



별 짚기도 못하던 내가 버그바운티를 하게 되었다?

: 보안 입문자가 화이트햇 스쿨에서 살아남기

화이트햇 스쿨 2기 교육생 명서아

CNTENTS

2024 29th Summer H4cking C4mp

01

명서아가 누구야

- 자기소개
- 보안 입문 과정

02

내가 버그바운티를?

- WHS 합격 여정
- 프로젝트에서 살아남기
- 프로젝트를 마치며

03

추후 계획

- WHS
- 개인 학습 및 목표
- 최종 목표

01

CHAPTER

명 서 아 가 누 구 야



01. 명서아가 누구야 : 자기소개



NAME 명 서 아



BIRTHDAY



별나라새싹
대표 업적 없음



1973-07-03



FIELD 모바일, 포렌식



GROUP 화이트햇 스쿨 2기 교육생



RANGE 대전, 천안, (가끔)충북



LIKE 책, 거북이, 빵, 수면



NICKNAME 멩더아, astronaut



01. 명서아가 누구야? : 보안 입문 과정



중학생 명서아



정보보호 영재교육원 지원



나우미래 Episode 06

해커 잡는 해커
화이트 해커



EO

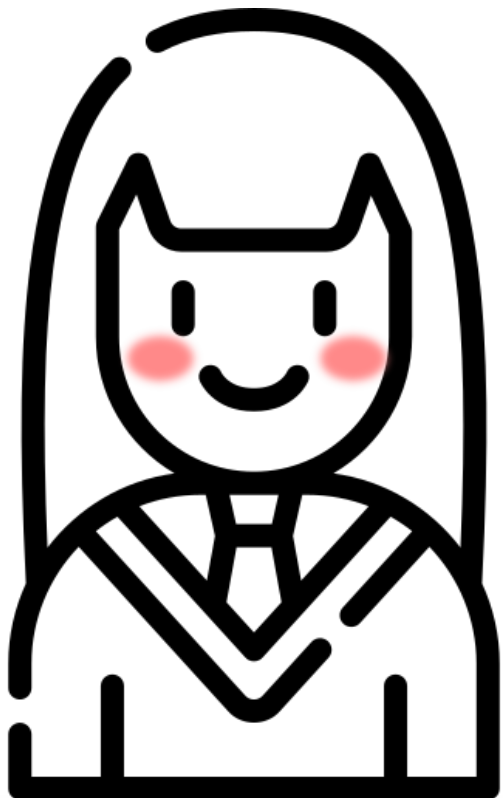
지한별님 화이트해커
소개 영상 시청



BOB를 포함한 다양한
보안 관련 단체 인식



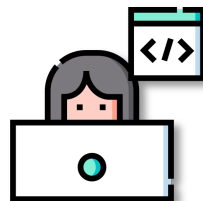
01. 명서아가 누구야? : 보안 입문 과정



고등학생 명서아



디지털 포렌식 기술 인식



누군가에게 실질적인 도움을 줄 수 있는
포렌식 전문가를 꿈꾸게 됨

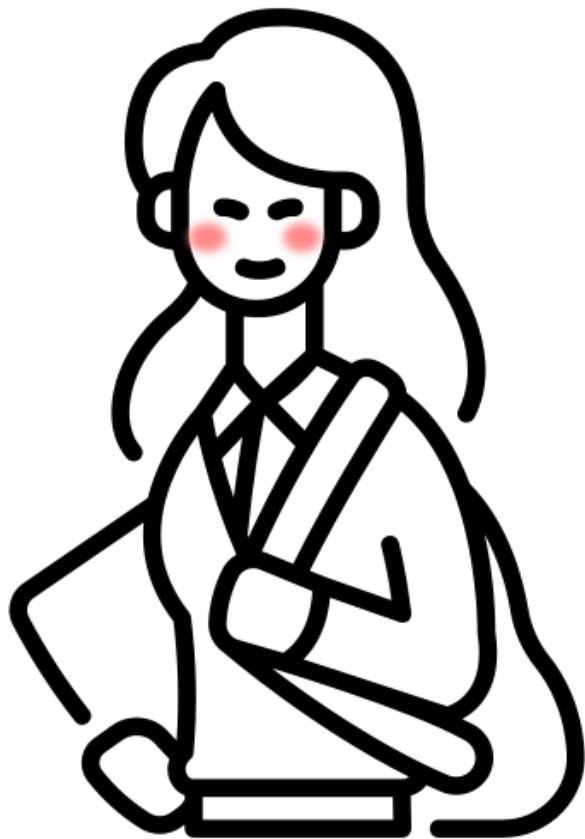


To. 명서아님
감사합니다!
파이팅!!
2023.8.12
박환

컨퍼런스 참가 및
보안 기초 관련 지식 함양



01. 명서아가 누구야? : 보안 입문 과정



대 학생 명서아



진로 고민 및 다양한 분야 경험



제 9회 BOB 정보보안
컨퍼런스 참여



화이트햇 스쿨
WhiteHat School

WhiteHat School
2기 교육생





깜짝 퀴즈!

명서아가 거북이를 좋아하는 이유를
말해보시오!

