

BoB 117I 회고록

(22. 7 ~ 23. 3)

2023. 04. 03

SCP 이예준



1. BoB란? / BoB 지원
2. BoB 교육과정
3. BoB 시작
4. 공통교육
5. 트랙교육
6. 프로젝트
7. 취약점 분류
8. 후기 및 느낀점



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

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

자기소개서

- 📄 자기소개서 (최대 1000자)
- 📄 본인이 이룬 가장 큰 성과 및 사례 (최대 1000자)
- 📄 지원 동기 (최대 1000자)
- 📄 합격 후 포부 (최대 1000자)

관심이 생긴 이유 / 성격에 대한 장단점 / 동기부여
시스템 해킹(c언어, 디버깅) / 네트워크(무선 와이파이)
좋은 프로젝트 환경 / 모교 학과 발전에 기여
하고싶은 프로젝트 / 적응력 / 에너지

학습계획서

- 📄 관심 분야에 대해서 (최대 1000자)
- 📄 BoB 학습 계획에 대해서 (최대 1000자)
- 📄 진로 계획에 대해서 (최대 1000자)

시스템 해킹(c언어, 디버깅) / 네트워크(무선 와이파이)
재귀 학습 / 창과 방패
인턴십 경험 희망 / 모교 학과 발전에 기여



1단계 전공교육

7월

발대식

- 전공교육
- 공동교육
- 기초 소양교육
- 명사특강

8월

트랙 교육

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

2단계 팀프로젝트 교육

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

3단계 경연 교육

1월

심화 교육

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

2월

경연 발표

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



워크샵 진행



노트북 지원



BoB 시작

오늘	<	>	2022년 7월	🔍	🕒	⚙️	📅	☰
월 27	화 28	수 29	목 30	금 7월 1일	토 2	일 3		
📌 성적공시 및 여의산청		● 오후 12시 경은 생일 (과자집)	● 오후 12시 초코송이쿠키	● 오전 9시 [임종인 석좌교수 특강] RSA	● 오전 10시 [유현] BoB 물리교육	● 오전 9시 [조성재] C언어와 정규표현식		
● 오전 9시 BoB 증명서류 제출		● 오후 1시 SCP 내부세미나		● 오후 1시 [유하준 센터장] BoB 오리엔	● 오후 2시 [김종원] BoB & 디지털포렌스	● 오후 1시 [이경문] 보안제품개발 트랙		
● 오후 1:30 스타일드					● 오후 4시 [구희진] 디지털포렌식과 회계	● 오후 2시 [이경문] 네트워크 실습 준비		
● 오후 4시 홍대 먹방나들이					● 오후 7시 [장민정] 모바일 악성코드	● 오후 7시 [박수현] 보안제품 종류/역할		
						● 오후 8시 SCP 임원진 회의		
4	5	6	7	8	9	10		
BoB 11기 발대식	● 오전 9시 [정승기] BoB 프로젝트(그랑)	1학기 성적학정	● 오전 9시 [조민재] 개발보안과 DevSec	● 오전 9시 [최원익] 사이버범죄 수사사례	● 오전 9시 [김영욱] 가트너/최신 보안 트	● 오전 10시 [이기택] 취약점분석트랙 소		
● 오후 2시 BoB 11기 발대식	● 오후 1시 [김정철] 누리캅스 설명회	● 오전 9시 [김정현] 보안컨설팅 소개	● 오후 1시 [전상현] MMORPG 게임개발	● 오후 2시 [박경태] 기업관사와 포렌식	● 오후 1시 [지한별] 웹앱 취약점 컨설팅	● 오후 1시 [정광운] IDA 및 WinDbg 활용		
	● 오후 4시 [김영철] 라이브 포렌식의 개	● 오후 1시 [정시행] 제품 취약점 컨설팅	● 오후 4시 [전상현] 유니코드 인코딩 정	● 오후 4시 [허원석] 금융IT 컴플라이언스	● 오후 3시 BoB 수료생과의 만남	● 오후 5시 우즈쓰		
	● 오후 7시 [김종현] 디지털포렌식 절차	● 오후 4시 [산통역] ISMS 컨설팅	● 오후 7시 [윤기순] 암호학 개론 #1	● 오후 7시 [박문범] 취약점 Exploit을 활	● 오후 4시 [김경권] 보안컨설팅 로드맵	● 오후 6시 [이상섭] 임베디드 해킹의 위		
	● 오후 9시 [유현] 사이버수사	● 오후 7시 [문광석] 보안 마스터클래스		● 오후 10시 SCP 임원진 회의	● 오후 7시 [조성규] 컨설팅 방법론 / 프			
