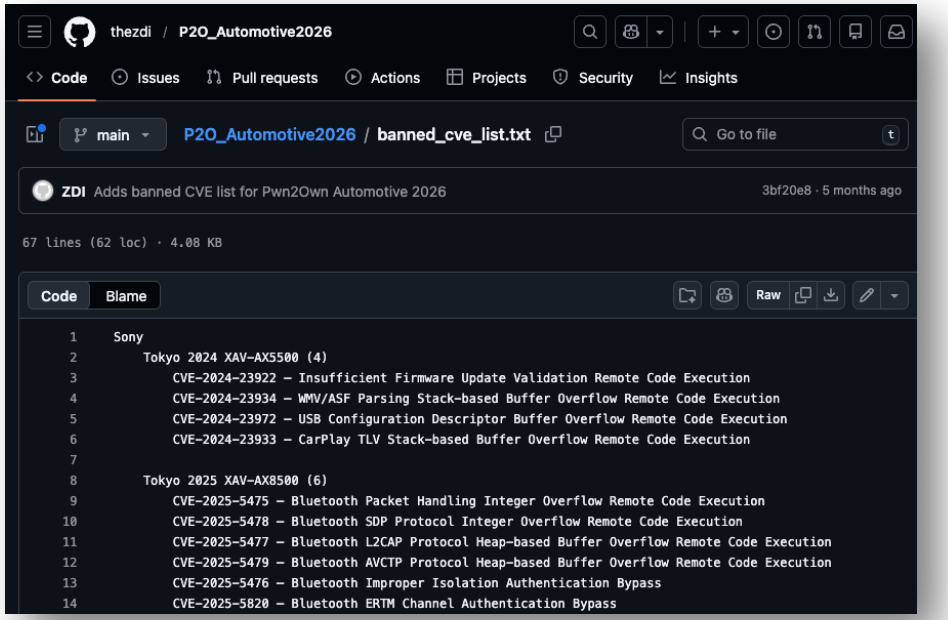


Here is a general overview on what to expect in the coming week and leading into the contest:

- **Now until registration close: Prepare target devices and field entry requests.**
- ***Thursday, January 15th:*** *Registration Closes (5PM Japan Standard Time)*
  - *We will review all cases reach out should we have any questions about your entry.*
  - *We will compile all the entries and prepare them for the Random Drawing.*
- *The last chance to withdraw your entries without penalty is* ***Currently Estimated to be Tuesday (January 20th) at 8:00 AM Local Time.***
- *The drawing is* ***tentatively scheduled to occur on Tuesday, January 20th, at 2:00-4:00PM – More Details to be provided.***
- *We will then use the drawing results to develop the schedule. After a quick QA, we will post the detailed schedule around* ***6:00 PM to the ZDI Blog.***
- *Both contestants and vendors will receive an email outlining the process for where and when to be for each entry.*

If you have any questions, don't hesitate to reach out! Best of luck at the contest!

Thanks,
The ZDI



04. 대회 참가 – 대회 등록

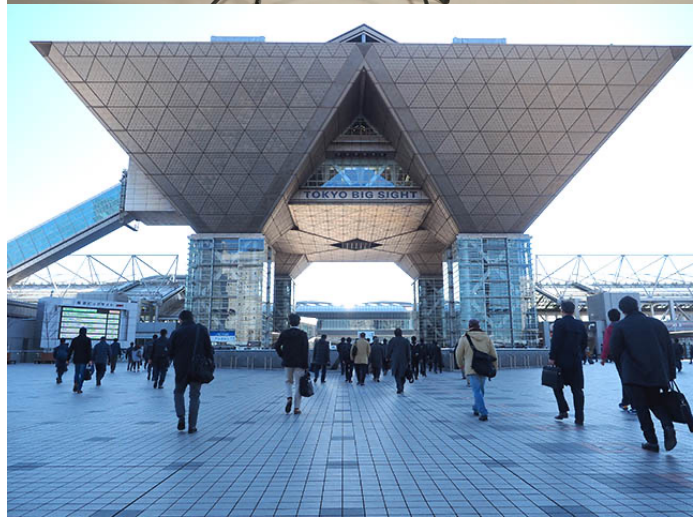
- **경쟁률** : 올해는 Alpine / Kenwood에서만 **32건**이 넘는 참가 신청이 발생하였고, 이는 작년도 베를린 대회 전체 참가 신청 수와 비슷하다고 함.