02

CHAPTER

내가 버그바운티를?



02. 내가 버그바운티를? : WHS 합격까지

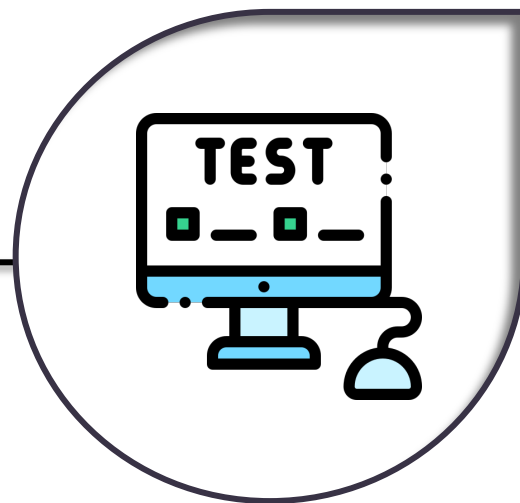
WHS 2기 지원 목표



지원을 위한 준비



WHS 2기 시험



WHS 2기 불합격?

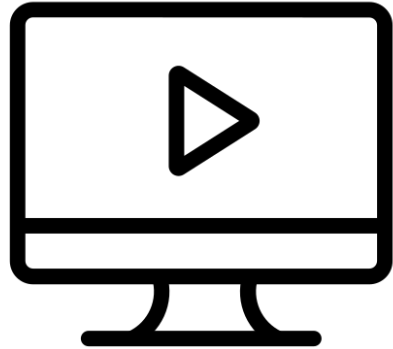
[Web발신]
안녕하세요. 한국정보기술연구원
BoB센터입니다.
화이트햇 스쿨 2기 추가합격을
축하드립니다.



02. 내가 버그바운티를? : 프로젝트에서 살아남기

- 프로젝트 선택 계기

모바일 취약점 강의



모바일 취약점 과제



02. 내가 버그바운티를? : 프로젝트에서 살아남기

- 프로젝트 소개

모바일 앱 취약점 자동화 연구



MOBSF



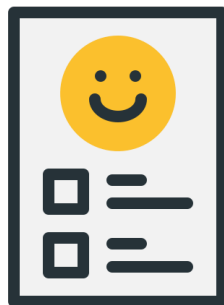
OSTORLAB

⋮

복잡한 결과 도출

긴 시간 소요

편의성 저하



식별하기 쉬운
결과 도출



시간 절약

apk 파일 다운 후
jadx 디컴파일
과정 자동화



사용성 편리

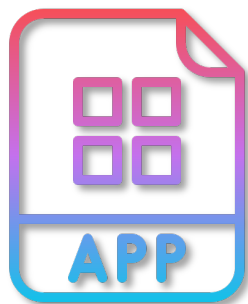
모든 OS에서
호환성 보장 및
실행 구성 편리



02. 내가 버그바운티를? : 프로젝트에서 살아남기

- 프로젝트 과정 : 버그바운티

STEP 1



대상 앱 선정

버그바운티 플랫폼 사용
Hackerone, 파인더갭 등

STEP 2



APK 분석 툴 사용

APK 디컴파일 툴 사용
Jadx-gui 등

STEP 3



취약점 분석

Android Manifest 부터 확인
코드를 읽으며 취약점 분석



02. 내가 버그바운티를? : 프로젝트에서 살아남기

- 프로젝트 과정 : 버그바운티

 **서아**

📄 MainActivity 찾는 방법

📄 Deep Link & [REDACTED] 확인

📄 [REDACTED] 확인

👤 SqlCipher

📄 SQLCipher로 SQLite3 암호/복호화

📄 암호화/복호화

📄 SQLCipher DB파일 decrypt 하기

📄 쿼리문

📄 웹뷰

📄 logging

📄 Android Manifest Provider

😊 🍀 힐내자 !!

프로바이더 기능 더 찾아보기 - 악용해서 외부 앱을 이용해서 sqlInjection → 해커원에서 sqlInjection 사례 찾아보기

1. Provider 공부
2. Provider 부분에서 취약점이 어떻게 발생할 지 생각하며 hackerone에서 사례 찾아보기
→ SQL injection android hackerone 등 검색하면 프로바이더 이용한 사례가 있을 것. 다른 취약점의 사례도 있을 수 있다.

[REDACTED] 취약점 진단 보고서 | ASAP |

화이트햇 스쿨
WhiteHat School

[REDACTED]

취약점 진단 보고서

| 소속 : 화이트햇 스쿨 2기

| 진단자 : ASAP 이예은 명서아

| 진단 기간 : 2024.6.1 ~ 2024.6.15

2024.06.17.

