BoB 11기 회고록

(22. 7 ~ 23. 3)

2023. 04. 03

SCP 이예준

00 목차

01 BoB(Best of the Best)란?

Best of the Best. 또는 차세대 보안리더 양성 프로그램이라고 부른다.
그냥 비오비(또는 밥)라고 부른다.

해당 프로그램은 한국정보기술연구원(KITRI)이 2011년 7월 7일 지식경제부에서 발표한 정책의 일환으로, 최정예 정보보안 인재확보를 목적으로 2012년도부터 시작하게 되었다.

01 BoB 지원

자기소개서

- 자기소개서 (최대 1000자) — 관심이 생긴 이유 / 성격에 대한 장단점 / 동기부여
- 본인이 이룬 가장 큰 성과 및 사례 (최대 1000자) — 시스템 해킹(c언어, 디버깅) / 네트워크(무선 와이파이)
- 지원 동기 (최대 1000자) — 좋은 프로젝트 환경 / 모교 학과 발전에 기여
- 합격 후 포부 (최대 1000자) — 하고싶은 프로젝트 / 적응력 / 에너지

학습계획서

- 관심 분야에 대해서 (최대 1000자) — 시스템 해킹(c언어, 디버깅) / 네트워크(무선 와이파이)
- BoB 학습 계획에 대해서 (최대 1000자) — 재귀 학습 / 창과 방패
- 진로 계획에 대해서 (최대 1000자) — 인턴십 경험 희망 / 모교 학과 발전에 기여

02 BoB 교육과정

1단계 전공교육

2단계 팀프로젝트 교육

3단계 경연 교육

7월

발대식

- 전공교육
- 공통교육
- 기초 소양교육
- 명사특강

8월

트랙 교육

- 전공교육
- 멤버십 트레이닝
- 보안산업시설 견학
- 1단계 교육평가

9월

프로젝트 팀빌딩

- 팀프로젝트 킥오프
- 팀별 멘토링

10월

프로젝트 1차 발표

- PT 경진대회
- 안보현장 체험
- 독도수호마라톤 대회참가
- 프로젝트 1차 발표 평가

11월

프로젝트 2차 발표

- 포렌식 챌린지
- Best of the Best 컨퍼런스
- 해외전문가 초청
- 프로젝트 2차 발표 평가

12월

최종발표

- 모의 사이버전
- 프로젝트 최종 발표 평가
- 2단계 교육평가

1월

심화 교육

- 트랙 심화교육
- 프로젝트 고도화
- 국가기관 견학
- 명사 특강

2월

경연 발표

- 경연 발표 평가
- 그랑프리 발표 평가
- 수료 평가
- 3단계 교육평가

03 BoB 시작

워크샵 진행

노트북 지원

BoB 시작

04 공통교육

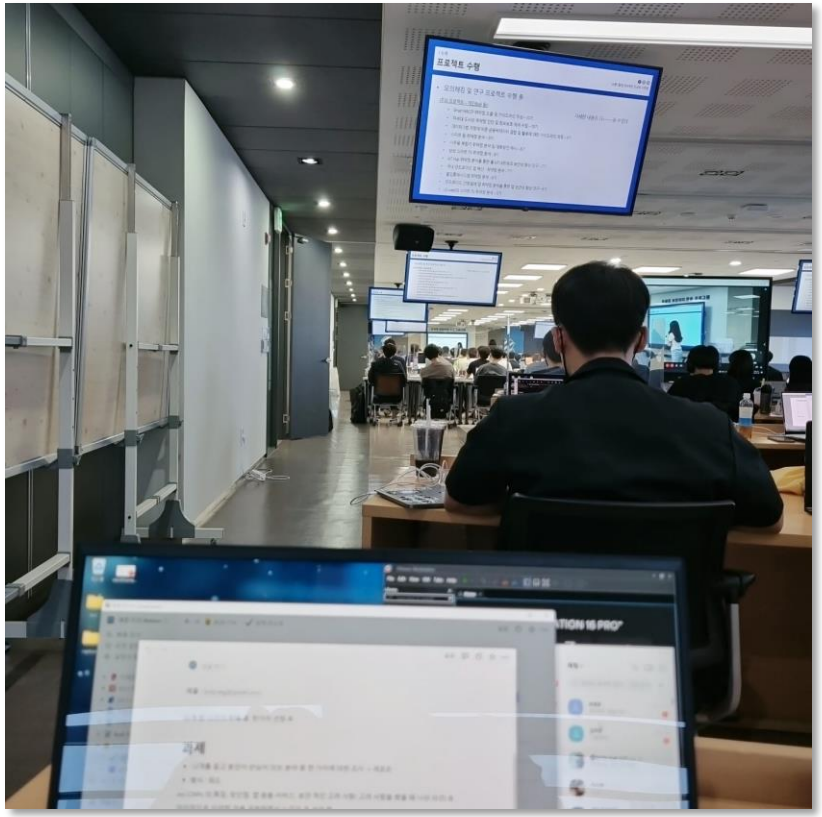
✔ 과제 리스트 (공통)

얼른 하고 쉬자..

