구글 검색 엔진을 이용한 웹 취약점 진단 도구

JMT

팀장 : 1821032 정 석 천 | 팀원 : 1921011 김 은 혜

210 팀

2023년 춘계 졸업작품회

구글 검색 엔진을 이용한 웹 취약점 진단 도구

CONTENTS

JMT

01 JMT

1. 정의 및 목적

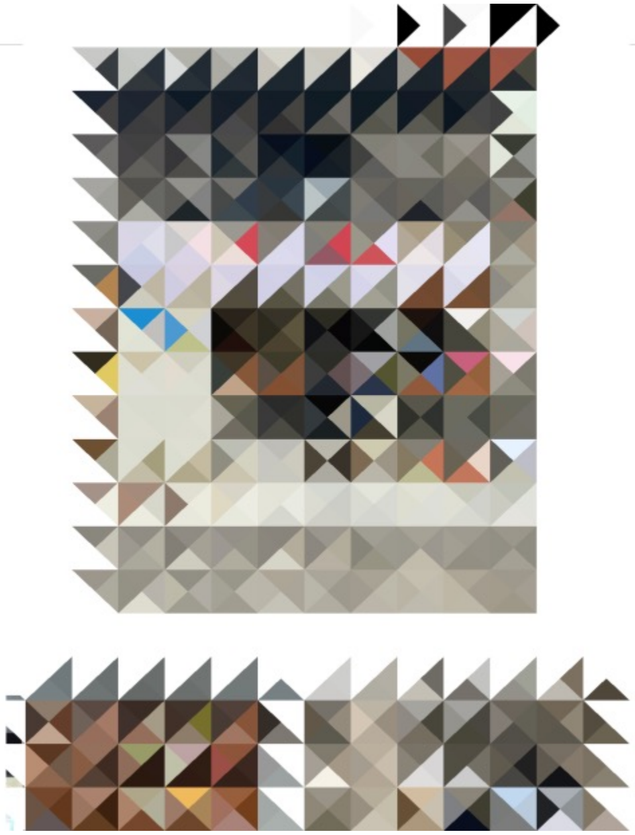
- "JMT"는 웹 사이트의 취약점을 진단하는 도구로, 다른 취약점 진단 도구와 달리 구글 검색 엔진을 사용하여 인터넷 상의 공개된 정보를 진단한다.
  이 도구를 통해 악의적인 사용자들이 웹 사이트를 공격하기 전 검색 등을 이용하여 공개된 정보를 수집하는 활동을 방지하는 것이 목적이다.

2. 개발 동기

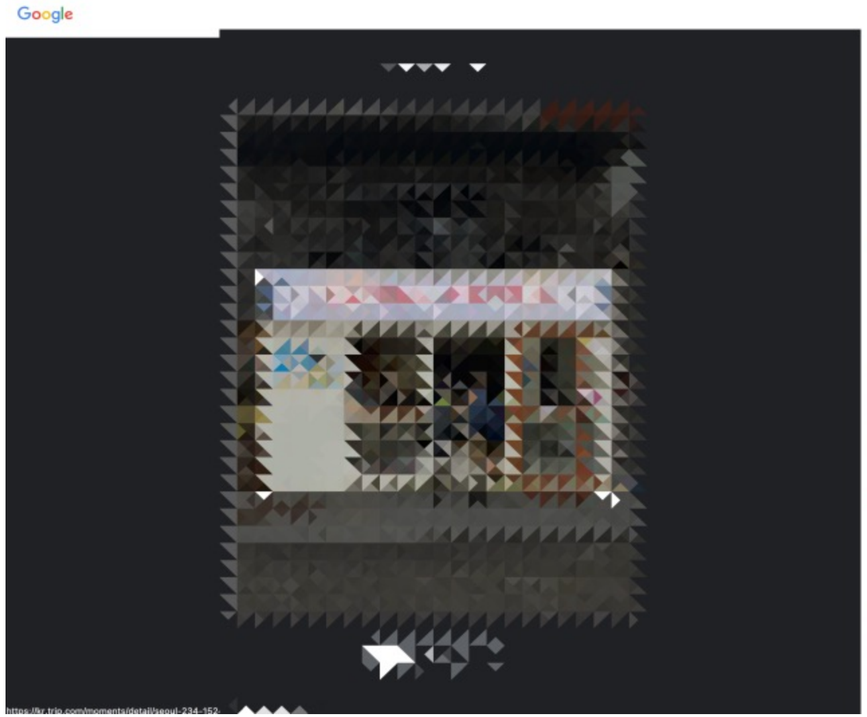

Google
naver.com
이미지
동영상
지도
뉴스
쇼핑
도서
항공편
금융
검색결과 약 2개 (0.16초)
naver.com
https://m.blog.naver.com ›
- 네이버 블로그
2022. 10. 1. — NAVER Corp. ...
blogId":"
'domainIdOrBlogId":"sorldjrqhdkqkdb","logNo":222889394612,"smartEditorVersio
twitter.com
https://mobile.twitter.com ›
/ Twitter
데뷔때부터 팬이었는데 트위터 할 줄 모름,,. 대한민국 Joined October 2016 ...
now.naver.com. NAVER NOW. 네이버 앱에서 듣는 라이브 오디오쇼.