화이트햇 스쿨 2기

Page 1 of 20

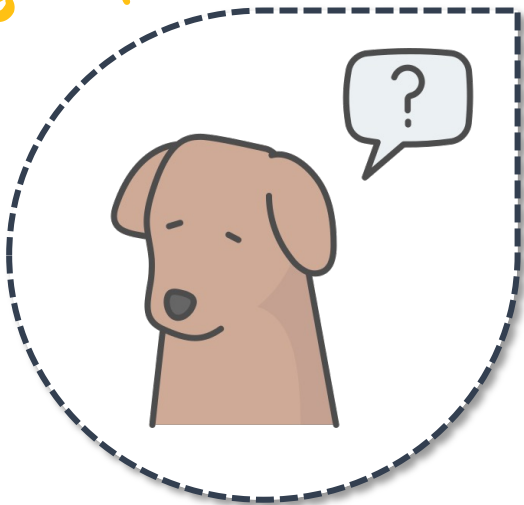
[REDACTED] 취약점 진단 보고서 | ASAP |



02. 내가 버그바운티를? : 프로젝트에서 살아남기

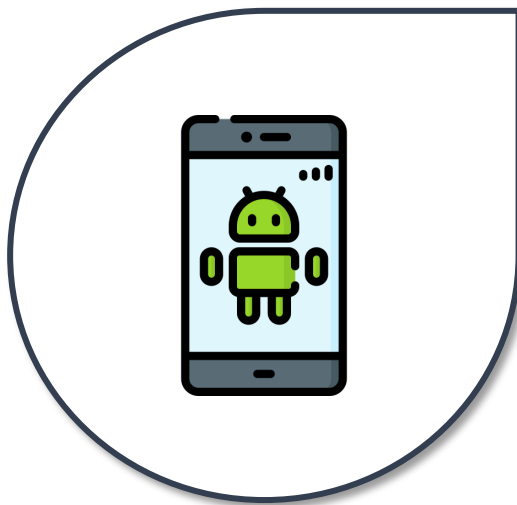
- 프로젝트 과정 : 개인 공부

CUE가 뭐지...? 버그바운티...?

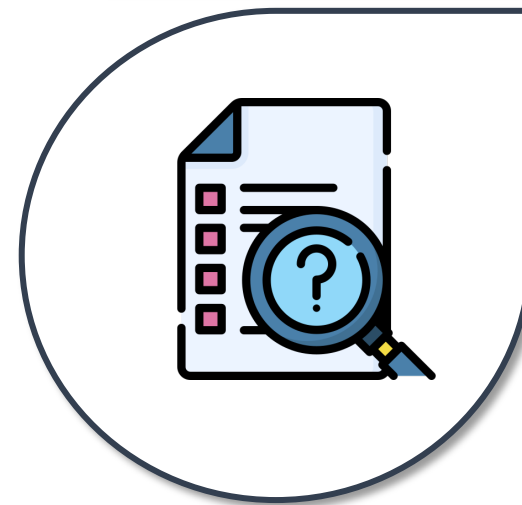


난 별찍기도 잘 못하는데...
내가 할 수 있을까...?

Android 취약점 지식



버그바운티 관련 지식



02. 내가 버그바운티를? : 프로젝트에서 살아남기

- 프로젝트 과정 : 개인 공부



DIVA

- 1 번 : INSECURE LOGGING
- 2 번 : HARDCODDING ISSUES - PART1
- 3 번: INSECURE DATA STROAGE - PART 1
- 4 번 : INSECURE DATA STORAGE - PART 2
- 5 번 : INSECURE DATA STORAGE - PART3
- 6 번 : INSECURE DATA STORAGE - PART4
- 7 번 : INPUT VALIDATION ISSUES - PART1
- 8 번 : INPUT VALIDATION ISSUES - PART 2
- 9 번 : ACCESS CONTROL ISSUES - PART 1
- 10 번 : ACCESS CONTROL ISSUES - PART 2
- 11 번 : ACCESS CONTROL ISSUES - PART 3
- (*)12 번 : HARDCODING ISSUES - PART 2
- (*)13 번 : INPUT VALIDATION ISSUES - PART 3

Frida

- Frida란?
- 1. Change class challenge_01's variable'call01' to: 1
- 2. Run chall02()

개인 공부

▶ 공부 방법

- XSS
- SQL Injection
- Deep Link
- URI, URL 차이점
- CSRF
- Webview
- 암호화/복호화
- Android Manifest Provider 기능
- python
- API와 XML의 상관관계

2024 년 06 월 07 일 금요일		오늘 하루 공부시간											
		목표시간	6 시간 30 분										
		달성시간	9 시간 25 분										
과목		10분 단위 시간체크											
ASAP	SQLInjection DBHook 공부	6											
	SQLInject 복호화 59 단계	7											
	21:00 보안 개념	8											
		9											
		10											
		11											
기타	방 청소	12											
	6.7 공월 계획한 재귀	1											
	비트바운티 연계 할바베키	2											
		3											
		4											
총	XSS 공부 (종료)	5											



02. 내가 버그바운티를? : 프로젝트에서 살아남기

- 프로젝트 과정 : 개인 공부



5월 14일 화요일

[Web발신]

휴학이 최종승인되었습니다.