Board View | 표 +

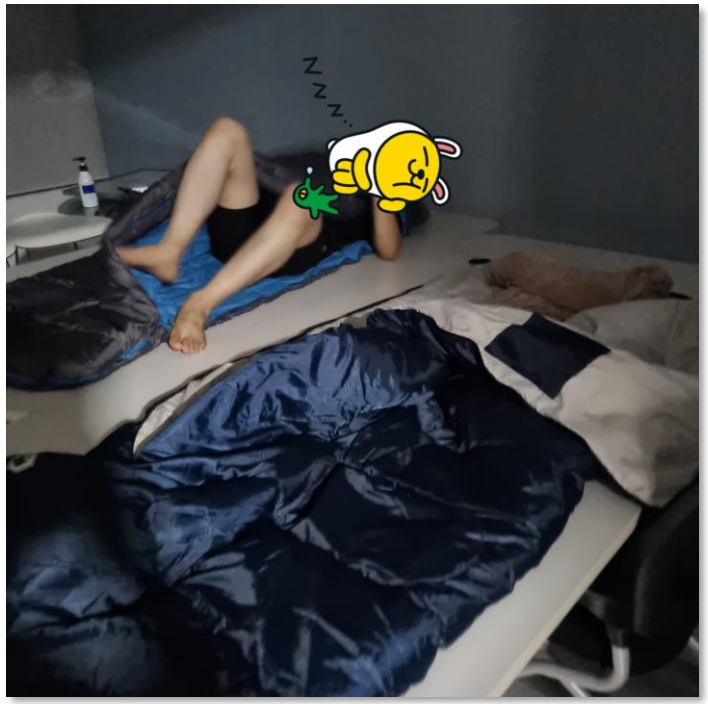
Aa 과제	멘토	마감일시	상태	제출
금융IT 컴플라이언스	허원석	7/14(금)	완료	☑
유니코드 해독	전상현	7/15(금)	완료	☑
The Secret Rules of Modern Living: A	김종현	7/16(토)	완료	☑
KISA 정보보호 진로 가이드 북	김종현	7/16(토)	완료	☑
자기소개서 작성	지한별	7/16(토)	완료	☑
가트너/최신 보안 트렌드	김영욱	7/16(토) 22시	완료	☑
정보보호 컨설팅 진단/평가 보고서	한철규	7/17(일)	완료	☑
[pwn] shitte2 exploit (UAF) (선택)	신정훈	7/21 오후 23시 5	완료	☑
[web] OS Command Injection	정도원	7/22(금) 18:59:59	완료	☑
[web] OWASP 10 (1)	정도원	7/22(금) 18:59:59	완료	☑
[web] source code patch	정도원	7/22(금) 18:59:59	완료	☑
[web] XSS	정도원	7/22(금) 18:59:59	완료	☑
[zer0day] with Junction Part	신정훈	7/23(토)	휴지통	☐
[chromium] Mojo... Crash	지현석	7/23(토)	완료	☑
[RSA] 공개키 암호 구현 과제	윤기순	7/23(토)	완료	☑
[Forensic] Data Analyze	Niko	7/23(토)	완료	☑
Credential Stuffing	지한별	7/24(일)	완료	☑
필수교육 개발보안 CICD	박수현	7/24(일)	완료	☑
Yara Rule	이강석	7/24(일)	완료	☑
Homework BoB 1 - PROVENZANO	Julien	7/25(월)	완료	☑
[pwn] kernel exploits	정광운	7/25(월) 22:00	완료	☑
[C++] Smart Pointer Analyze	김종명	7/25(월) 24:00	완료	☑

04 공통교육



공통교육

카페인



동선 최소화

샤워용 헬스

05 트랙교육

트랙 안내

취약점 분석

개념	학습내용
▪ 보안 취약점이 발생하는 원인 이해 ▪ 사고를 미연에 방지하기 위한 정보보안 기술의 트렌드 학습	▪ 리버스 엔지니어링 기법 ▪ 취약점 이해 ▪ 네트워크, 운영체제원리

디지털 포렌식

개념	학습내용
▪ 디지털 포렌식 기초 개념 이해 ▪ 실 사례연구를 통해 활용방안을 익히며 사례실습	▪ 디지털 포렌식 기초 개념 ▪ 침해사고 시스템 분석 ▪ 시스템 분석 절차 연구 ▪ 적용 사례 연구