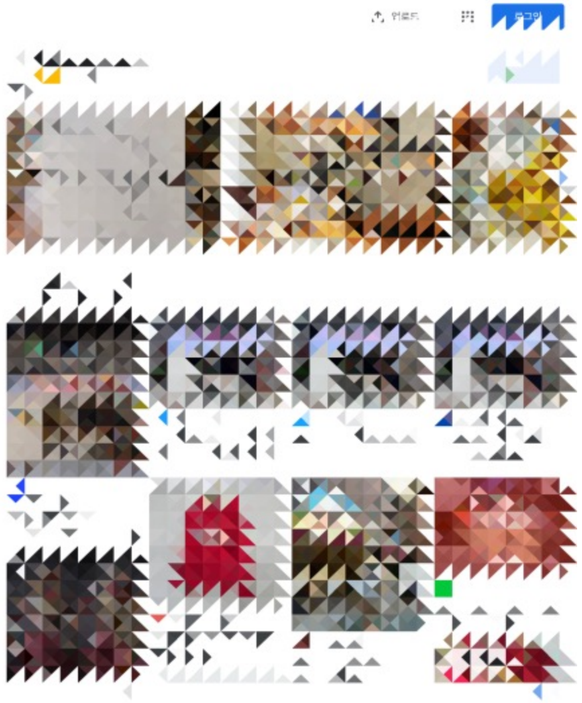
2. 개발 동기

blog



2. 개발 동기





2. 개발 동기

itworld.co.kr
https://www.itworld.co.kr › news

"구글 계정이 침입 통로" 시스코 해킹 사고의 전모 - ITWorld Korea

2022. 8. 17. — 엔비디아와 마이크로소프트, 유비소프트, 삼성, 보다폰에 이어 시스코가 유명 IT 업체의 **해킹 피해 사례**에 이름을 올렸다. 지난 5월 말 한 공격자가 시스코 네트워크에 ...

zdnet.co.kr
https://zdnet.co.kr › view

구글 파이 해킹당했다…"전화번호·SIM 등 개인정보 유출"

2023. 2. 1. — **구글**의 알뜰폰(MVNO) 서비스 '**구글** 파이'의 고객 정보 일부가 유출됐다. 테크크런치는 31일(현지시간) **구글** 파이가 자사 데이터에 해커가 접근했다는 사실을 확인 ...

누락된 검색어: 파해 | 다음 정보가 포함되어야 합니다. **피해**

boannews.com
https://m.boannews.com › html › detail

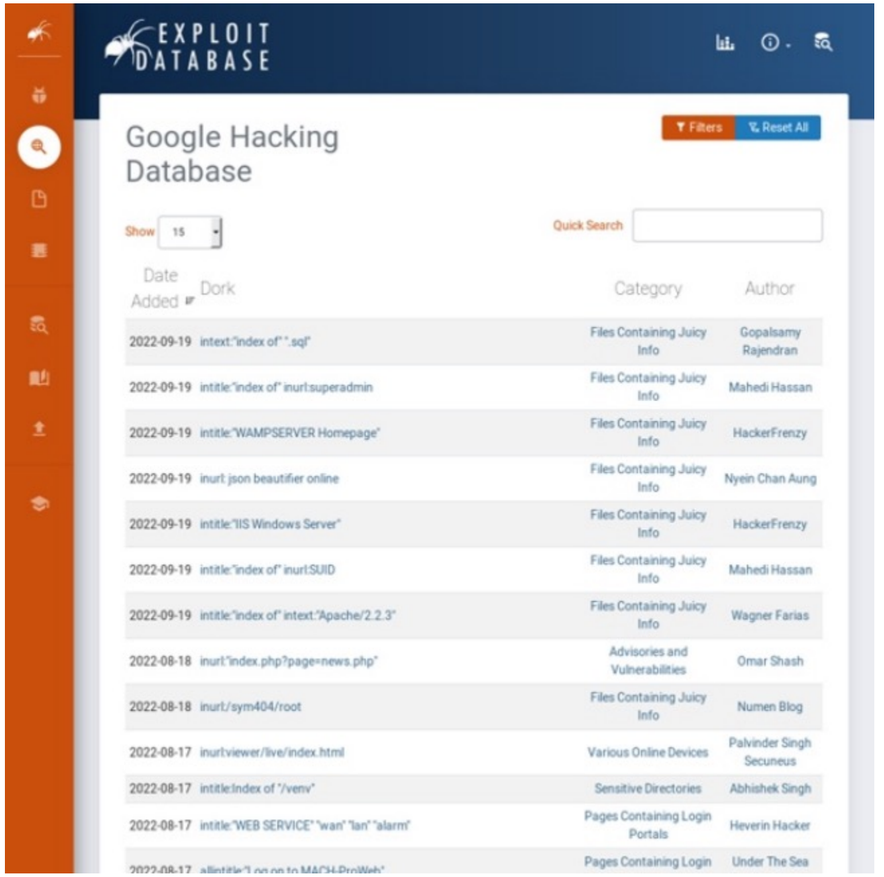
구글 키워드 검색으로 노출되는 피싱 페이지 주의... 구글 애즈 ...

2023. 2. 3. — **구글** 키워드 **검색** 시 노출되는 피싱 페이지를 통한 **해킹 피해**가 지속되고 있는 만큼 **검색**엔진 사용 시 각별한 주의가 요구된다. △광고 **검색** 결과[자료=이스트시큐리티 ...