오후 4:28

공부시간

◀ 5월 ▶

월	화	수	목	금	토	일
29 02:40	30 07:07	1 00:55	2	3	4 00:51	5 05:15
6 07:52	7 06:14	8 00:01	9 02:03	10 10:53	11 00:18	12 00:55
13 02:01	14 05:07	15 03:13	16 04:40	17 02:33	18 05:03	19 01:18
20 07:01	21 04:15	22 02:41	23 02:45	24 07:23	25 03:00	26
27 00:14	28 07:25	29 01:31	30 00:50	31 08:15	1 01:05	2 04:11

공부시간

◀ 6월 ▶

월	화	수	목	금	토	일
27 00:14	28 07:25	29 01:31	30 00:50	31 08:15	1 01:05	2 04:11
3	4	5	6 01:51	7 09:25	8 07:48	9 06:26
10 00:16	11 00:20	12 06:45	13 07:12	14 07:58	15 06:16	16 08:20
17 07:03	18 06:41	19 01:33	20 01:06	21 04:25	22 04:15	23 03:35
24 04:48	25 15:38	26 07:56	27 07:56	28 07:34	29 07:43	30 09:03



02. 내가 버그바운티를? : 프로젝트에서 살아남기

- 프로젝트 과정 : 내가 맡은 역할 - 도구 개발

Permission

- Permission은 OWASP Mobile Top 10에 포함되지 않음
- 앱에 불필요하게 많은 권한이 있는 경우
- 향후에 취약점으로 파급력이 커질 수 있음

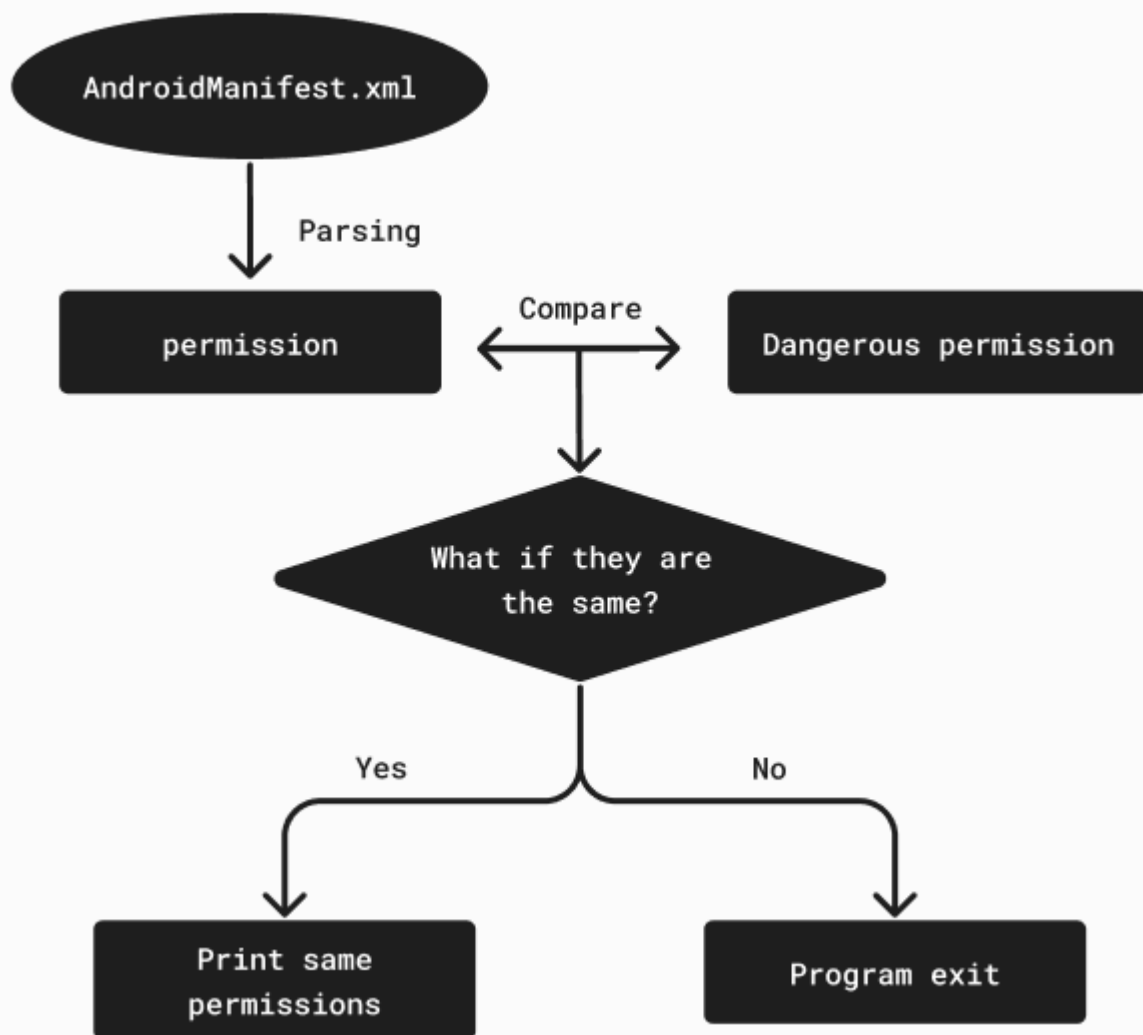
Log

- OWASP Mobile Top 10
M9 안전하지 않는 데이터 저장
- log.v, log.i, log.e, log.d, log.wtf
민감한 데이터 확인 가능
- log { } 괄호 안에 있는
session, token 등의 키워드로
민감한 데이터 확인 가능



