

# SOS Finder

Sick Open-source Software Finder

1조 SOFA  
송창헌 박민경 정성민  
차진원 정현석 핫산



# 추진배경 및 필요성

# 현 시대는 4차 산업 혁명 시대, 대세는 IoT(사물인터넷)



# IoT 기기의 취약한 오픈소스 사용

[IoT 시대가 온다] “IoT도 오픈소스 리눅스가 지배”

2014.02.18 13:42:49 / 심재석 sis@ddaily.co.kr



[디지털데일리 심재석기자] 지난 1월 미국 라스베이거스에서 열린 소비자가전쇼(CES) 2014 현장은 사물인터넷(IoT)의 미래를 엿볼 수 있는 자리였다. 웨어러블 기기에서부터 스마트가전, 스마트카에 이르기까지 모든 기기가 하나로 연결되는 세상이 열리고 있음을 눈으로 확인할 수 있는 자리였다.

하지만 눈에 보이지 않지만 이 움직임의 중심에 있는 것이 있다. 바로 리눅스(Linux)다. 3D 프린터에서 무인 비행기, 전화, 태블릿, TV, 전기 냄비 등까지 리눅스는 CES 2014 전시회장의 모든 곳에서 만날 수 있었다.

# 취약한 오픈소스 사례

Over 199,500 Websites Are Still Vulnerable to Heartbleed  
OpenSSL Bug

Sunday, January 22, 2017 Swati Khandelwal

57 2.4K 5982



Heartbleed and the Risk to IoT  
"한국, 세계 2위 하트블리드 취약점 보유국"

임민철 기자 | 2017.01.26



쇼단 보고서 "보유조직 SKB·KT·보라넷 등...취약점 서버 세계 20만대"  
세계 각지 웹사이트와 서버 20만곳이 암호화 통신을 엿볼 수 있는 취약점 '하트블리드(Heartbleed)'를 3년째 방치해 온 것으로 드러났다. 이런 서버가 많은 나라 순위를 매기니 미국이 1위, 이어 한국이 2위였다.

하트블리드 서버 (출처=CNET)

IT Pro

ynet

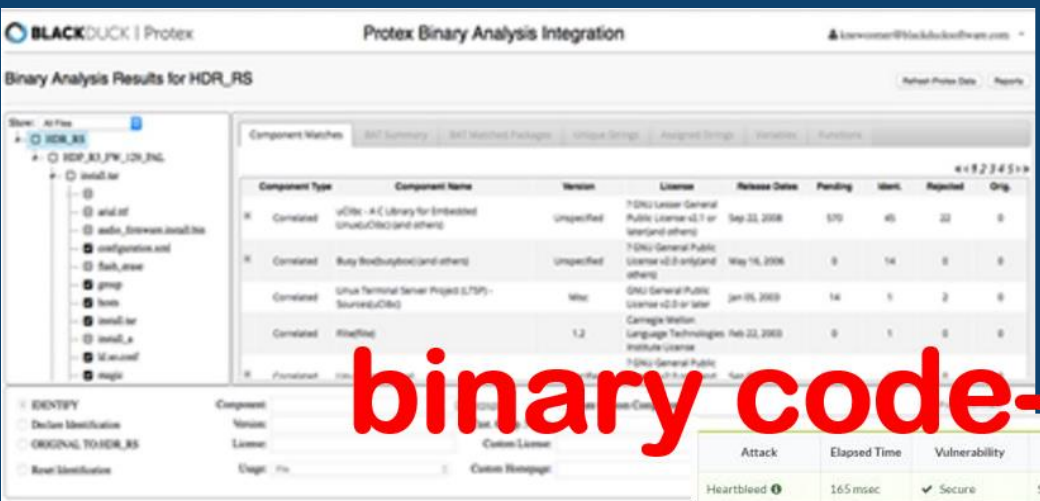
e OpenSSL  
Google security  
:arlier this month,  
atest security  
aise questions  
rity.

?

'sical objects that contain embedded technology to  
ternal states or the external environment." It is  
t within the next decade. According to Gartner  
cted devices could grow to as many as 26 billion  
even higher than that. [More: How Will 26B IoT

Units Affect Data Centers in 2020?]

# 바이너리 코드 기반 진단의 필요성



binary code-based

BAT Tools

For License

IoTcube (WhiteBox)

Source code-based

Attack	Elapsed Time	Vulnerability	Description
Heartbleed	165 msec	Secure	Server returned error, likely not vulnerable.
RCA attack	59 msec	Vulnerable	The target server selected 'TLS_ECDHE_RSA_WITH_RC4_128_SHA' which is included in vulnerable cipher suites.
SLOTH attack	15 msec	Secure	The target server does not support MD5 and SHA1 algorithm.
Drown attack	77 msec	Secure	Server does not support SSLv2. It is secure against CROWN attack.
POODLE attack	65 msec	Vulnerable	The target server selected CBC mode cipher suite with SSLv3.