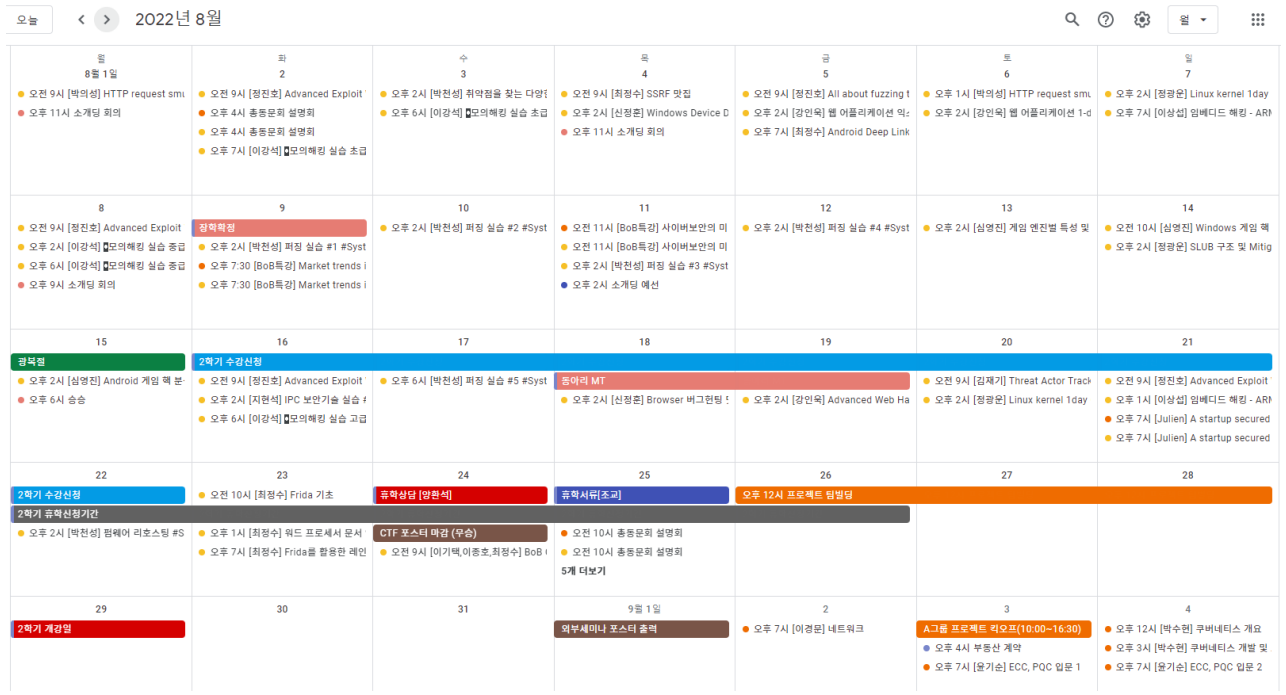
보안 컨설팅

개념	학습내용
▪ 최신 정보보안 정책 및 관리 체계에 대해 학습 ▪ 컨설팅 기법 및 법제도에 대한 이해를 통해 컨설팅 기초소양 배양	▪ 보안컨설팅 기법 ▪ 보안인증체계 및 법/제도 ▪ 감사 및 산업보안 ▪ 보안 시장 동향

보안제품개발

개념	학습내용
▪ 정보자원의 기밀성, 무결성, 가용성을 유지하기 위한 보안통제 기능의 SW를 구현함으로써 사이버보안 위협에 대응 ▪ 안전한 SW 개발을 위해 소스코드 등에 존재할 수 있는 잠재적인 보안취약점을 제거하고, 보안을 고려하여 기능을 설계 및 구현	▪ 개발보안 방법론 ▪ 소프트웨어 개발 보안 ▪ 개발보안 강화 활동 ▪ 개발보안 구현

05 트랙교육



과제 리스트 (트랙교육)