02. 내가 버그바운티를? : 프로젝트에서 살아남기

- 프로젝트 과정 : 내가 맡은 역할 - 도구 개발

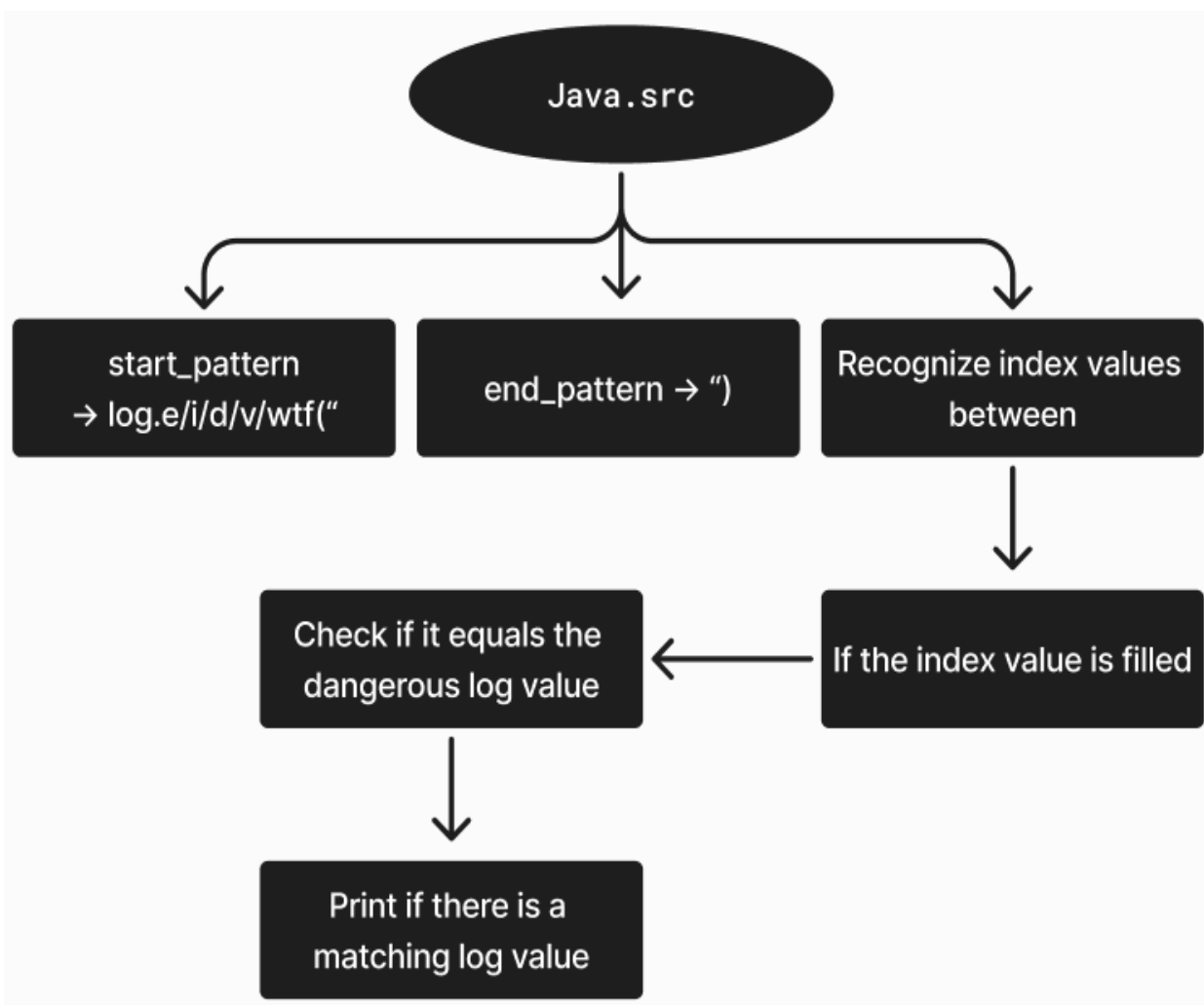


```
class PermissionAnalyzer:
    def __init__(self):
        self.dangerous_Permissions = [
            "android.permission.READ_CALENDAR",
            "android.permission.WRITE_CALENDAR",
            "android.permission.CAMERA",
            "android.permission.READ_CONTACTS",
            "android.permission.WRITE_CONTACTS",
            "android.permission.GET_ACCOUNTS",
            "android.permission.ACCESS_FINE_LOCATION",
            "android.permission.ACCESS_COARSE_LOCATION",
            "android.permission.RECORD_AUDIO",
            "android.permission.READ_PHONE_STATE",
            "android.permission.CALL_PHONE",
            "android.permission.ADD_VOICEMAIL",
            "android.permission.USE_SIP",
            "android.permission.READ_CALL_LOG",
            "android.permission.WRITE_CALL_LOG",
            "android.permission.SEND_SMS",
            "android.permission.RECEIVE_SMS",
            "android.permission.READ_SMS",
            "android.permission.RECEIVE_WAP_PUSH",
            "android.permission.RECEIVE_MMS",
            "android.permission.READ_EXTERNAL_STORAGE",
            "android.permission.WRITE_EXTERNAL_STORAGE",
        ]
]
```