Heartbleed

CVE-2014-0160

National Vulnerability Database (NVD)

Detail Description

Heartbleed is a security bug disclosed in April 2014 in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol. Heartbleed may be exploited regardless of whether the party using a vulnerable OpenSSL instance for TLS is a server or a client. It results from improper input validation (due to a missing bounds check) in the implementation of the TLS heartbeat extension, that the bug's name derives from "heartbeat". The vulnerability is classified as a buffer over-read[5]a situation where more data can be read than should be allowed.

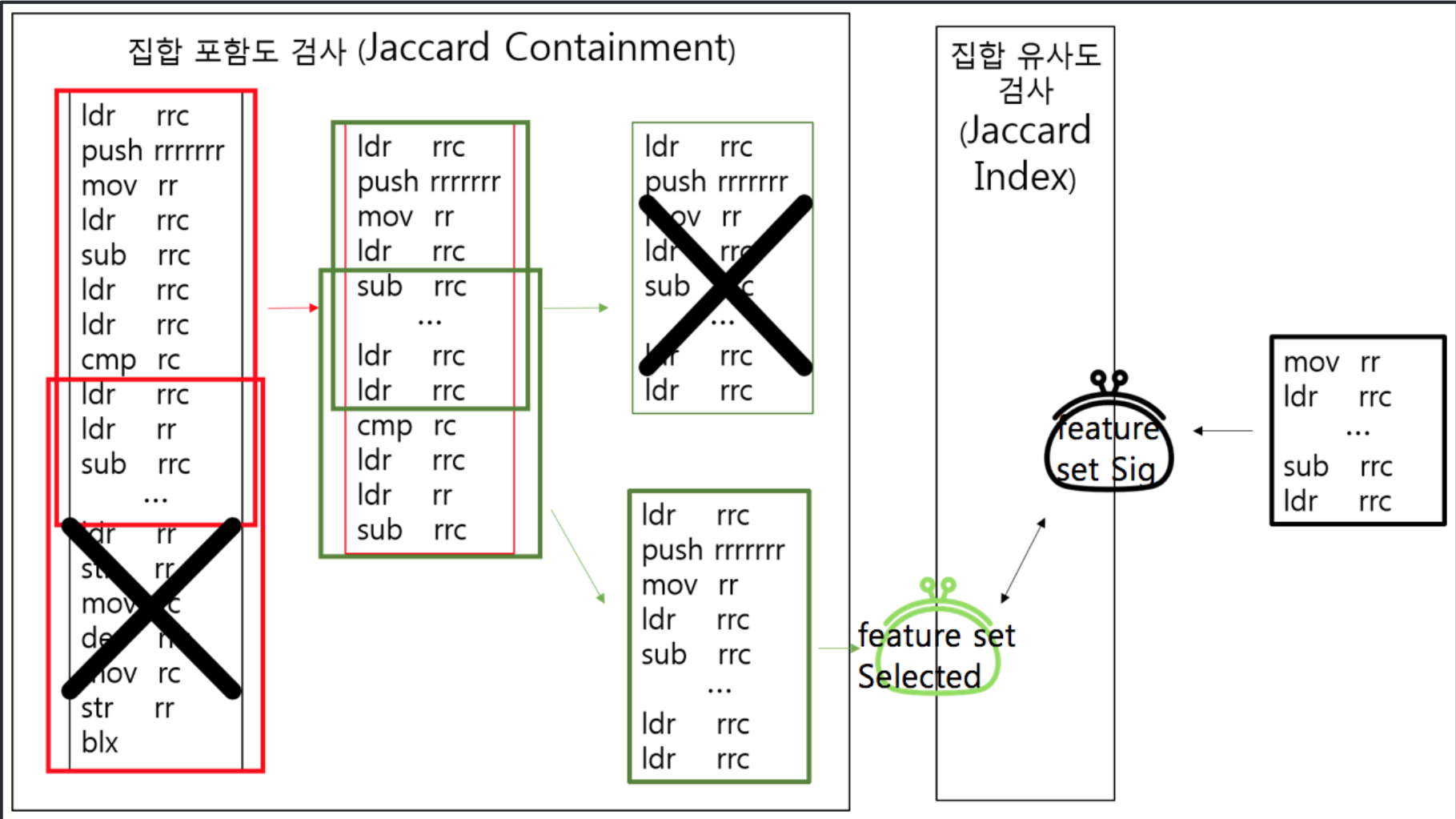
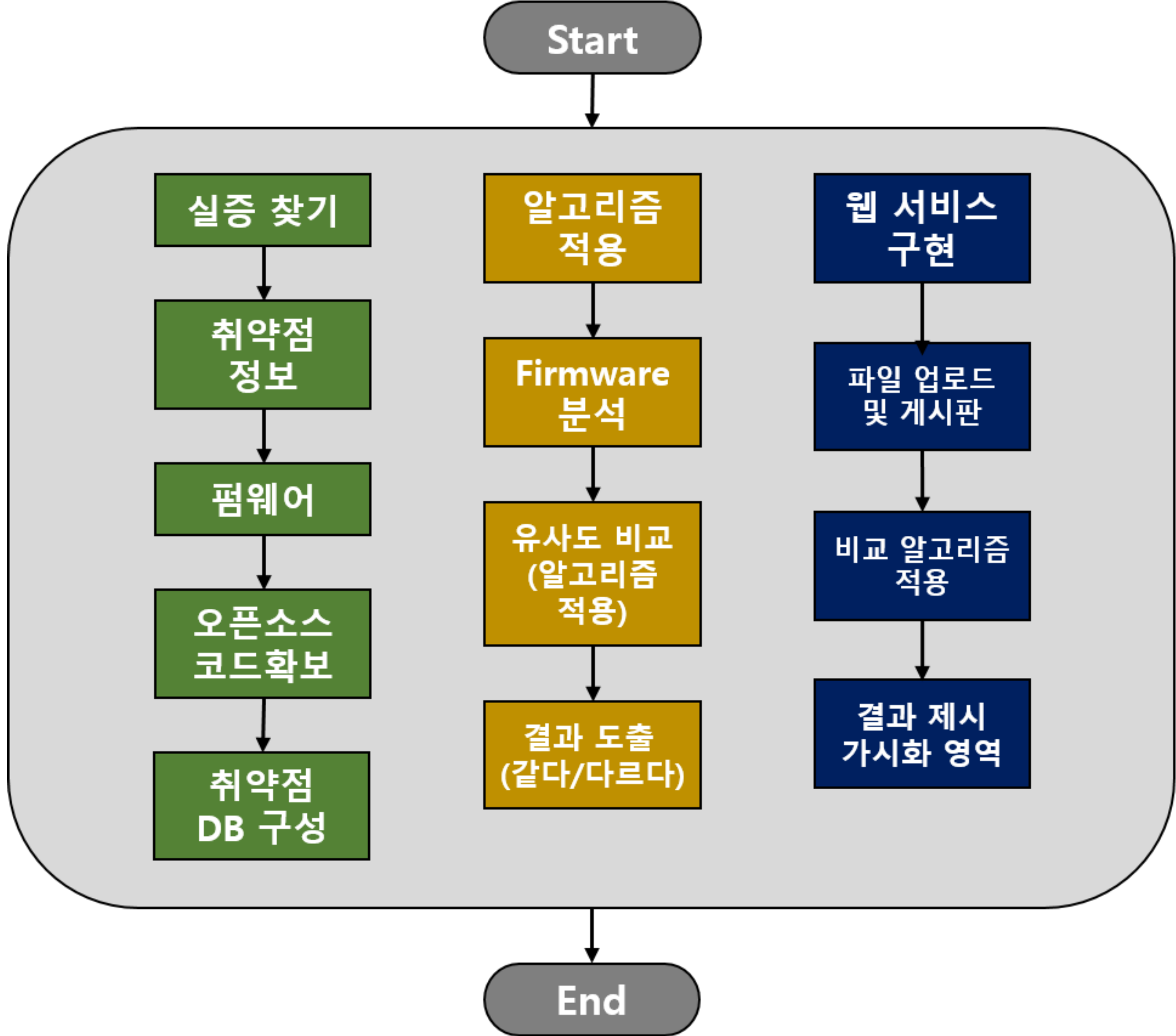