11	12	13	14	15	16	17		
● 오전 9시 [장대명] 검색엔진의 원리	● 오전 9시 [정진호] Your first exploit #	● 오전 9시 [김종현] 커뮤니케이션 및 문	● 오전 11시 [신정훈] 취약점 연구 시작하	● 오후 2시 [안철수 특강] 사이버보안 대	용아침 결혼식	제단점		
● 오후 1시 [윤기순] 암호학 개론 #2	● 오후 1시 [박의성] 웹의 역사로 알아보	● 오후 1시 [한철규] 프로젝트 관리	● 오후 2시 [신정훈] Real-world 취약점	● 오후 4:30 [박세준] 해커의 관점에서 비	● 오전 9시 [김경태] 디지털포렌식 핵심	● 오전 9시 [지한별] 정보보호 컨설팅 이		
● 오후 4시 [남성영] Windows Mitigati	● 오후 3시 [KISA] 취약점정보 신고포상	● 오후 4시 송이민서	● 오후 3:30 [신정훈] 시스템 해킹 맞보기	● 오후 7:30 [정도원] HTTP를 해킹하는	● 오후 1시 [유현] 디지털포렌식 핵심기술	● 오후 1시 [한철규] 정보보호 컨설팅 진		
● 오후 7시 [조수현] 파이썬 정복	● 오후 4시 [지현석] 대략 전공 수업과 위	● 오후 4시 [김두민] 개인정보보호	● 오후 7:30 [김재기] 바이너리 분석 101	● 오후 11시 컨류전 모임	● 오후 7시 [박문범] 침해사고대응 I	● 오후 3시 [산통역] ISMS 인증 평가		
	● 오후 7:30 [이강석] 다크웹에 접속하는	● 오후 7시 [박창현] 산업 보안 컨설팅	● 오후 11시 소개팅 회의			● 오후 7시 [김종진] 보안컨설팅 보고서		
18	19	20	21	22	23	24		
● 오전 9시 [정진호] Exploit Writing Ba	● 오전 9시 [조성재] C 언어와 정규표현	● 오전 9시 [니코] Incident Response	● 오전 9시 [정광운] ITW 에서의 커널 휘	● 오전 9시 [김현민] 웹 취약점 분석 컨설팅	● 오전 9시 [전상현] 악성코드 분석엔진	● 오전 9시 [정광운] 리눅스 커널 디버깅		
● 오후 1시 [김종현] Modern C++ 취약	● 오후 12시 [윤기순] 공개키암호 구현	● 오후 3시 [유현] 디지털포렌식 핵심기술	● 오전 11시 [신정훈] Windows 10 Ex	● 오후 1시 [김두민] 웹 취약점 분석 컨설팅	● 오후 1시 [박수현] 코드품질 및 CID	● 오후 2시 [이상섭] 하드웨어해킹(필레		
● 오후 4시 [지현석] IPC 보안 기술팀 #Sys	● 오후 3시 [조성재] C 언어와 정규표현	● 오후 7시 [조성재] C 언어와 정규표현	● 오후 1시 [신정훈] Windows 10 Com	● 오후 4시 [김두민] 전자 보안 체계 진단	● 오후 4시 [조성재] C 언어와 정규표현	● 오후 7시 [정도원] 웹해킹 이론과 실		
● 오후 7시 [이강석] YARA for RCE #Re	● 오후 6시 [이경문] 네트워크		● 오후 7시 [이강석] ATM Cyber Attack	● 오후 7시 [문광석] 개인정보보호 컨설팅	● 오후 7시 [박문범] 침해사고대응 II			
● 오후 11시 소개팅 회의			● 오후 11시 소개팅 회의					
25	26	27	28	29	30	31		
● 오전 9시 [Anthony] binary emulation	● 오전 9시 [Anthony] target attack an	● 오전 9시 [Anthony] target attack an	● 오전 9:30 공통필수 교육 평가시험	BoB센터 Maintenance	● 오전 9시 [김재기] IDAPython 을 활용	● 오후 1시 [이상섭] 임베디드 해킹 - 로지		
● 오후 2시 [Julien] AWARENESS LEC1	● 오후 2시 [Aviram] Why you should s	● 오후 1시 [권익] 서울경찰청 사이버수사	● 오후 12시 [권익] 사이버보안센터(40명)	트랙교육(7:30~8:25)	● 오후 1시 [정진호] Intermediate Exp	● 오후 7시 [박의성] HTTP request sm		
● 오후 7시 [이종호] 기술&관리	● 오후 4:20 피싱트랙 수요조사 및 시험	● 오후 2시 [권익] 사이버보안센터(40명)	● 오후 11시 소개팅 회의		● 오후 3시 [최정수] Cheat Engine 토큰			
	● 오후 4:30 [박세준] 해커의 관점에서 비	● 오후 2:30 [권익] 서울경찰청 사이버수			● 오후 7시 [최정수] 소트웨어의 통신			
	● 오후 7시 [박세준] 해커의 관점에서 비	● 오후 4시 미용실						