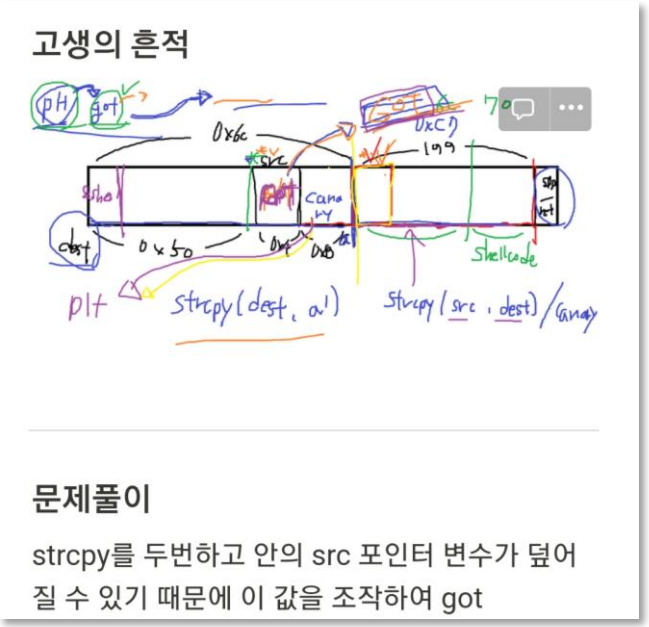
후딱하고.. 쉬자,,,

표 | 필터 | 정렬 | 새로 만들기

기한 | 이소연 | 기한 | 필터 추가

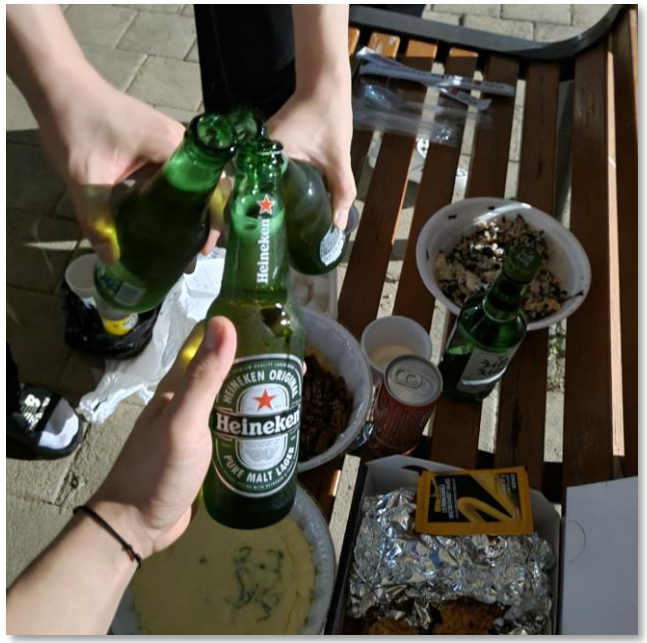
Aa 과제	멘토님	기한	김지연	이소연	이예준
[Embedded] Firmware extraction	이상섭	07/31/2022	complete	complete	complete
[Yara] target attack analysis	Anthony	08/03/2022	drop	drop	drop
통신구간 암호화 관련 recv 함수 찾기	최정수	08/05/2022	complete	complete	complete
원하는 싱글 게임 핵 만들기	최정수	08/05/2022	complete	complete	complete
PayPal - Smuggling	박의성	08/05/2022	complete	submit	submit
openSSL Hooking	이상섭	08/07/2022	complete	complete	complete
Migrating to 64-Bit 논문 정리	박천성	08/09/2022	complete	complete	complete
윈도우 디바이스 드라이버 분석	신정훈	08/11/2022	submit	submit	submit
MINI CTF 과제	강인욱	08/13/2022	complete	complete	complete
BBC Algorithms Quick Sort 구현 및 개선 (선택)	김중현	08/14/2022	drop	drop	complete
CVE-2022-1015 full lpe exploit 코드 작성	정광운	08/19/2022	drop	drop	drop
Remote Code Execution 과제	강인욱	08/21/2022	complete	complete	complete
SLUB 실습 및 디버깅	정광운	08/21/2022	drop	drop	drop
vTable 하이재킹	지현석	08/21/2022	complete	complete	complete
MINI CTF 과제 - XSS	강인욱	08/22/2022	complete	complete	complete
[pwn] lab02~03	정진호	08/23/2022	submit	complete	complete
[pwn] lab04~05	정진호	08/23/2022	In process	submit	complete
[pwn] lab06~07	정진호	08/23/2022	In process	submit	complete
[pwn] lab09	정진호	08/23/2022	In process	submit	complete
모의해킹 분석 보고서 작성	이강석	08/23/2022	In process	complete	complete
HW crack challenge	최정수	08/24/2022	Not started	drop	drop

05 트랙교육



열심히 할땐 하고..

잠자리의 진화..