# 프로젝트 개요 및 목표

# 프로젝트 절차 및 개발 내용

Filtering like Binary Search 기법 → **빠르고 상세한** IoT 기기 점검



## [SOSfinder 모듈]

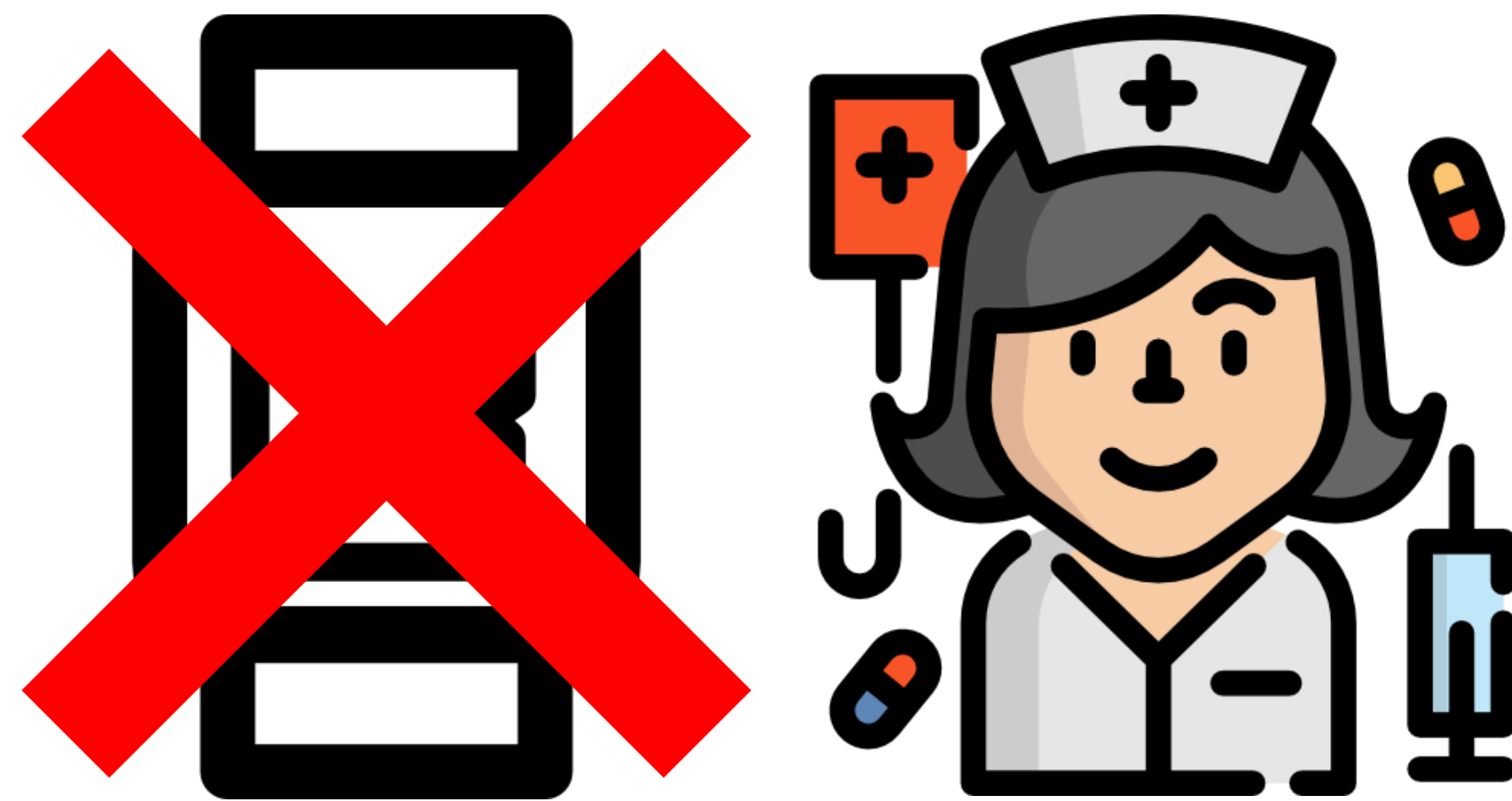
1. Jaccard Index & Jaccard Containment  
**바이너리 코드** 기반으로, 취약 모듈과 대상 파일의 유연성있는 **유사도 비교**를 통한 **취약 정도 진단**