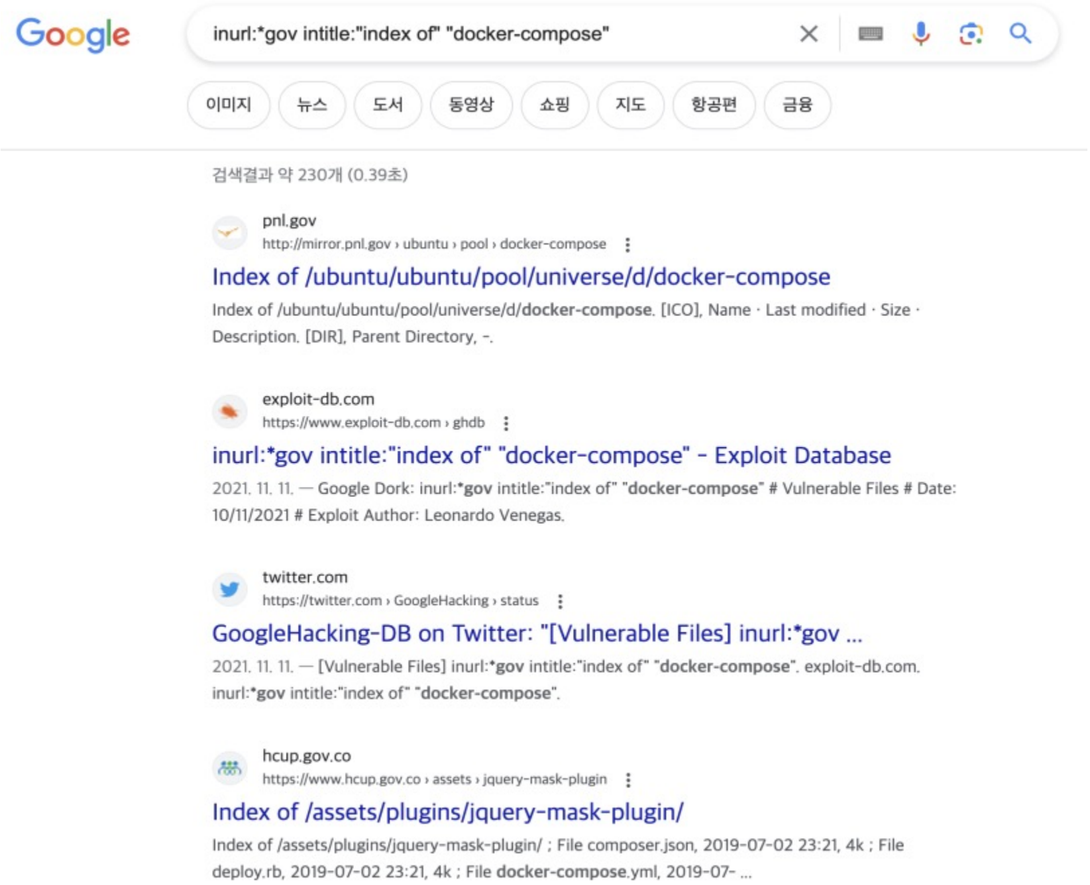
yna.co.kr
https://www.yna.co.kr › 경제 › 전체뉴스

정부 유튜브 해킹에 보안업계 "구글 취약점 아닌 계정관리 문제"

2022. 9. 5. — 이들 **해킹** 사건의 정확한 경위는 아직 밝혀지지 않고 있다. 그는 이번 **해킹**이 **구글** 자체를 상대로 벌어진 공격일 가능성은 극히 낮다고 봤다. 해외에서는 비슷한 **해킹 사례** ...



2. 개발 동기


Google
inurl:*gov intitle:"index of" "docker-compose"
이미지
뉴스
도서
동영상
쇼핑
지도
항공편
금융
검색결과 약 230개 (0.39초)
pnl.gov
http://mirror.pnl.gov › ubuntu › pool › docker-compose
Index of /ubuntu/ubuntu/pool/universe/d/docker-compose
Index of /ubuntu/ubuntu/pool/universe/d/docker-compose. [ICO], Name · Last modified · Size · Description. [DIR], Parent Directory, -.
exploit-db.com
https://www.exploit-db.com › ghdb
inurl:*gov intitle:"index of" "docker-compose" - Exploit Database
2021. 11. 11. — Google Dork: inurl:*gov intitle:"index of" "docker-compose" # Vulnerable Files # Date: 10/11/2021 # Exploit Author: Leonardo Venegas.
twitter.com
https://twitter.com › GoogleHacking › status
GoogleHacking-DB on Twitter: "[Vulnerable Files] inurl:*gov ...
2021. 11. 11. — [Vulnerable Files] inurl:*gov intitle:"index of" "docker-compose". exploit-db.com. inurl:*gov intitle:"index of" "docker-compose".
hcup.gov.co
https://www.hcup.gov.co › assets › jquery-mask-plugin
Index of /assets/plugins/jquery-mask-plugin/
Index of /assets/plugins/jquery-mask-plugin/ ; File composer.json, 2019-07-02 23:21, 4k ; File deploy.rb, 2019-07-02 23:21, 4k ; File docker-compose.yml, 2019-07- ...