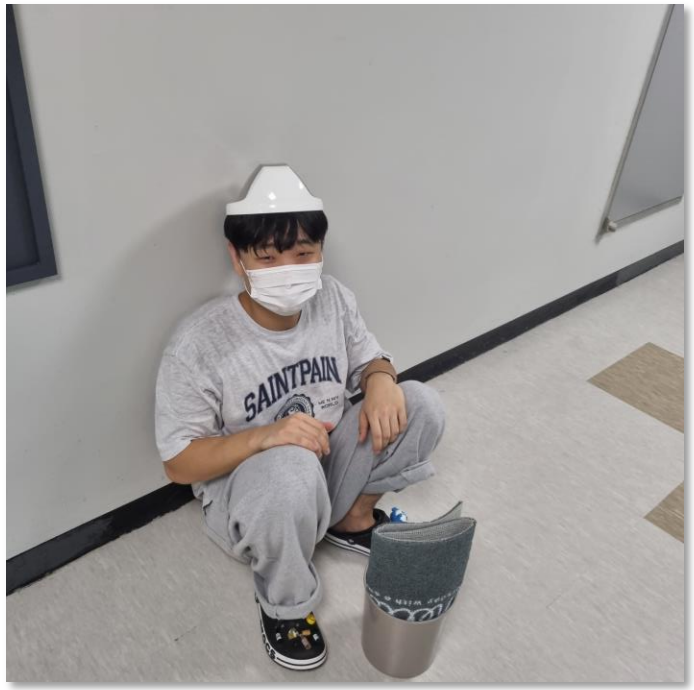


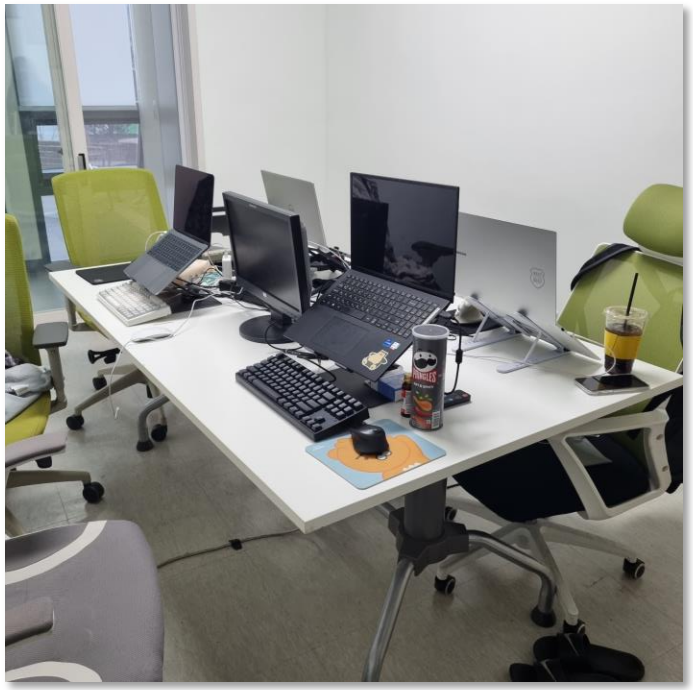
에라 모르겠다

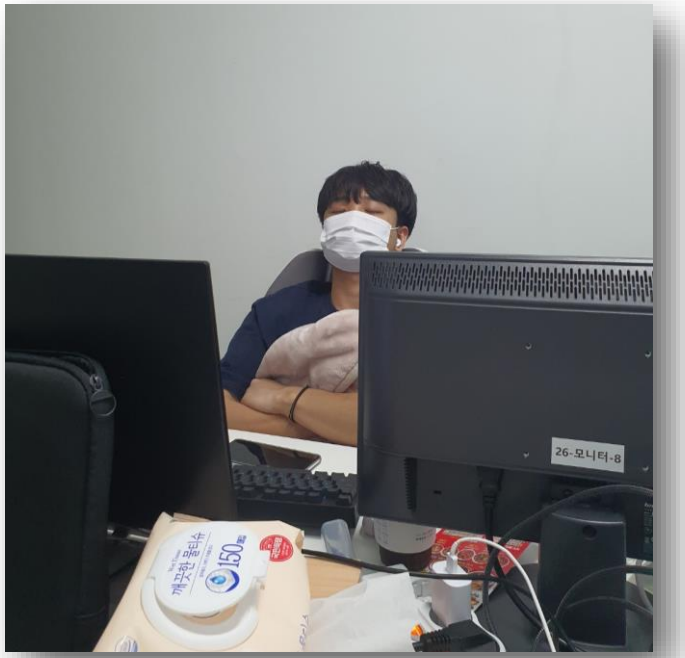
팀 구성

5인 1조

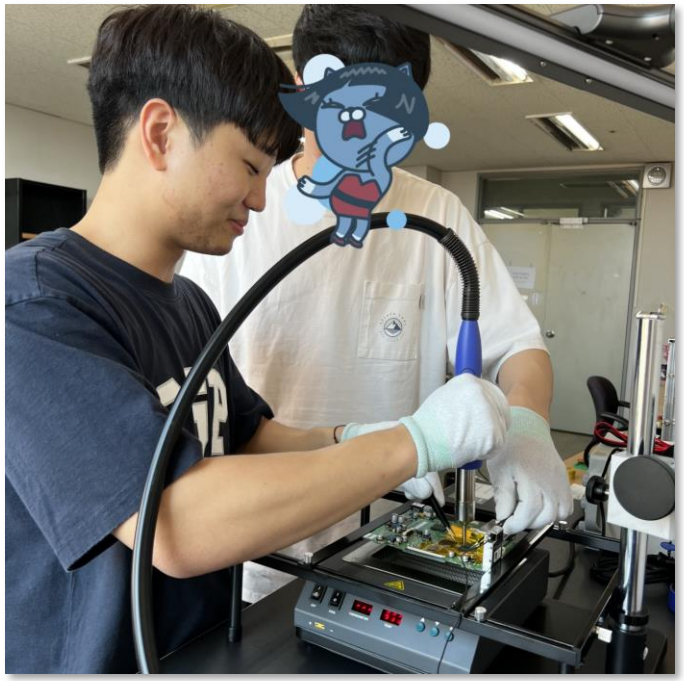
자유롭게 구성

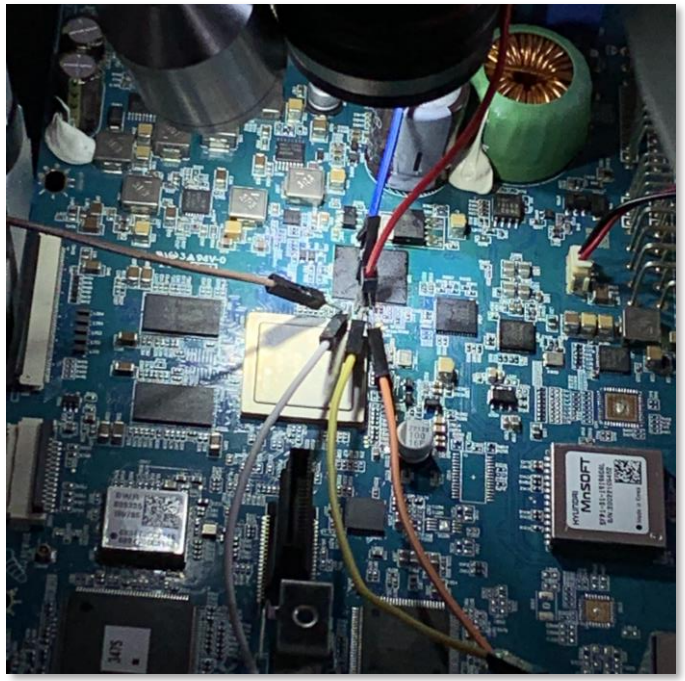

SAINTPAIN

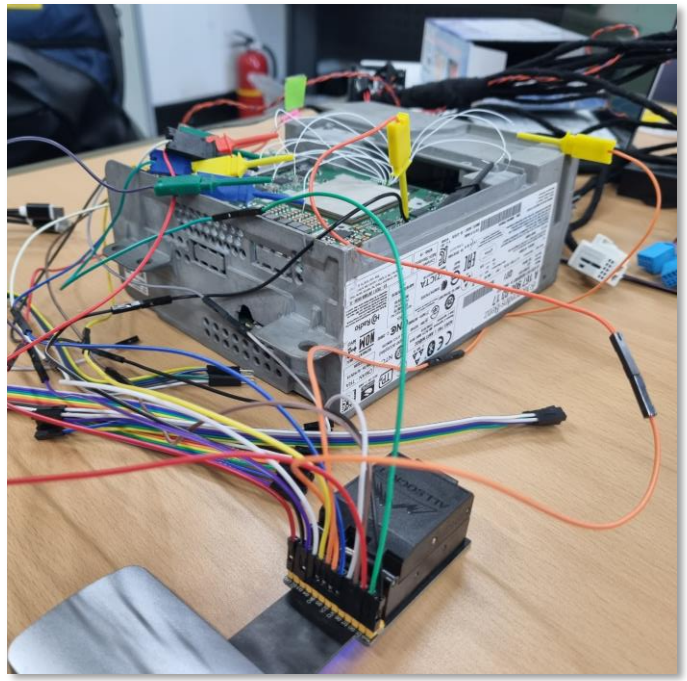



26-모니터-8

프로젝트







프로젝트

분석

Name	Responsibility	Property
Tivoli backdoor 사용 방법	예준 이	2023년 1월 12일 오후 5:34
가상 환경 구축	진명 박	2023년 1월 1일 오후 11:16
Tivoli IVI 내부 기능 분석	Yujin Bae	2023년 1월 1일 오후 11:16
분석 시 주의사항		2023년 1월 1일 오후 11:16
QNX	eigenkyeong	2023년 1월 1일 오후 11:16
QNX 파일시스템 분석	eigenkyeong	2023년 1월 1일 오후 11:16
HeadUnit 및 배선 테스트	예준 이	2023년 1월 1일 오후 11:16
안드로이드 파일 변환 및 디컴파일	진명 박	2023년 1월 1일 오후 11:16
Firmware Handling	안상혁	2023년 1월 1일 오후 11:16
Backdoor	진명 박	2023년 1월 1일 오후 11:16
삽질일기		2023년 1월 1일 오후 11:16