2. 취약점 Database 구성  
각 취약점 코드의 컴파일옵션 및 운영체제 환경에 대비하기 위한 취약점 비교 파일 확보

# 프로젝트 목표



보안 경각심 부여



새로운 형태의 IOT 보안

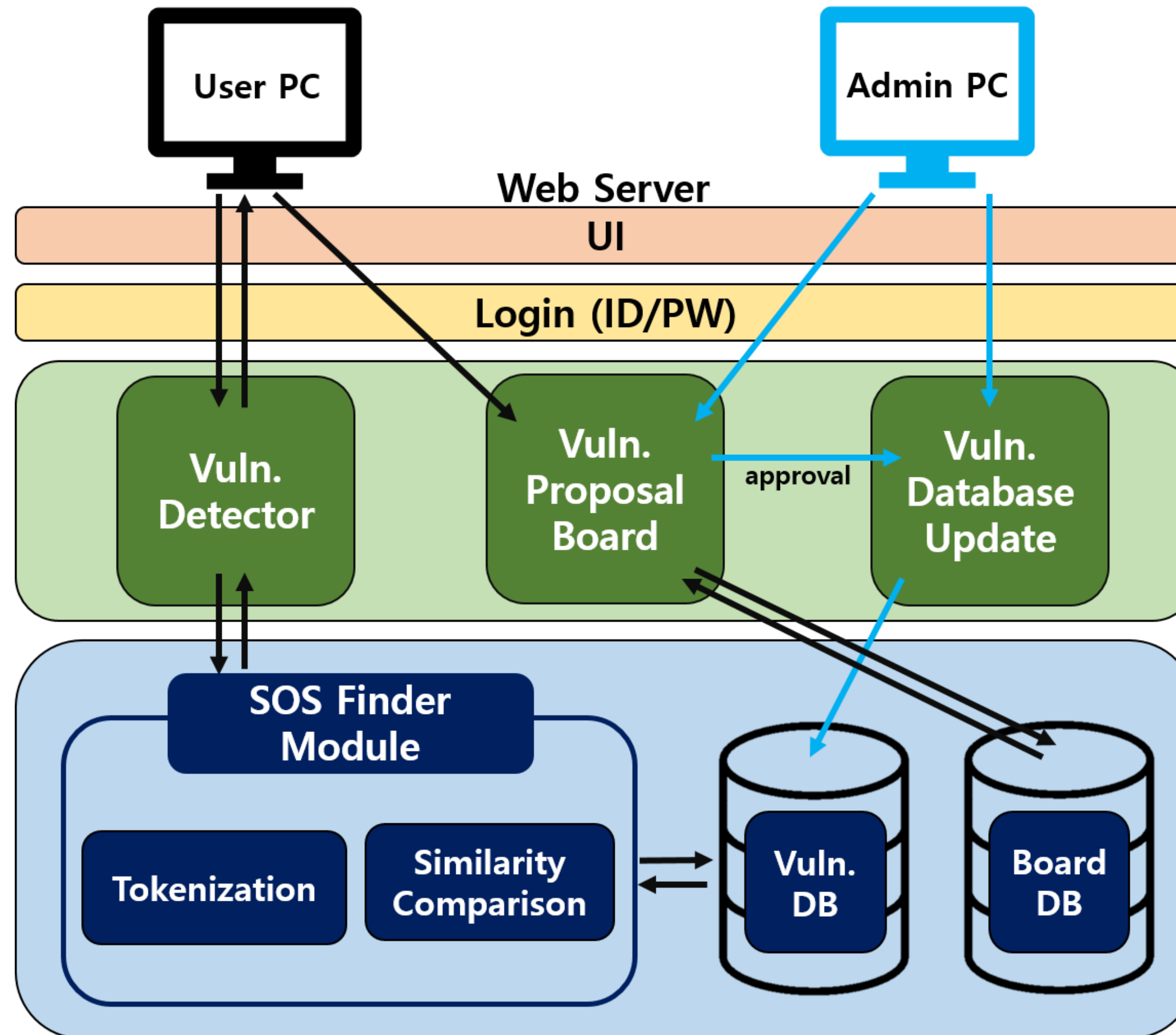