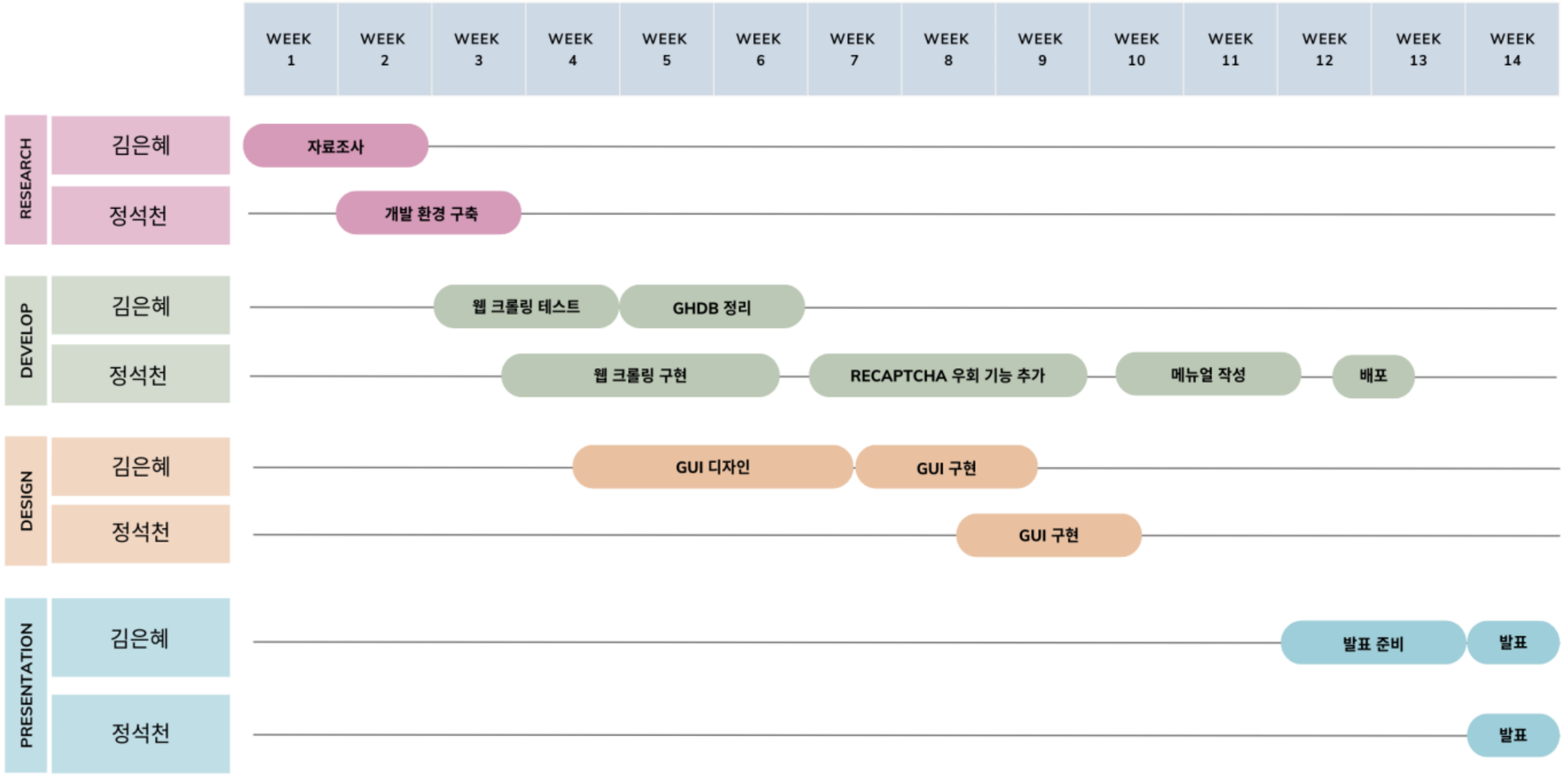
01 JMT

설계 목표	• 구글 검색 엔진을 이용한 웹 취약점 진단 도구 개발 및 배포
대상	• 보안 담당자 • 웹 개발자
설계 요구사항	• 구문 자동 수집 시 reCAPTCHA 우회를 할 수 있어야 함 • 사용자가 보기 쉽도록 Report 파일 결과를 Markdown 형식 저장해야 함 • 깔끔하고 편리한 GUI 화 및 실행파일화 되어야 함