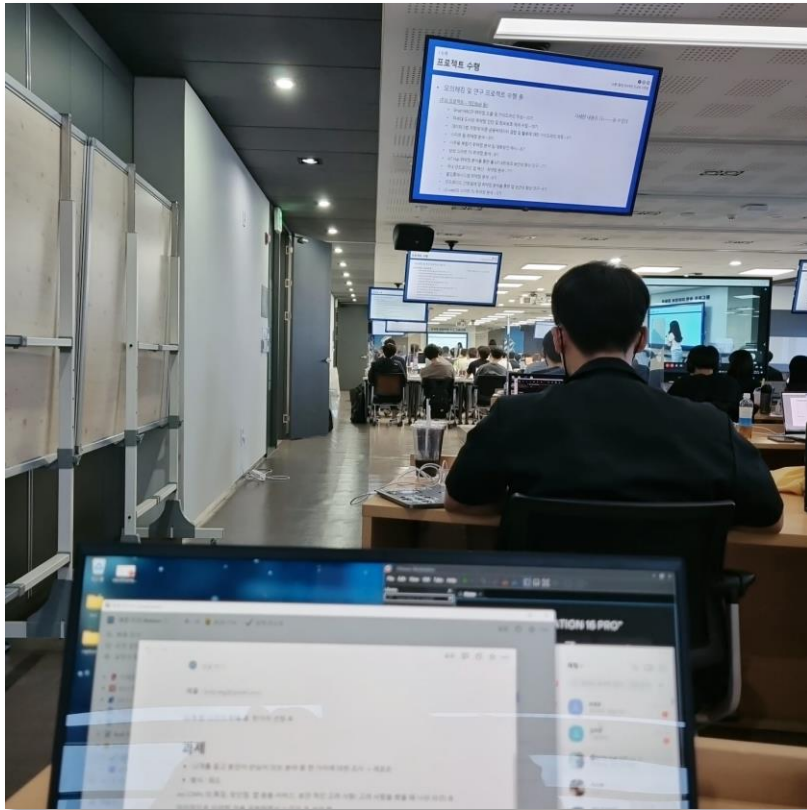
✓ 과제 리스트 (공통)

일본 하고 쉬자.

Board View

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) 18:59:5	완료	✓
📄 [web] OWASP 10 (1)	정도원	7/22(금) 18:59:5	완료	✓
📄 [web] source code patch	정도원	7/22(금) 18:59:5	완료	✓
📄 [web] XSS	정도원	7/22(금) 18:59:5	완료	✓
📄 [zer0day] with Junction Part	신정훈	7/23(토)	유지통	☐
📄 [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	✓