실행파일 검사 서비스



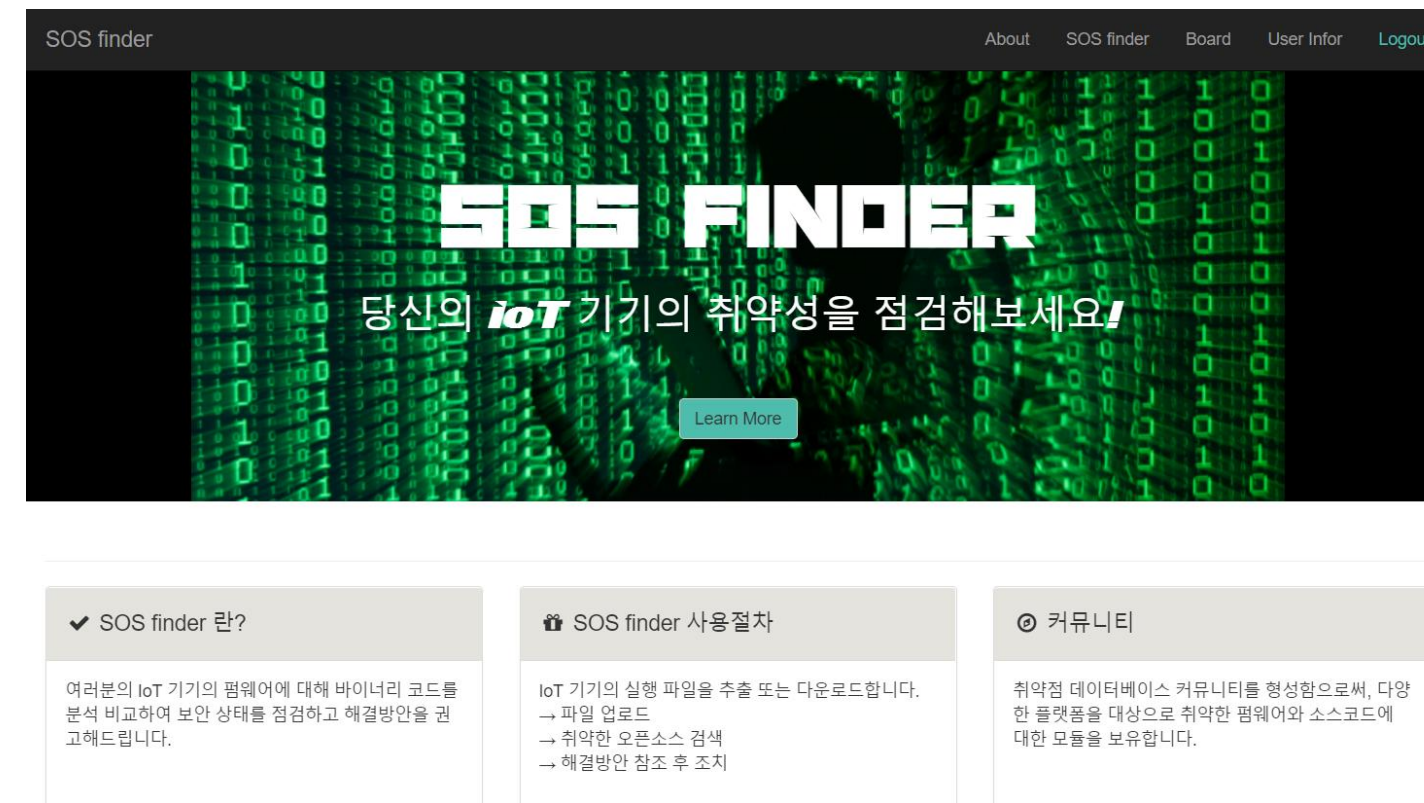
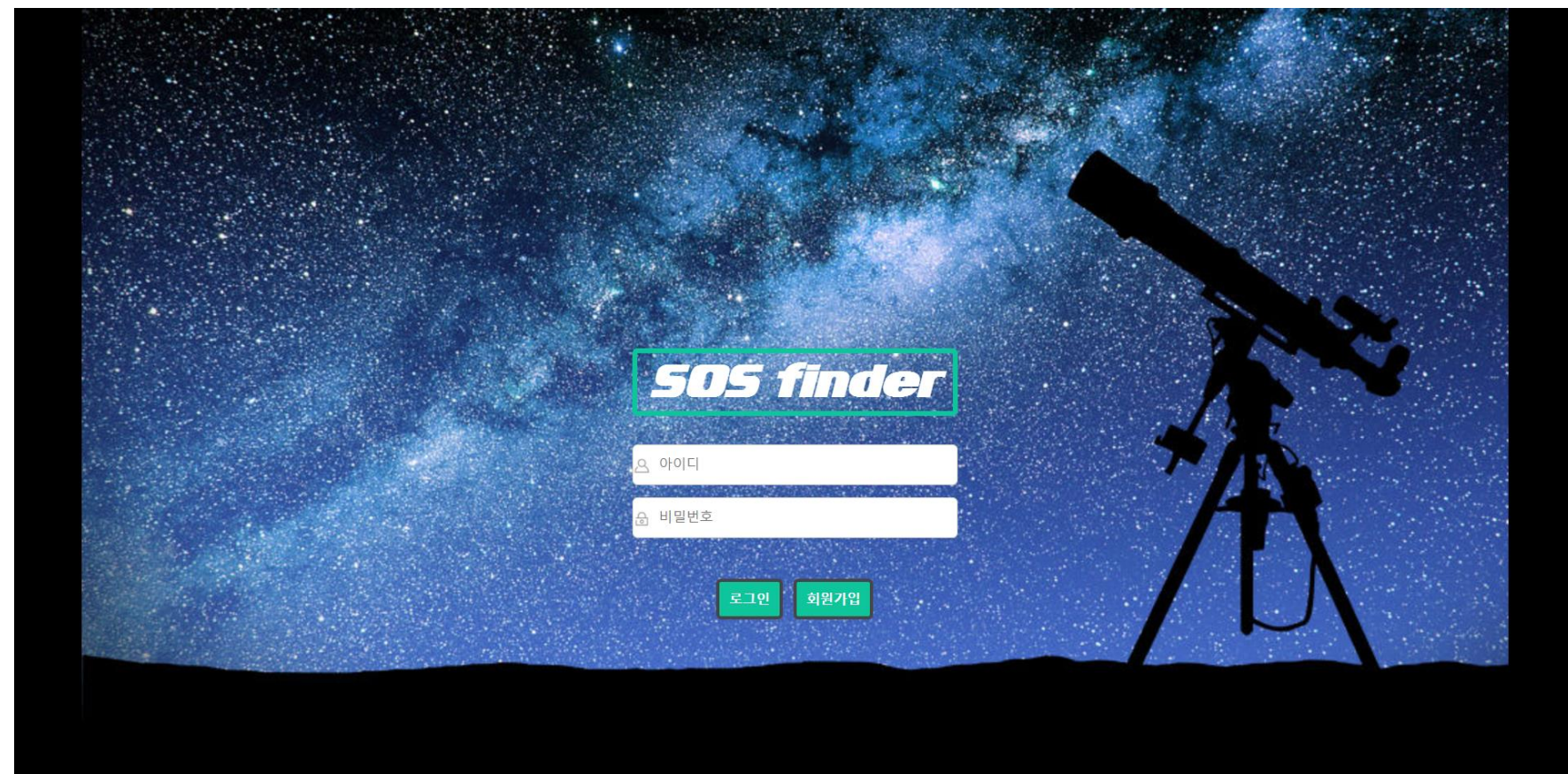
# 서비스 기능 및 구조