> We appreciate your patience during this time, and we ask that you please be available to answer any inquiries we may have about your registration. The schedule will be jam packed as we were flooded with over *thirty-two (32)* entries across Alpine and Kenwood alone — which is about the same amount of entries, if not more than we get for the entire Berlin(formerly known as Vancouver) contest!

- **펌웨어 이슈** : Kenwood의 경우 장비 마다 설치된 펌웨어 버전이 달랐는데, 대회 측이 가지고 있는 장비의 버전은 **1.9.0003.1000이었고,** 우리의 보유 장비는 **1.7.0003.1000**이었으며 최신 펌웨어는 **공개되지 않았음**
- 결과적으로 설정 시간 동안 펌웨어 정보를 읽을 수 있는 시간이 별도로 주어짐(방법은 알아서)？？？

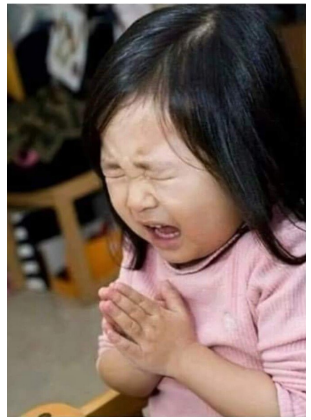
> **Kenwood Firmware**
>
> ***For Kenwood, we will allow you to make an attempt to get a firmware readout during your setup window. As mentioned in our recent Kenwood blog, SSH is exposed and there is potentially a way to get a readout. We won't do your homework for you, but this is probably the best we can offer as we are already short on devices to begin with and cannot offer a "communal" device and we must stay within the contest framework.***