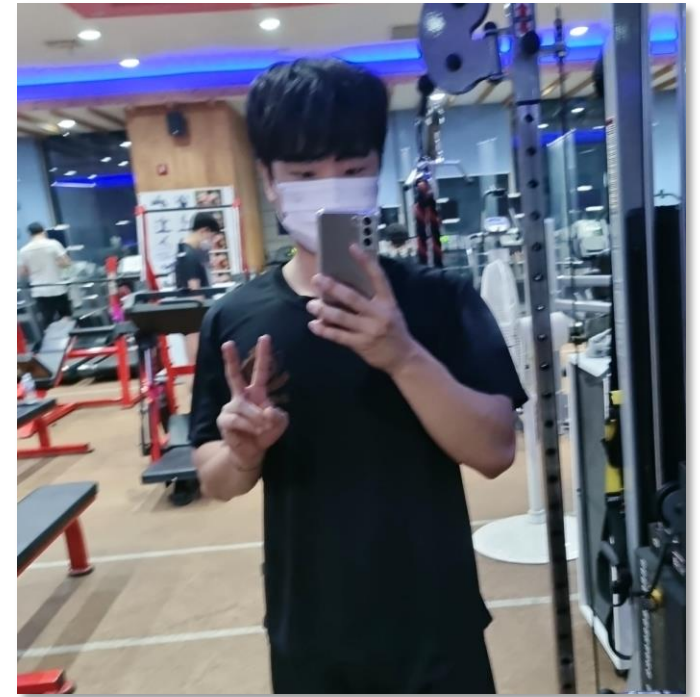




카페인



동선 최소화



샤워용 헬스

트랙 안내

취약점 분석

개념	학습내용
<ul style="list-style-type: none"> ▪ 보안 취약점이 발생하는 원인 이해 ▪ 사고를 미연에 방지하기 위한 정보보안 기술의 트렌드 학습 	<ul style="list-style-type: none"> ▪ 리버스 엔지니어링 기법 ▪ 취약점 이해 ▪ 네트워크, 운영체제원리

보안 컨설팅

개념	학습내용
<ul style="list-style-type: none"> ▪ 최신 정보보안 정책 및 관리 체계에 대해 학습 ▪ 컨설팅 기법 및 법제도에 대한 이해를 통해 컨설팅 기초소양 배양 	<ul style="list-style-type: none"> ▪ 보안컨설팅 기법 ▪ 보안인증체계 및 법/제도 ▪ 감사 및 산업보안 ▪ 보안 시장 동향

디지털 포렌식

개념	학습내용
<ul style="list-style-type: none"> ▪ 디지털 포렌식 기초 개념 이해 ▪ 실 사례연구를 통해 활용방안을 익히며 사례실습 	<ul style="list-style-type: none"> ▪ 디지털 포렌식 기초 개념 ▪ 침해사고 시스템 분석 ▪ 시스템 분석 절차 연구 ▪ 적용 사례 연구

보안제품개발

개념	학습내용
<ul style="list-style-type: none"> ▪ 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 	<ul style="list-style-type: none"> ▪ 개발보안 방법론 ▪ 소프트웨어 개발 보안 ▪ 개발보안 강화 활동 ▪ 개발보안 구현