# 시스템 구조도



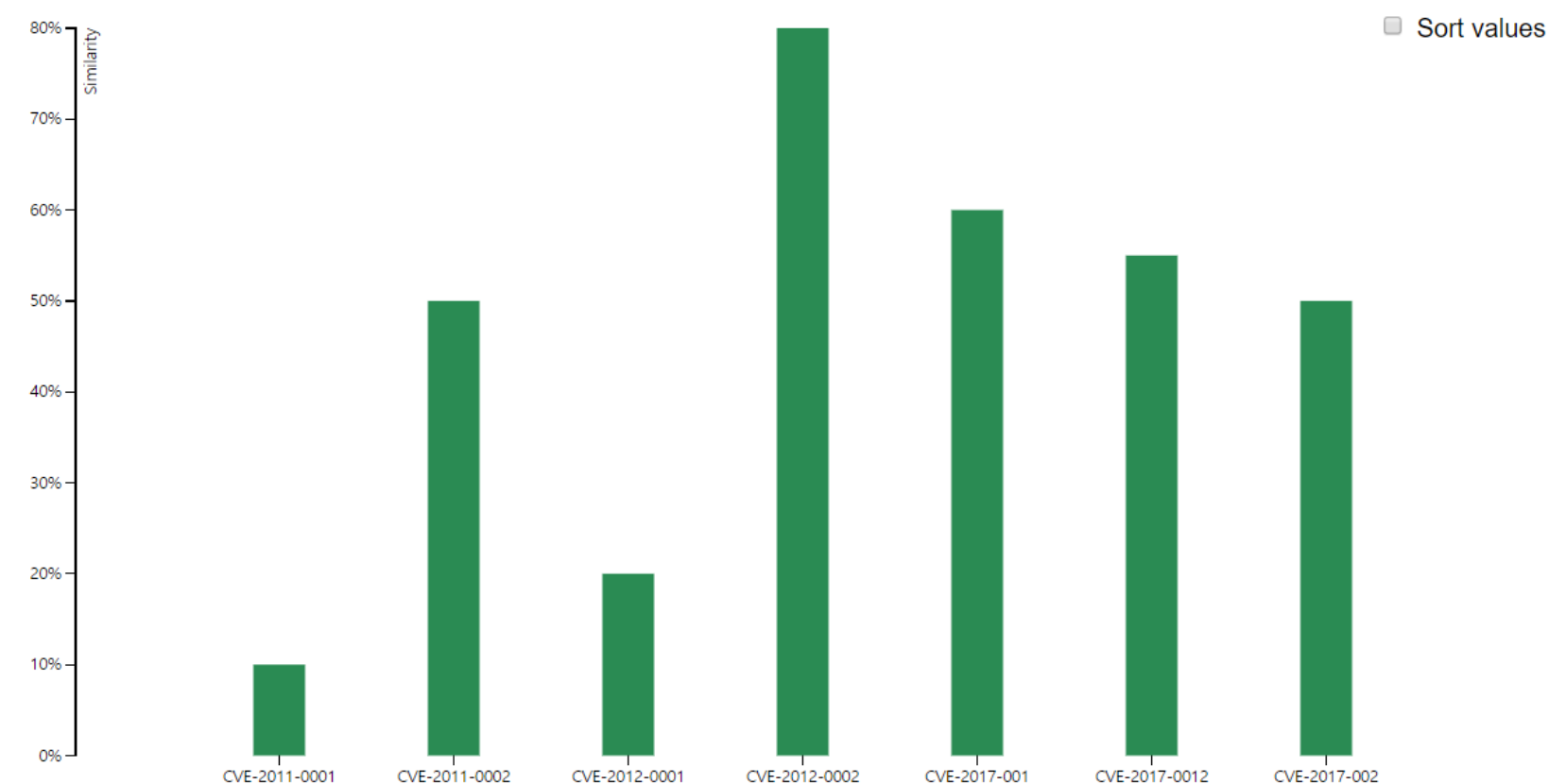
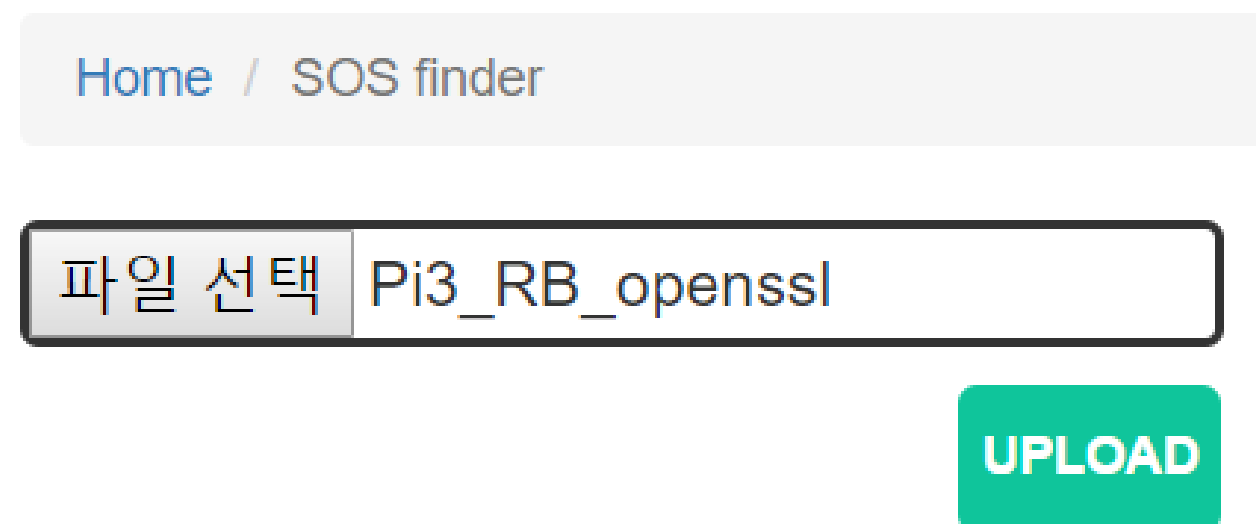