04. 대회 참가 – 대회 현장



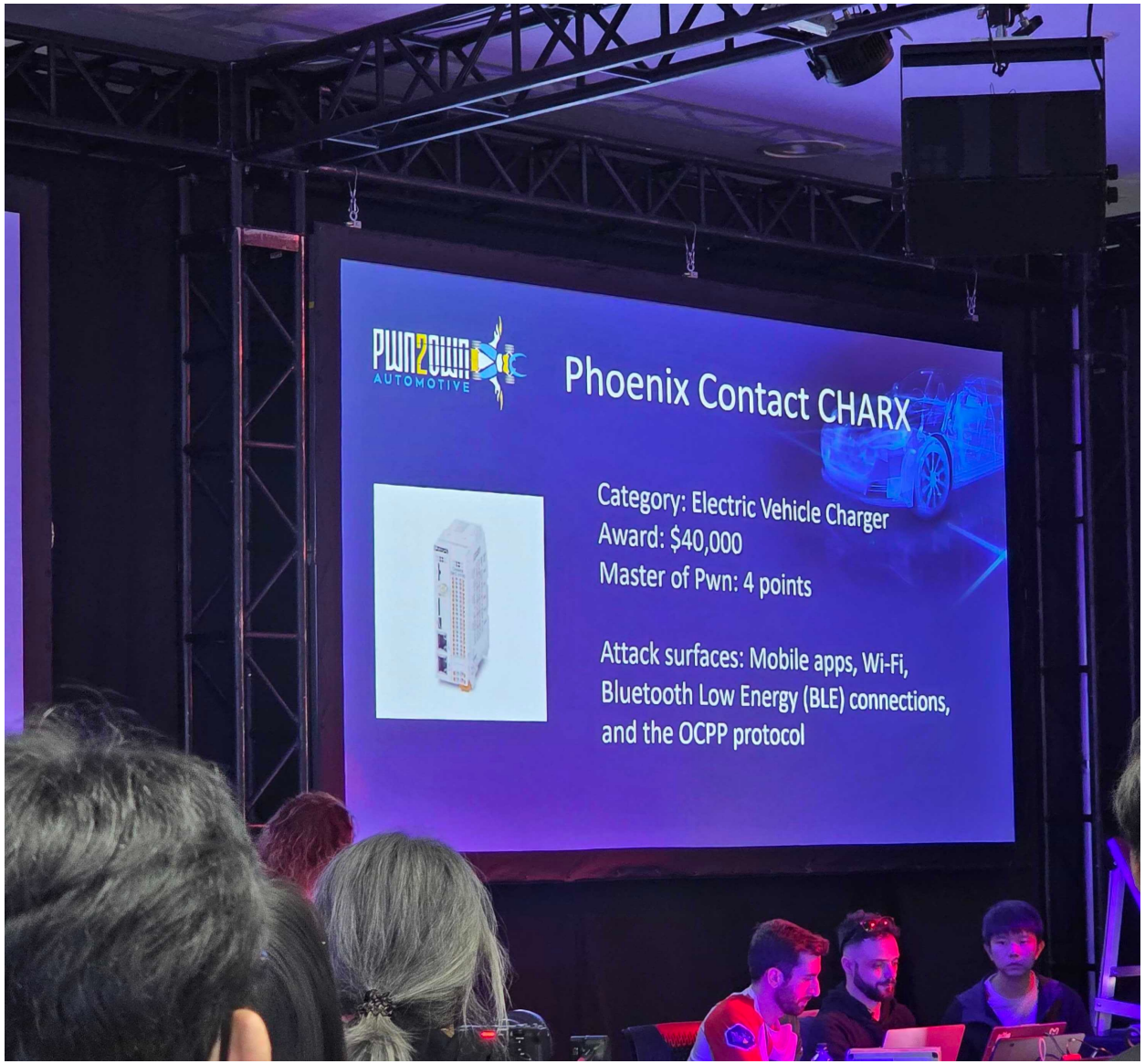
- **선발** : 대회 전날에 제비 뽑기로 순서를 선발
- **상금**
  - 1라운드 시연자에게는 상금의 **100%** 지급
  - 2,3,4,5라운드 시연자에게는 상금의 **50%** 지급
  - 나머지 시연자에게는 상금의 **25%** 지급
  - 취약점 중복 시 하나당 일정 비율의 점수 차감(4개의 버그 체인에서 2개가 중복될 시 50%차감)
- **장소** : 도쿄 빅사이트 AUTOMOTIVE WORLD 2026의 특정 부스에서 진행

6:30 p.m.	FPT NightWolf	Kenwood DNR1007XR	In-Vehicle Infotainment (IVI) Systems
	Team K	Alpine iLX-F511	In-Vehicle Infotainment (IVI) Systems
	78 ResearchLab	Phoenix Contact CHARX SEC-3150	Level 2 Electric (EV) Chargers
	Jonathan Conrad	Grizzl-E Smart 40A	Level 2 Electric (EV) Chargers



04. 대회 참가 – 대회 현장

04. 대회 참가 – 대회 현장



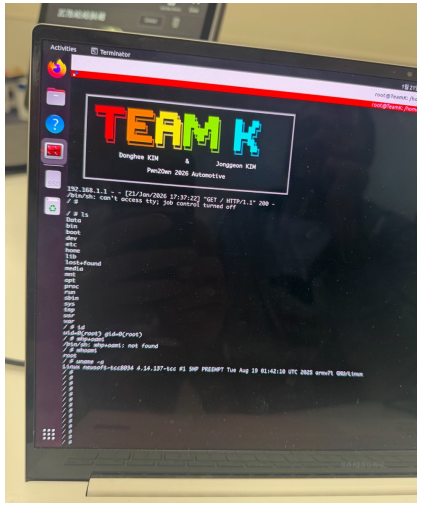
- 뽑기 순서대로 본인 차례에 맞춰 시연
- 시연 전 초기 장비 세팅하는 시간이 충분히 주어짐

  (Wi-fi 연결 / Bluetooth 페어링 등)
- 각 팀당 10분씩 3번의 기회가 주어짐
- Kenwood / alpine의 경우 많은 참가자 수로 인해