02. 내가 버그바운티를? : 프로젝트에서 살아남기

- 프로젝트 과정 : 내가 맡은 역할 - 도구 개발



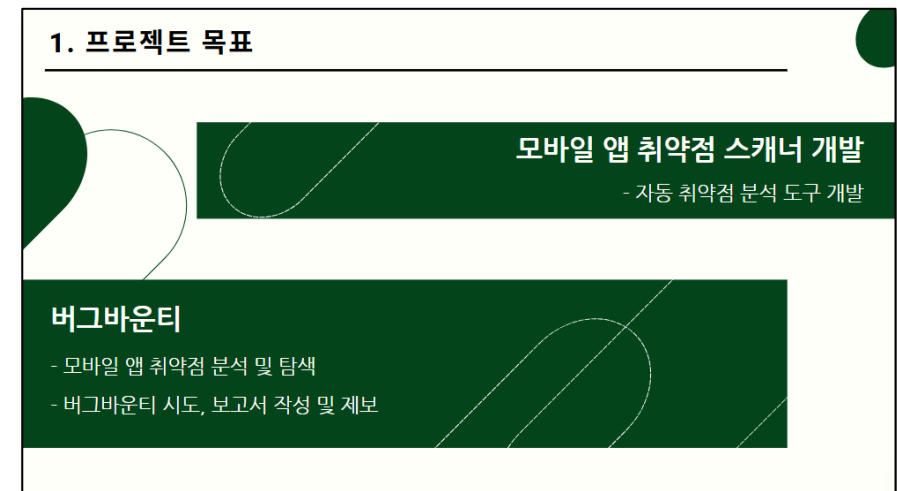
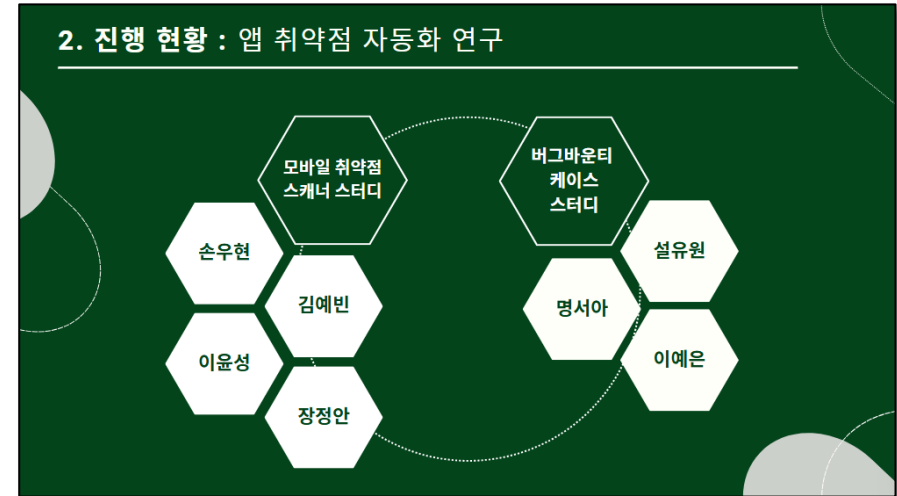
```
def contains_sensitive_info(self, message):  
    sensitive_keywords = [  
        'access_token', 'password', 'secret', 'admin_id',  
        'adminId', 'admin_pw', 'adminPw', 'admin_password',  
        'admin_secret', 'api_secret', 'user_id', 'userId',  
        'user_pw', 'userPw', 'user_password', 'user_secret',  
        'api_key', 'private_key', 'privateKey', 'private_token',  
        'privateToken', 'auth_token', 'authToken', 'credit_card',  
        'ssn', 'pin_code', 'session_id', 'IP_address', 'IPaddress',  
        'Cookies', 'Cookie', 'SESSIONID'  
    ]
```

```
def extract_messages(self, content):  
    results = []  
    log_levels = ['v', 'd', 'i', 'e', 'w', 'wtf']  
  
    lines = content.split('\n')  
  
    for level in log_levels:  
        pattern = f'Log\\. {level.upper()}\\(''  
  
        for line_num, line in enumerate(lines, start=1):  
            if not self.is_ignored(line):  
                if re.search(pattern, line, re.IGNORECASE):  
                    if self.contains_sensitive_info(line):  
                        results.append((line_num, line))  
  
    return results
```