Chip Off	예준 이 eigenkyeong	2023년 1월 1일 오후 11:16
Firmware Dump 데이터 분석	안상혁 eigenkyeong 예준 이	2023년 1월 1일 오후 11:16
Tivoli - Smali Code Injection	예준 이	2023년 1월 1일 오후 11:16
1-day 분석	Yujin Bae eigenkyeong	2023년 1월 1일 오후 11:16
헤드유닛 기능 검사	eigenkyeong	2023년 1월 1일 오후 11:16
Benz IVI 내부 기능 분석	eigenkyeong	2023년 1월 1일 오후 11:16
논문	안상혁	2023년 1월 1일 오후 11:16
DirtyCow 1-day Exploit	진명 박	2023년 1월 1일 오후 11:16
취약점 제보	예준 이	2023년 1월 1일 오후 11:16
arm 어셈블리 코딩 및 크로스 컴파일	진명 박 eigenkyeong	2023년 1월 1일 오후 11:16
Fuzzing	안상혁 진명 박	2023년 1월 1일 오후 11:16
Firmware Dump 취약점 분석		2023년 1월 1일 오후 11:16
소스코드 분석	안상혁 eigenkyeong 예준 이 진명 박	2023년 1월 1일 오후 11:16

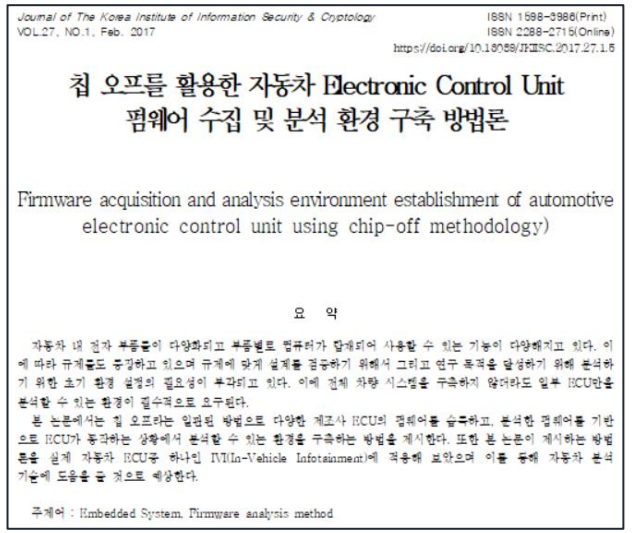
Done 29

Name	Due Date	Responsibility	Status
마무리	2022년 12월 17일	안상혁 Yujin Bae	Done
등적 분석 장비 구매 목록	2022년 11월 3일	eigenkyeong Yujin Ba	Done
데이터 분석 논문	2022년 10월 28일	안상혁	Done