  메인 스테이지가 아닌 별도 회의실에서 진행

04. 대회 참가 – 대회 현장

- 카메라 하나 없는 회의실에서 ZDI 직원 2명과 함께 시연
- 초기 세팅 시간은 충분하기 때문에 네트워크 상태, 장비 연결 등 확인 필수
- 시연 이후에는 제출한 결과보고서를 바탕으로 ZDI 측과 상세 검토 진행
- 취약점 및 재현 조건에 대해서도 구체적인 질의 응답이 이어짐
- 결과보고서는 현장 문답에 대응할 수 있도록 자세하게 작성 추천
- Wi-Fi기반 취약점의 경우, pcap 파일도 함께 준비 및 제출



04. 대회 참가 – 대회 결과

Alpine

Kenwood

Charx

- 구매한 장비 5개 중 3개 성공 (원격 임의 코드 실행)
  - Alpine : Out-of-Bounds Read + Stack Buffer Overflow (Unique)
  - Kenwood : Default Credential + Command injection (Collision)
  - Charx : DoS + Command injection 등 버그 4개 체인 (Unique + Collision)
- 실질적으로 상금 액수는 랜덤하게 배정된 순번의 영향이 매우 큼
- 대회 장비는 매번 공장 초기화되거나 새 장비로 교체되는 방식이 아니었기 때문에,