02. 내가 버그바운티를? : 프로젝트에서 살아남기

- 프로젝트 과정 : 내가 맡은 역할 - PPT 제작



02. 내가 버그바운티를? : 프로젝트에서 살아남기

- 프로젝트 과정 : 내가 맡은 역할 - PPT 제작



모바일 앱 취약점 자동화 연구

이예은 김예빈 명서아 설유원 손우현 이윤성 장정안 | 김주원 멘토님 | 박성광 PL님
이예은: 취약점 발견, 취약점 도출, 취약점 분석, 취약점 검증, 취약점 보고, 취약점 조치, 취약점 모니터링, 취약점 관리, 취약점 개선, 취약점 평가, 취약점 측정, 취약점 분석, 취약점 검증, 취약점 보고, 취약점 조치, 취약점 모니터링, 취약점 관리, 취약점 개선, 취약점 평가, 취약점 측정

1. 프로젝트 소개

1-2. 프로젝트 목표 및 필요성



복잡한 결과 도출

긴 시간 소요

편의성 저하



식별하기 쉬운
결과 도출



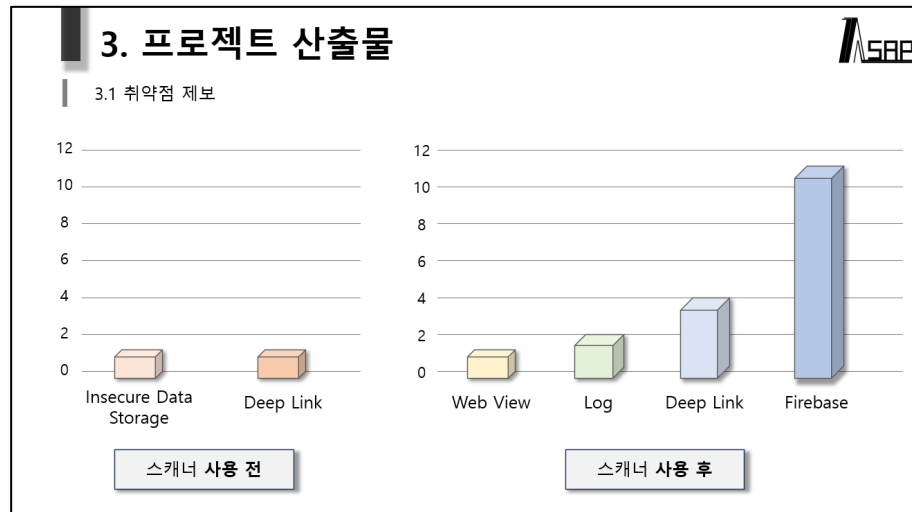
시간 절약

apk 파일 다운 후
jadx 디컴파일
과정 자동화



사용성 편리

모든 OS에서
호환성 보장 및
실행 환경 구성 편리



프로젝트를 마치며

2024.04.26 ~ 2024.07.13



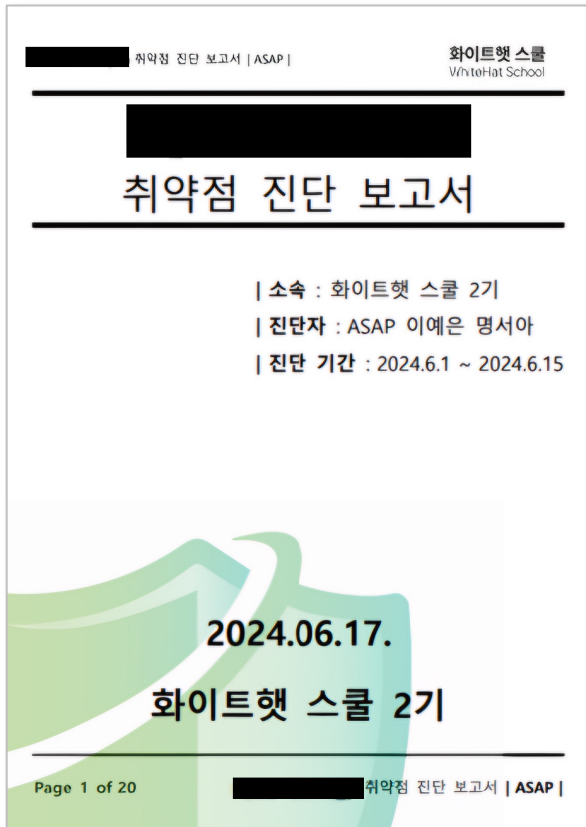
ASAP 팀 만났습니다!
ASAP 팀의 생일 파티!
ASAP 팀의 생일 파티!
ASAP 팀의 생일 파티!
ASAP 팀의 생일 파티!