JTAG&UART 실험	2022년 10월 8일	Yujin Bae	Done
JTAG&UART 사전 조사	2022년 10월 4일	eigenkyeong	Done
산출물 보고서 역할 분배	2022년 9월 30일	Yujin Bae	Done
Firmware 데이터 분석	2022년 9월 25일	안상혁	Done
eMMC reader 구매	2022년 9월 21일	안상혁	Done
Input Vector 조사	2022년 9월 19일	진명 박	Done
단국대 미팅 준비	2022년 9월 18일	Yujin Bae	Done
AGL 가상 환경 구축	2022년 9월 17일	진명 박	Done
AVN 분해 해보기	2022년 9월 17일		Done
수집 관련 포렌식 도구	2022년 9월 11일	안상혁	Done
Chip Off 방법 조사	2022년 9월 11일	예준 이 eigenkyeong	Done
IVI 관련 최신 기술 동향	2022년 9월 11일	예준 이	Done
펌웨어 다운로드 사이트	2022년 9월 11일	예준 이	Done
선행 연구 및 관련 자료	2022년 9월 11일	안상혁	Done
개발 보드 조사	2022년 9월 9일		Done
Chip Off Toolkit 및 관련 특허 조사	2022년 9월 9일	Yujin Bae	Done
수행계획서 및 WBS 작성	2022년 9월 7일	Yujin Bae	Done
IVI 장비 수급 업체 조사	2022년 9월 6일	eigenkyeong	Done
개발 계획서 작성	2022년 9월 5일	안상혁	Done
사무실 및 인터넷	2022년 9월 2일	예준 이	Done
PPT& 보고서 템플릿	2022년 8월 30일	Yujin Bae	Done