오늘	<	>	2022년 8월	🔍	🔗	⚙️	📅	📱
월 8월 1일	화 2	수 3	목 4	금 5	토 6	일 7		
<ul style="list-style-type: none"> 오전 9시 [박의성] HTTP request smi 오후 11시 소개팅 회의 	<ul style="list-style-type: none"> 오전 9시 [정진호] Advanced Exploit 오후 4시 총동문회 설명회 오후 4시 총동문회 설명회 오후 7시 [이강석] 모의해킹 실습 초급 	<ul style="list-style-type: none"> 오후 2시 [박전성] 취약점을 찾는 다영! 오후 6시 [이강석] 모의해킹 실습 초급 	<ul style="list-style-type: none"> 오전 9시 [최정수] SSRF 멧집 오후 2시 [신정훈] Windows Device D 오후 11시 소개팅 회의 	<ul style="list-style-type: none"> 오전 9시 [정진호] All about fuzzing t 오후 2시 [강인욱] 웹 어플리케이션 익: 오후 7시 [최정수] Android Deep Link 	<ul style="list-style-type: none"> 오후 1시 [박의성] HTTP request smi 오후 2시 [강인욱] 웹 어플리케이션 1-d 	<ul style="list-style-type: none"> 오후 2시 [정광운] Linux kernel 1day 오후 7시 [이상섭] 임베디드 해킹 - AR 		
8	9	10	11	12	13	14		
<ul style="list-style-type: none"> 오전 9시 [정진호] Advanced Exploit 오후 2시 [이강석] 모의해킹 실습 중급 오후 6시 [이강석] 모의해킹 실습 중급 오후 9시 소개팅 회의 	<ul style="list-style-type: none"> 강학박진 오후 2시 [박전성] 피싱 실습 #1 #Syst 오후 7:30 [BoB특강] Market trends i 오후 7:30 [BoB특강] Market trends i 	<ul style="list-style-type: none"> 오후 2시 [박전성] 피싱 실습 #2 #Syst 	<ul style="list-style-type: none"> 오전 11시 [BoB특강] 사이버보안의 미 오전 11시 [BoB특강] 사이버보안의 미 오후 2시 [박전성] 피싱 실습 #3 #Syst 오후 2시 소개팅 예선 	<ul style="list-style-type: none"> 오후 2시 [박전성] 피싱 실습 #4 #Syst 	<ul style="list-style-type: none"> 오후 2시 [심영진] 게임 엔진별 특성 및 	<ul style="list-style-type: none"> 오전 10시 [심영진] Windows 게임 핵 오후 2시 [정광운] SLUB 구조 및 Mitig 		
15	16	17	18	19	20	21		
관복일 <ul style="list-style-type: none"> 오후 2시 [심영진] Android 게임 핵 분 오후 6시 술술 	2학기 수강신청 <ul style="list-style-type: none"> 오전 9시 [정진호] Advanced Exploit 오후 2시 [지현석] IPC 보안기술 실습 # 오후 6시 [이강석] 모의해킹 실습 고급 	<ul style="list-style-type: none"> 오후 6시 [박전성] 피싱 실습 #5 #Syst 	중국의 MT <ul style="list-style-type: none"> 오후 2시 [신정훈] Browser 버그헌팅 ! 	<ul style="list-style-type: none"> 오후 2시 [강인욱] Advanced Web Ha 	<ul style="list-style-type: none"> 오전 9시 [김재기] Threat Actor Track 오후 2시 [정광운] Linux kernel 1day 	<ul style="list-style-type: none"> 오전 9시 [정진호] Advanced Exploit 오후 1시 [이상섭] 임베디드 해킹 - AR 오후 7시 [Julien] A startup secured 오후 7시 [Julien] A startup secured 		
22	23	24	25	26	27	28		
2학기 수강신청 <ul style="list-style-type: none"> 2학기 유학신청기 오후 2시 [박전성] 펌웨어 리보스팅 #S 	<ul style="list-style-type: none"> 오전 10시 [최정수] Frida 기초 오후 1시 [최정수] 워드 프로세서 문서 오후 7시 [최정수] Frida를 활용한 레인 	유학신청 [광원석] <ul style="list-style-type: none"> CTF 포스터 마감 (무수) 오전 9시 [이기택,이종호,최정수] BoB 	유학시험[조규] <ul style="list-style-type: none"> 오전 10시 총동문회 설명회 오전 10시 총동문회 설명회 5개 더보기 	오후 12시 프로젝트 팀일일				
29	30	31	9월 1일	2	3	4		
2학기 개강일			워부세미나 포스터 출력	<ul style="list-style-type: none"> 오후 7시 [이경훈] 네트워크 	A그룹 프로젝트 리오트(10:00~16:30) <ul style="list-style-type: none"> 오후 4시 부등산 계획 오후 7시 [윤기순] ECC, PQC 입문 1 	<ul style="list-style-type: none"> 오후 12시 [박수현] 쿠버네티스 개요 오후 3시 [박수현] 쿠버네티스 개발 및 오후 7시 [윤기순] ECC, PQC 입문 2 		

과제 리스트 (트랙교육)

후딱하고.. 쉬자...

필터

↑ 기한

이소연

기한

+ 필터 추가

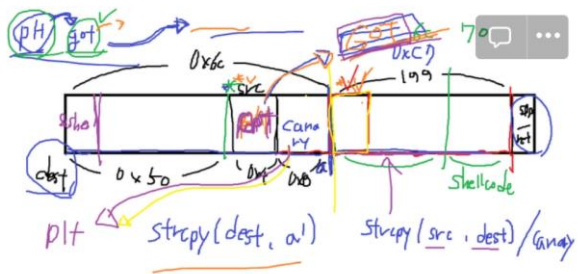
정렬

...