# 취약점 탐지 웹 서비스



펌웨어 (실행파일)로  
점검하는 IoT 기기 보안

## SOS finder



취약점 DB 와  
유사도 비교를 통해  
취약 정도를 그래프로  
가시화

# 취약점 DB 커뮤니티 게시판

## SOS finder Community Board

[Home](#) / Board

번호	글제목	글쓴이	작성일
1	Software	minkyung	2017-05-15

글쓰기

취약점 소프트웨어 건의하기

글제목

글내용

FILE

파일 선택

선택된 파일 없음

글쓰기

## SOS finder Community Board

[Home](#) / Board

글제목

작성자

작성일

글내용

첨부파일

Software

minkyung

2017-05-15

test

목록

글쓰기

댓글쓰기

## User Profile

[Home](#) / Profile

아이디

이름

Good 게시물 갯수

test

test

1

\* Good 게시물이란, 커뮤니티 게시판에 올린 사용자의 글 중 관리자가 선택한 게시물을 의미합니다.

MODIFY PASSWORD

LOGOUT

게시판 운영을 통해  
보안 커뮤니티 형성

점검 모듈  
DB 구성의 확장성

# 활용방안 및 기대 효과



보안에 미숙한 개발자들의 검정




파워 유저가 자신의 IoT 디바이스 검사



취약점 관련 커뮤니티 형성

*SOS finder*





시연 동영상



# ***SOS finder***

아이디

비밀번호

로그인

회원가입





# 역할 분담



Name: 송창현

- 전체 프로젝트 총괄 및 설계
- 유사도 비교 알고리즘 구현



Name: 차진원

- 유사도 비교 알고리즘 설계
- 알고리즘 성능 테스트



Name: 정성민

- 웹 서비스 구현 (software 업로드 및 알고리즘 연동)
- 가시화 구현(Dashboard)



Name: 박민경

- 웹 서비스 구현 (회원 관리 및 게시판 등의 커뮤니티)
- 가시화 구현(Dashboard)



Name: 정현석

- 웹 UI / UX 디자인
- 타겟 기기의 binary code 추출



Name: 핫산

- 취약한 펌웨어 자료 조사

# 감사합니다

Thank you

1조 SOFA  
송창헌 박민경 정성민  
차진원 정현석 핫산