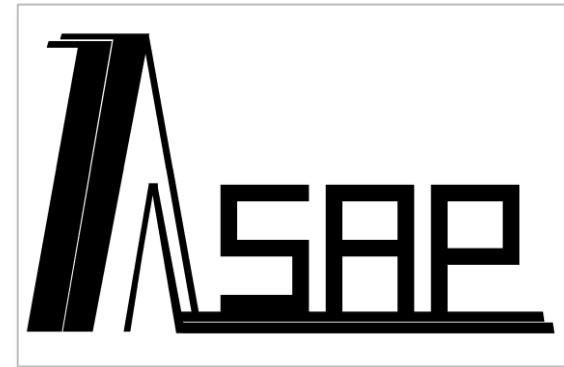
02. 내가 버그바운티를? : 프로젝트에서 살아남기

- 프로젝트 과정 : 내가 맡은 역할 - 보고서 디자인 및 로고 제작

| 보고서 디자인 제작

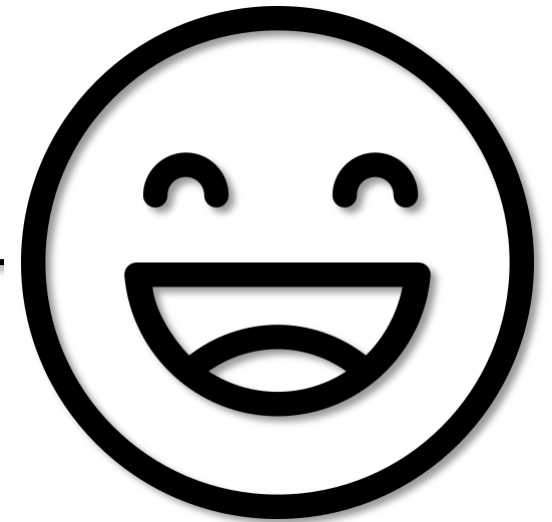
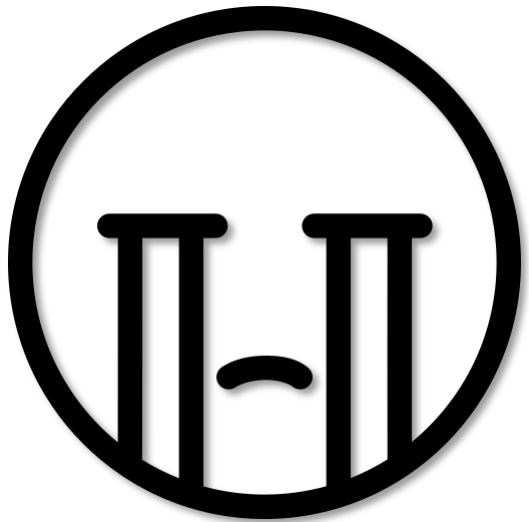


| ASAP 로고 제작



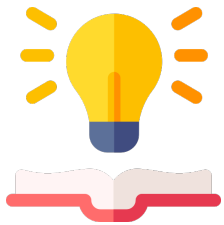
02. 내가 버그바운티를? : 프로젝트에서 살아남기

- 프로젝트 과정 : 멘탈 관리



02. 내가 버그바운티를? : 프로젝트를 마치며

- 프로젝트를 통해 배운 점



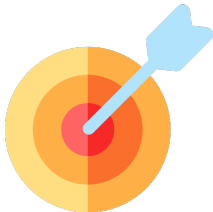
01. 공부 자세

프로젝트를 하기 전에는 이 만큼 열심히 공부에 임한 적이 없었기 때문에 프로젝트를 통해 공부하는 자세를 배우게 됨.



02. 멘탈 관리

멘탈이 약한 편이라 한 번 무너지면 일의 속도가 느려지곤 했지만, 프로젝트를 진행하며 멘토님의 격려 덕분에 멘탈을 빠르게 회복할 수 있었고, 혼자서도 극복하는 능력이 향상됨.



03. 목표 의식

막연하게 꿈꾸던 보안을 공부하고 프로젝트를 진행하면서, 어떤 부분을 집중해야 할지와 희망하는 분야를 명확히 알게 되어 목표 의식이 생기게 됨.



04. 자기 확신감

자기 확신감이 없던 편인데 프로젝트 중도 하차 없이 잘 마치고 나니 자기 확신감이 형성됨.



02. 내가 버그바운티를? : 프로젝트를 마치며

- 프로젝트를 통해 배운 점

Success
성공



what people think
it looks like

사람들이 막연히 생각하는 것

Success
성공



what it really
looks like

실제로는...

그래도
해야지
어떡해



깜짝 퀴즈!

간혹 앱에서 사용하지 않는 '이것'이 많기 때문에
향후 취약점이 발견되었을 때 '이것'은 파급력이 커질 수 있다.

여기서 '이것'은 무엇인가?

03

CHAPTER

추 후 계 획



03. 추후 계획 : WHS

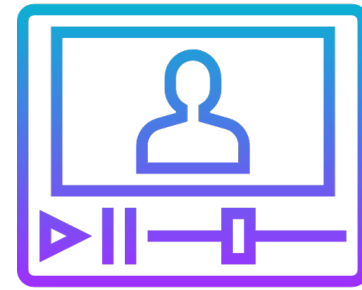
- 프로젝트 고도화 및 3단계



프로젝트 고도화



1단계 교육 수강 및
과제 수행



3단계 교육 수강

03. 추후 계획 : 개인 학습 및 목표

해킹 팀 입단



BOB 15기 합격



해킹캠프 발표자



03. 추후 계획 : 최종 목표

기술적 요소



보안 컨설팅 전문가



예술학적 요소



인문학적 요소

QnA



Discord : 별나라새싹



E-mail : astronaut0703@gmail.com



Facebook : 명서아



Instagram : @a_stronaut07



THANK YOU



지금까지 저의 발표를 들어주셔서 감사합니다

화이트햇 스쿨 2기 교육생 명서아