새로 만들기

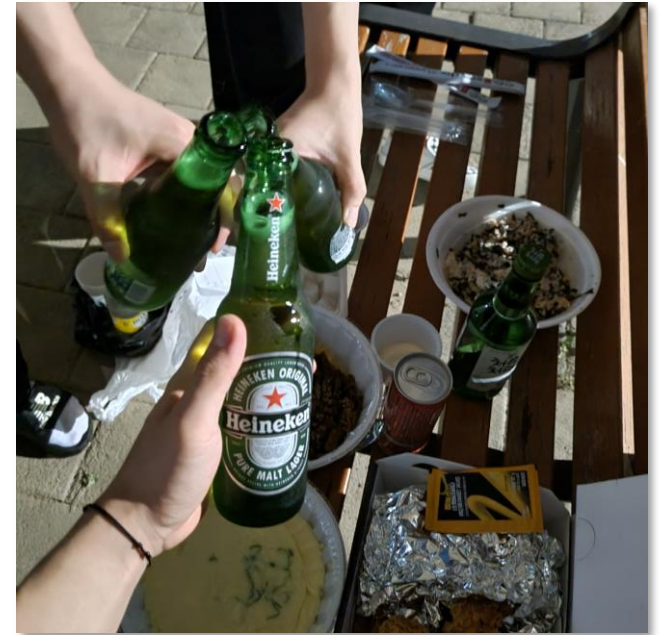
과제	멘토님	기한	김지연	이소연	이예준
[Embedded] Firmware extraction	이상섭	07/31/2022	complete	complete	complete
[Yara] target attack analysis	Anthony	08/03/2022	drop	drop	drop
통신구간 암호화 관련 recv 함수 찾기	최정수	08/05/2022	complete	complete	complete
원하는 싱글 게임 핵 만들기	최정수	08/05/2022	complete	complete	complete
PayPal - Smuggling	박의성	08/05/2022	complete	submit	submit
openssl Hooking	이상섭	08/07/2022	complete	complete	complete
Migrating to 64-Bit 논문 정리	박전성	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)	김종현	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

고생의 흔적



문제풀이

strcpy를 두번하고 안의 src 포인터 변수가 덮어질 수 있기 때문에 이 값을 조작하여 got



열심히 할땐 하고..

잠자리의 진화..

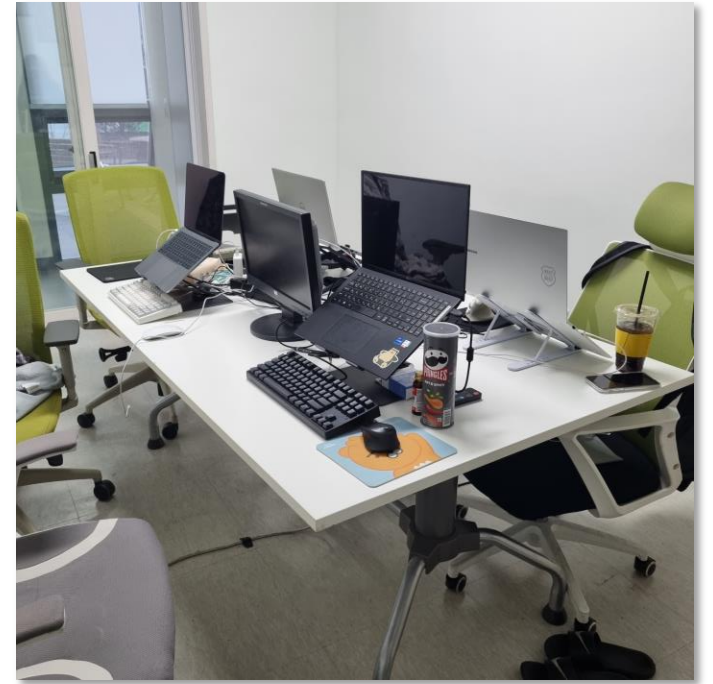
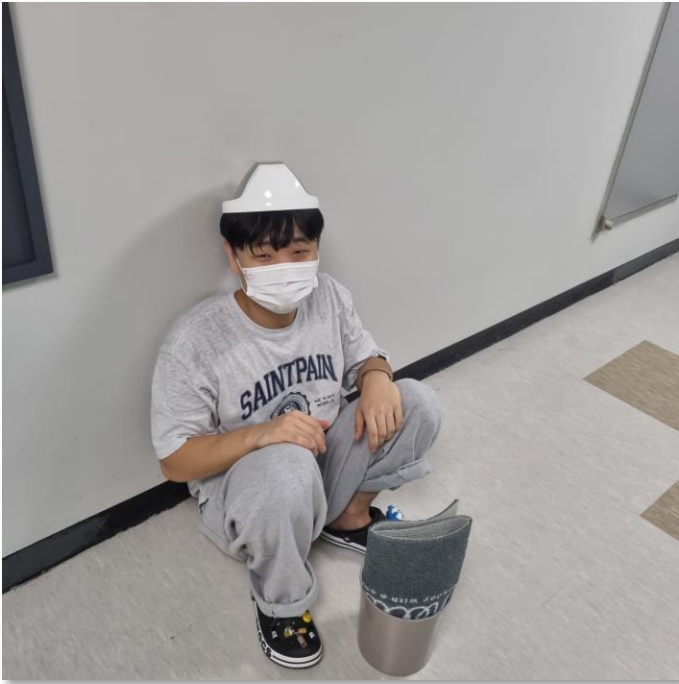
에라 모르겠다