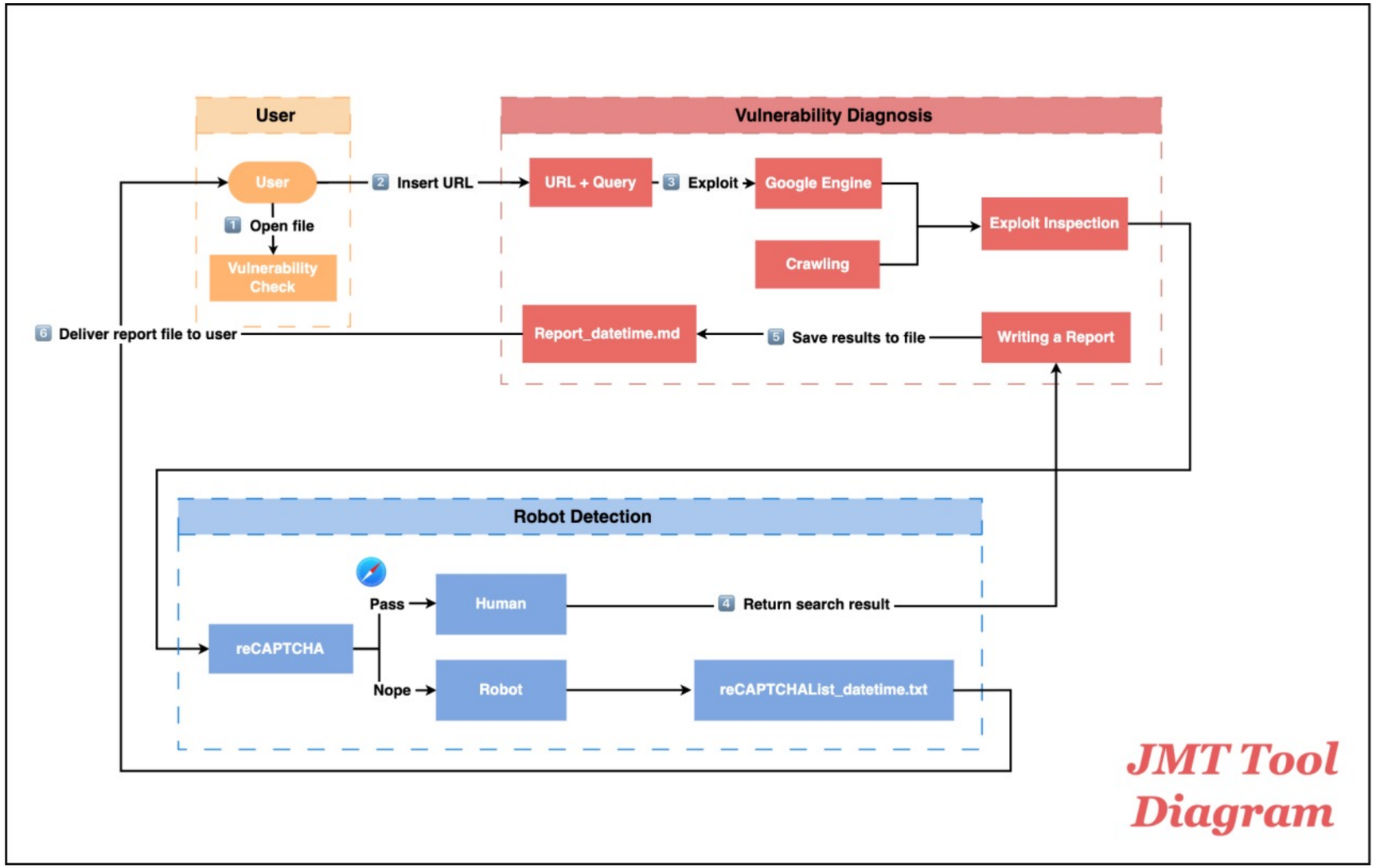
개발 과정

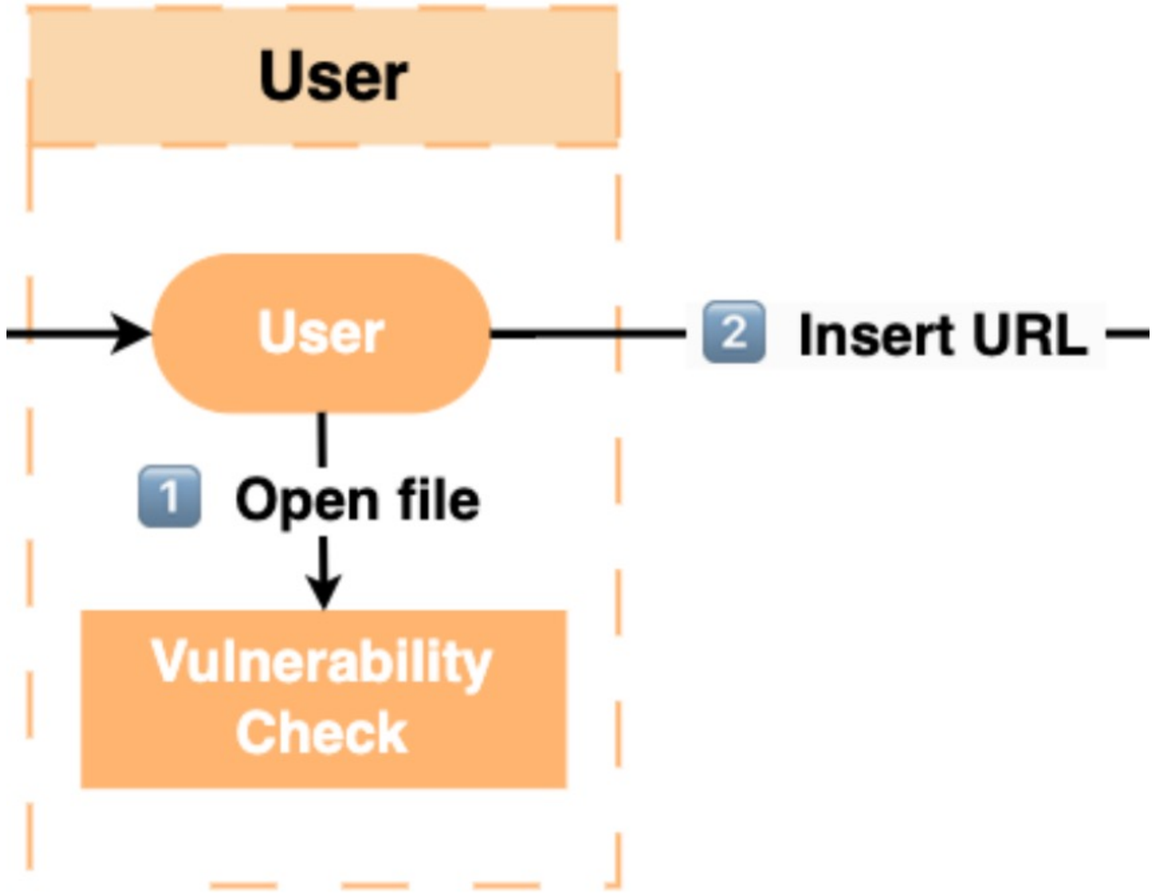
02

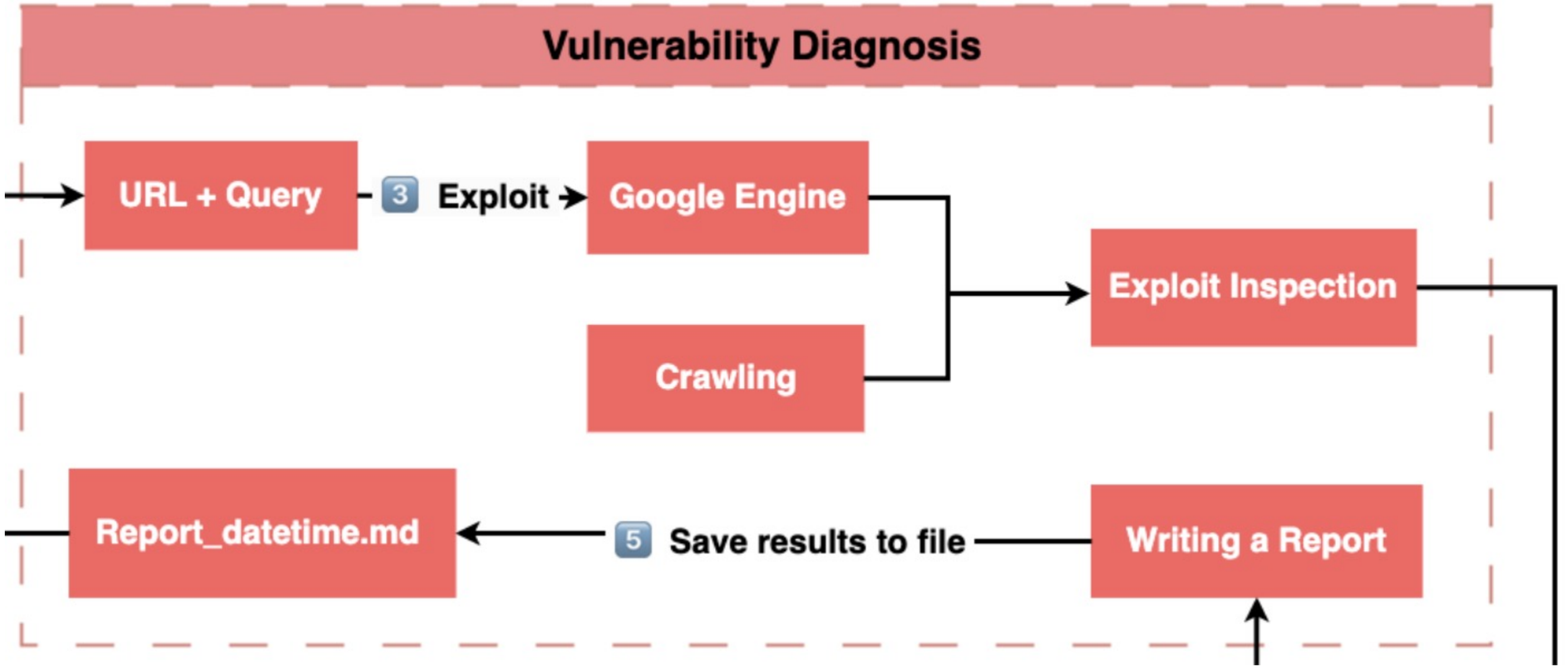
개발 과정