프로젝트


HOME
MODE
NAVI
PHONE
SETUP
USER
yejun@ubuntu:~$ nc -lvp 4545
Listening on 0.0.0.0 4545
DESKER
MOTION DESK

11월 8일 진행된 Codegate 2022
BoB Session에서 발표 진행


Journal of The Korea Institute of Information Security & Cryptology
VOL.27, NO.1, Feb. 2017
ISSN 1598-3986(Print)
ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.1.5

칩 오프를 활용한 자동차 Electronic Control Unit
펌웨어 수집 및 분석 환경 구축 방법론

Firmware acquisition and analysis environment establishment of automotive electronic control unit using chip-off methodology)

요 약

자동차 내 전자 부품들이 다양화되고 부품별로 컴퓨터가 탑재되어 사용할 수 있는 기능이 다양해지고 있다. 이에 따라 규제들도 증가하고 있으며 규제에 맞게 설계를 검증하기 위해서 그리고 연구 목적을 달성하기 위해 분석하기 위한 초기 환경 설정의 필요성이 부각되고 있다. 이에 전체 차량 시스템을 구축하지 않더라도 일부 ECU만을 분석할 수 있는 환경이 필수적으로 요구된다.

본 논문에서는 칩 오프라는 일관된 방법으로 다양한 제조사 ECU의 컴퓨터를 습득하고, 분석한 컴퓨터를 기반으로 ECU가 동작하는 상황에서 분석할 수 있는 환경을 구축하는 방법을 제시한다. 또한 본 논문이 제시하는 방법론을 실제 자동차 ECU중 하나인 IVI(In-Vehicle Infotainment)에 적용해 보았으며 이를 통해 자동차 분석 기술에 도움을 줄 것으로 예상한다.

주제어 : Embedded System, Firmware analysis method

학술지 투고 예정 (2023. 04)

취약점 제보

07 취약점의 분류

제로데이 (0-day)

- 알려지지 않은 취약점. 취약점으로 공격을 당했지만, 현재 보안 패치가 없는 상태.

원데이 (1-day)

- 최신 취약점에 대한 패치가 발표 되었지만, 여러 사유로 인하여 패치를 적용하지 않은 상태.

올데이 (Olday)

- 취약점에 대한 분석이 끝나고 보안 패치도 있으나, 담당자의 부재 및 인식 부족으로 패치를 적용하지 않은 상태.

취약점의 분류

ex) CVE-2022-23766

목록 조회수 : 118

CVE-2022-23766 | BigFileAgent 임의 파일 실행 취약점 2022.09.19

□ 개요

o ㈜블루트리社 BigfileAgent.exe의 취약한 설치 로직을 통해 발생하는 임의 파일 실행 취약점

㈜블루트리社 BigfileAgent.exe의 취약한 설치 로직을 통해 발생하는 임의 파일 실행 취약점

취약점 종류	영향	심각도	CVSS 점수	CVE-ID
부적절한 입력 검증	임의 파일 실행	High	7.8	CVE-2022-23766

□ 설명

o BigFileAgent에서 프로그램 설치 시 전달되는 파일명이 임의로 조작될 수 있어 발생하는 취약점

o 공격자는 자신이 호스팅하는 페이지로 접속을 유도하거나 일반 웹사이트에 XSS 등을 수행, 취약점을 유발하는 스크립트를 삽입하여 피해 유발 가능

□ 영향받는 제품 및 버전

영향받는 제품 및 버전

제품	영향 받는 버전	환경
BigFileAgent	1.0.1.9 및 이전 버전	윈도우

□ 해결 방안

o 취약한 버전의 제품 이용자는 BigFileAgent 버전 1.0.2.0 이상으로 설치

□ 참고

o https://www.bigfile.co.kr/index.php

□ 기타

o 취약점 KrCERT 홈페이지를 통해 이규호님께서 제공해주셨습니다.

08 후기 및 느낀점

장점

- 하나의 프로젝트에 몇 달간 몰두 해보는 경험.
- 전국에 보안 관련 인맥이 생김.
- 현직에서 근무하시는 많은 멘토들과 연결고리 생김

단점

- 발표자는 주 6일 10시부터 22시까지 프로젝트를 진행함.
- 공통교육, 트랙교육도 주7일 10시부터 22시까지 진행함.
- 집에 가고 싶음. 놀고 싶음. 울고 싶음.

Q & A

SCP 이예준