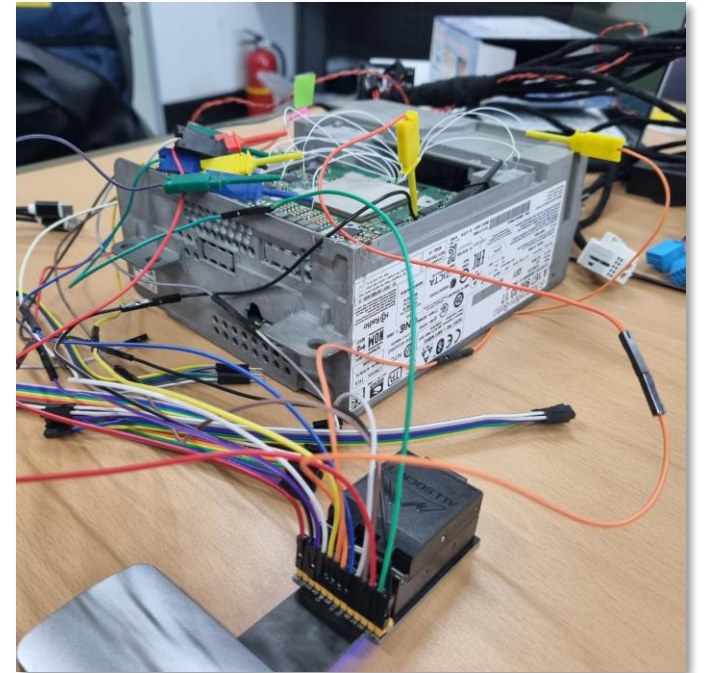
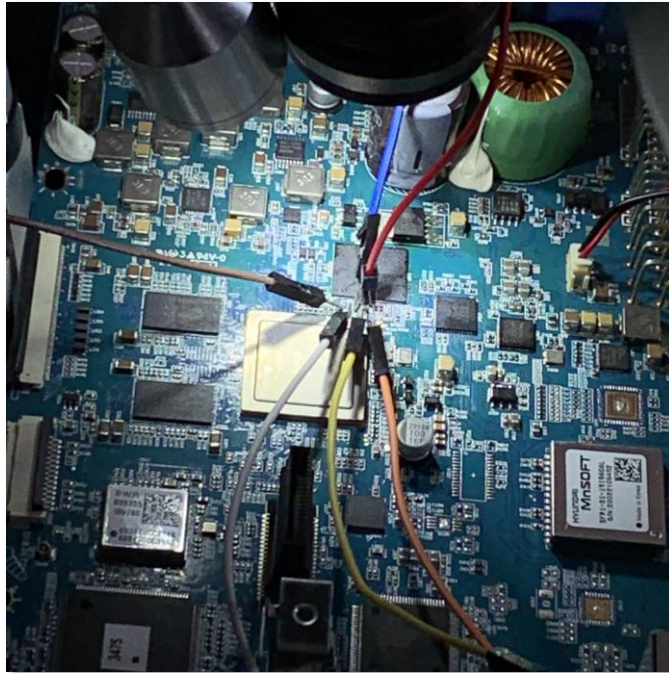
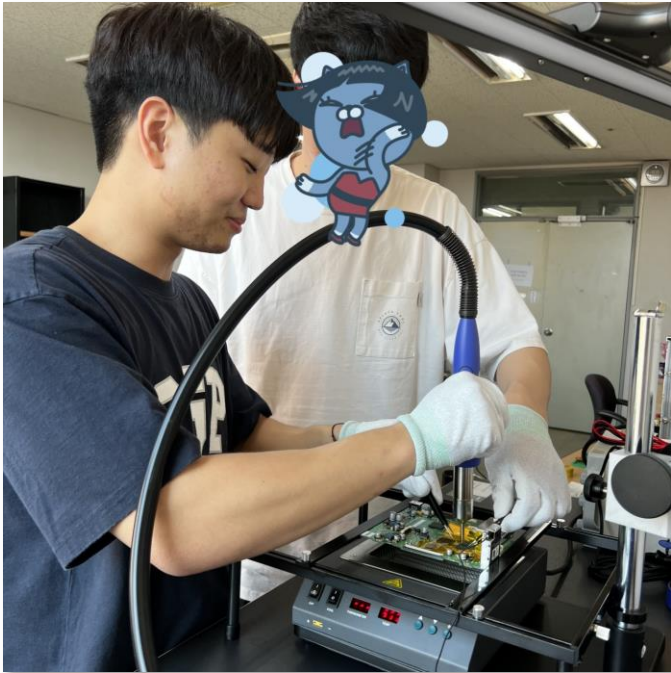
팀 구성