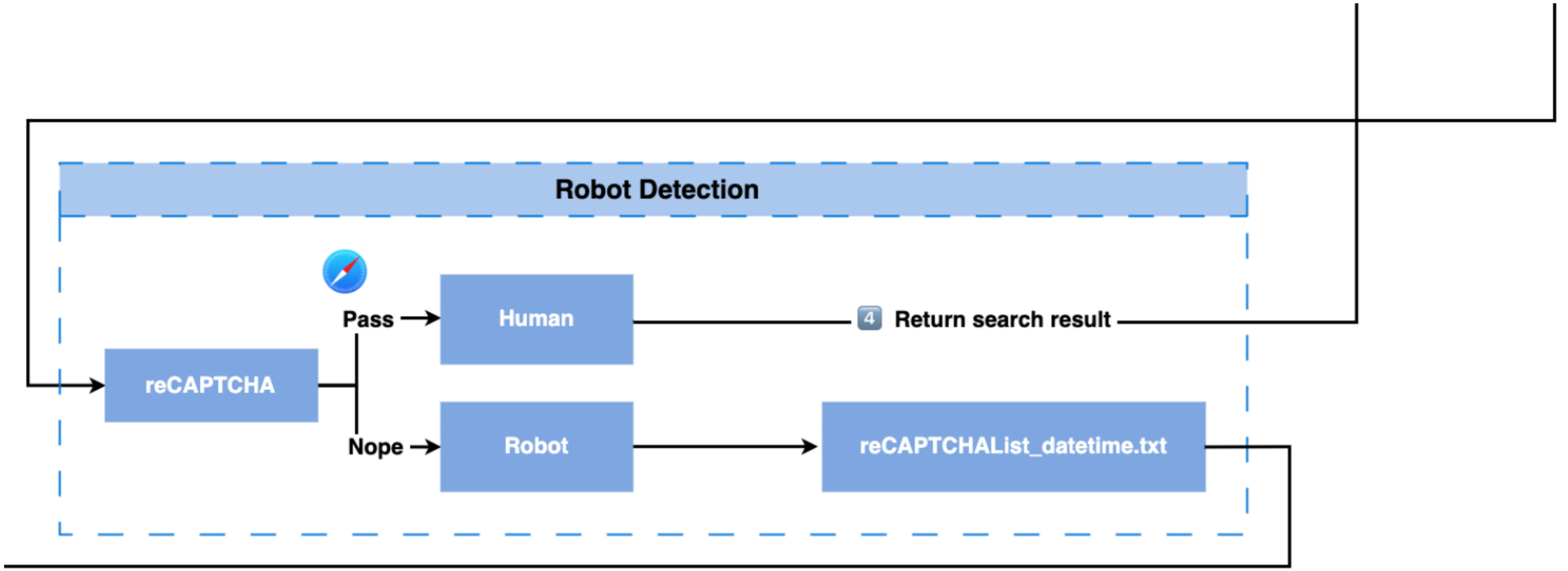

WEEK 1
WEEK 2
WEEK 3
WEEK 4
WEEK 5
WEEK 6
WEEK 7
WEEK 8
WEEK 9
WEEK 10
WEEK 11
WEEK 12
WEEK 13
WEEK 14
RESEARCH
김은혜
자료조사
정석천
개발 환경 구축
DEVELOP
김은혜
웹 크롤링 테스트
GHDB 정리
정석천
웹 크롤링 구현
RECAPTCHA 우회 기능 추가
메뉴얼 작성
배포
DESIGN
김은혜
GUI 디자인
GUI 구현
정석천
GUI 구현
PRESENTATION
김은혜
발표 준비
발표
정석천
발표