  이전 시연의 영향 등 다양한 변수를 고려해야 했음

04. 대회 참가 – 여담

미나토구, 일본의 공동 주택 전체

최대 인원 8명 · 침실 1개 · 침대 12개 · 욕실 1개

★ 4.82 · 후기 49개

센가쿠지 근처

셀프 체크인

세탁기 및 건조기

에어컨

TV

주방

04. 대회 참가 – 여담

和牛焼肉びやんどWagyu Beef
Yakiniku BIYANGDO田町芝浦

びやんど

4.9 ★★★★★ (1,402)
야키니쿠 전문식당 · ✕

https://maps.app.goo.gl/FnqA3R4ihtWNxqiH9

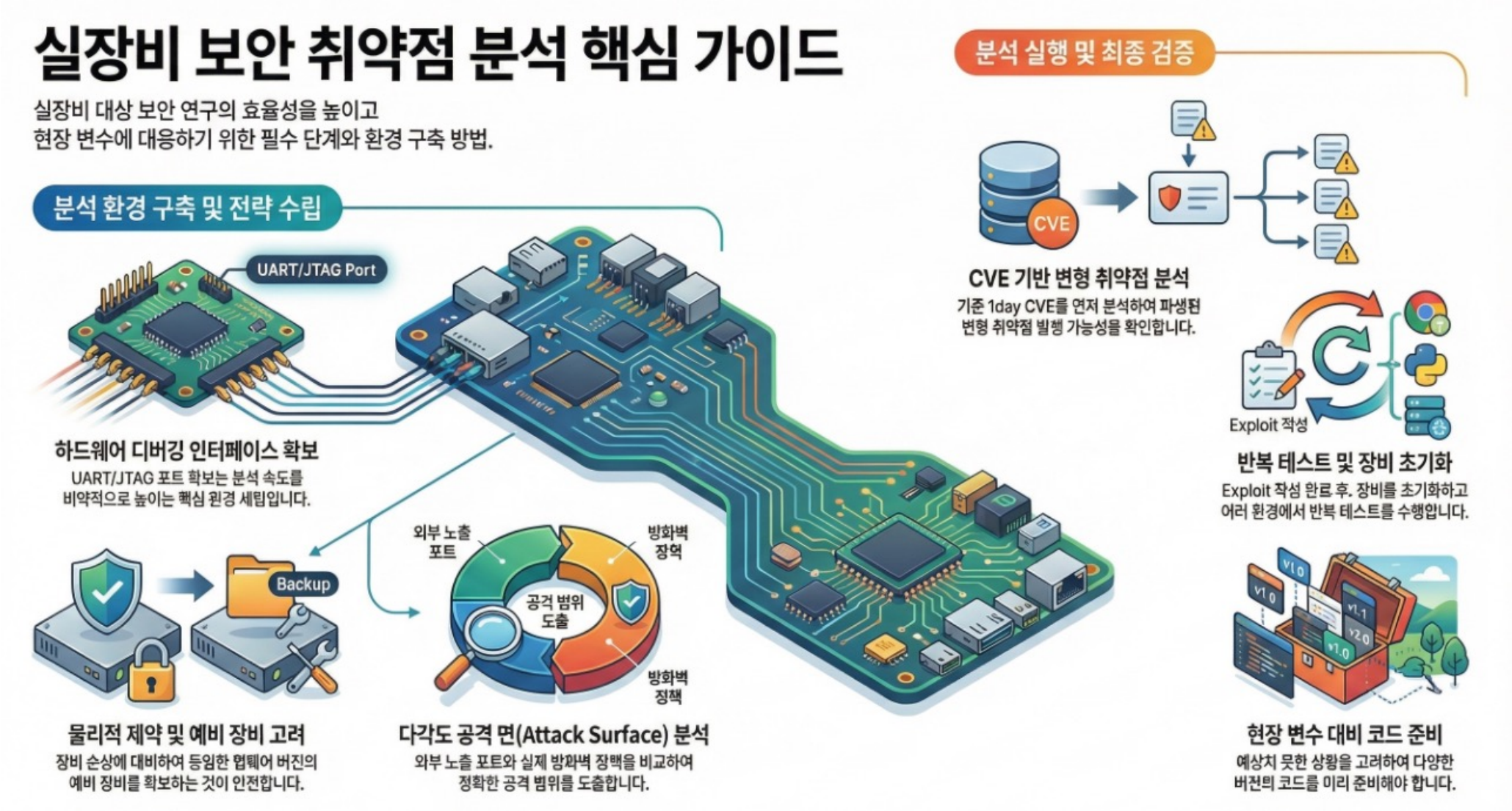
Chapter

05

대회 참가 회고

- 핵심 교훈
- 향후 계획

05. 대회 참가 회고 – 핵심 교훈

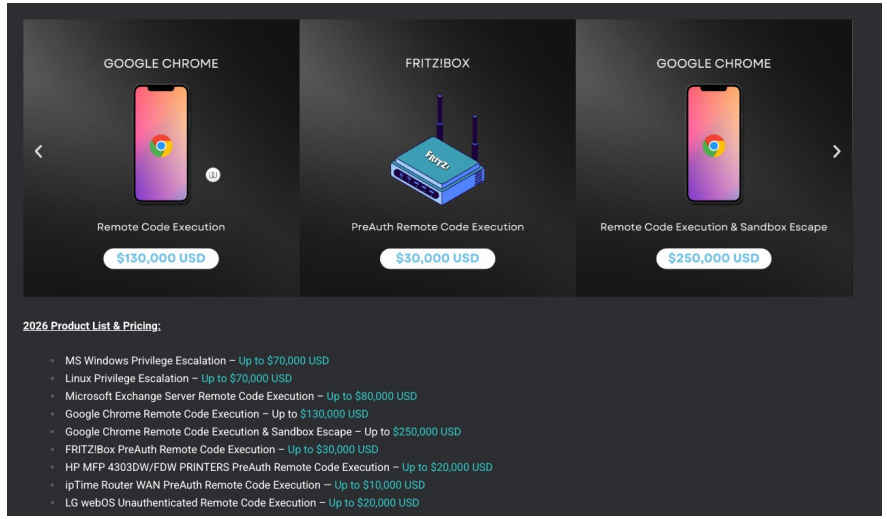


05. 대회 참가 회고 – 핵심 교훈

도전이 고민된다면, 고민보다 GO!!!

05. 대회 참가 회고 – 향후 계획

Typhoonpwn 2026



- **대회명** : Typhoonpwn 2026
- **주최사** : SSD Secure disclosure
- **일시** : 2026.05.24~29
- **위치** : 대한민국 서울 명동

PWN2OWN 2026 Berlin

Target	Cash Prize	Master of Pwn Points
Ollama	$40,000	4
LiteLLM	$40,000	4
LM Studio	$40,000	4
Llama.cpp	$40,000	4

- **대회명** : PWN2OWN 2026 Berlin
- **주최사** : ZDI
- **일시** : 2026.05.14~2026.05.16
- **위치** : 베를린

Q & A

감사합니다

@HEEHEE0219