5인 1조

자유롭게 구성







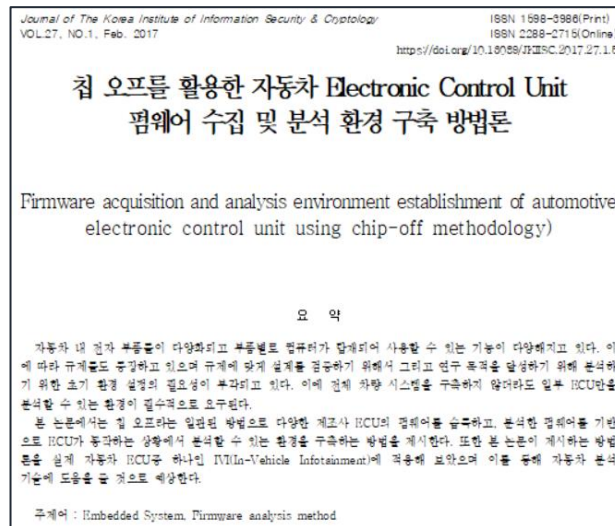
🔍 분석 ...		
📄 Aa Name	👤 Responsibility	🕒 Property
🔒 Tivoli backdoor 사용 방법	예준 이	2023년 1월 12일 오후 5:34
⚙️ 가상 환경 구축	진명 박	2023년 1월 1일 오후 11:16
🔍 Tivoli IVI 내부 기능 분석	Yujin Bae	2023년 1월 1일 오후 11:16
⚠️ 분석 시 주의사항		2023년 1월 1일 오후 11:16
🔍 QNX	eigenkyeong	2023년 1월 1일 오후 11:16
🔍 QNX 파일시스템 분석	eigenkyeong	2023년 1월 1일 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 - Small 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 ... +			
📄 Aa Name	🕒 Due Date	👤 Responsibility	🟢 Status
🔒 마무리	2022년 12월 17일	안상혁 Yujin Bae	🟢 Done
🔍 동적 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





11월 8일 진행된 Codegate 2022
BoB Session에서 발표 진행



학술지 투고 예정 (2023. 04)



취약점 제보

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.



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.

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