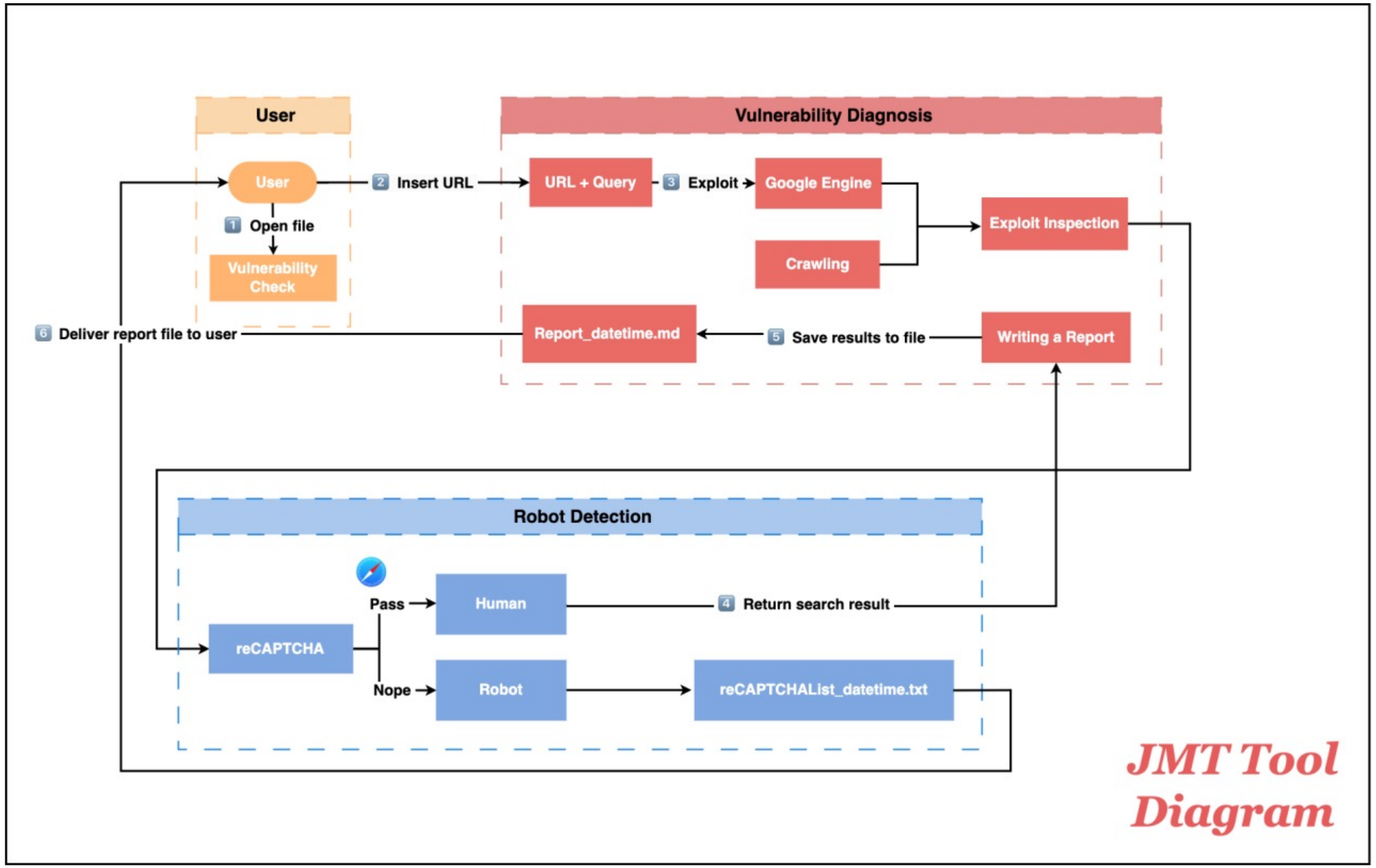
기능 및 시연


User
Vulnerability Diagnosis
User
1 Open file
Vulnerability Check
2 Insert URL
URL + Query
3 Exploit
Google Engine
Crawling
Exploit Inspection
6 Deliver report file to user
Report_datetime.md
5 Save results to file
Writing a Report
Robot Detection
Pass
Human
4 Return search result
reCAPTCHA
Nope
Robot
reCAPTCHAList_datetime.txt
JMT Tool Diagram


User
User
2 Insert URL
1 Open file
Vulnerability Check


Vulnerability Diagnosis
URL + Query
3
Exploit
Google Engine
Crawling
Exploit Inspection
Report_datetime.md
5
Save results to file
Writing a Report


Robot Detection
Pass
Human
4 Return search result
reCAPTCHA
Nope
Robot
reCAPTCHAList_datetime.txt


User
Vulnerability Diagnosis
User
1 Open file
Vulnerability Check
2 Insert URL
URL + Query
3 Exploit
Google Engine
Crawling
Exploit Inspection
6 Deliver report file to user
Report_datetime.md
5 Save results to file
Writing a Report
Robot Detection
Pass
Human
4 Return search result
reCAPTCHA
Nope
Robot
reCAPTCHAList_datetime.txt
JMT Tool Diagram

03 기능 및 시연

- GitHub URL : https://github.com/accio3014/JMT

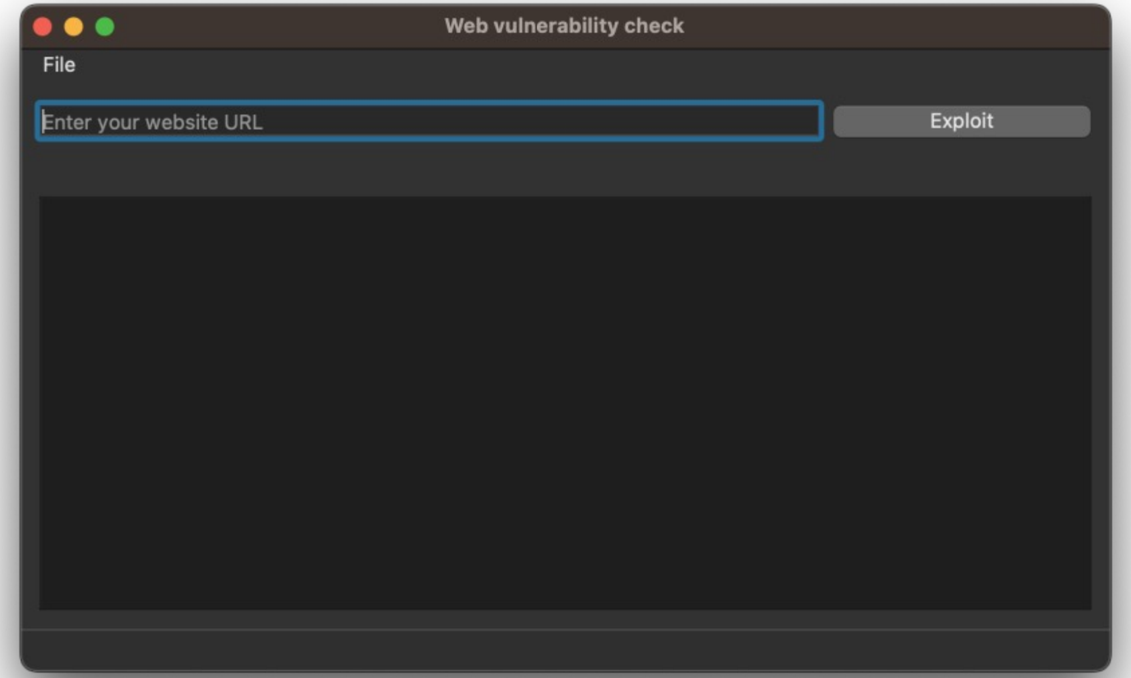
Safari 자동화 허용:

```
Safari → Develop → Allow Remote Automation
```

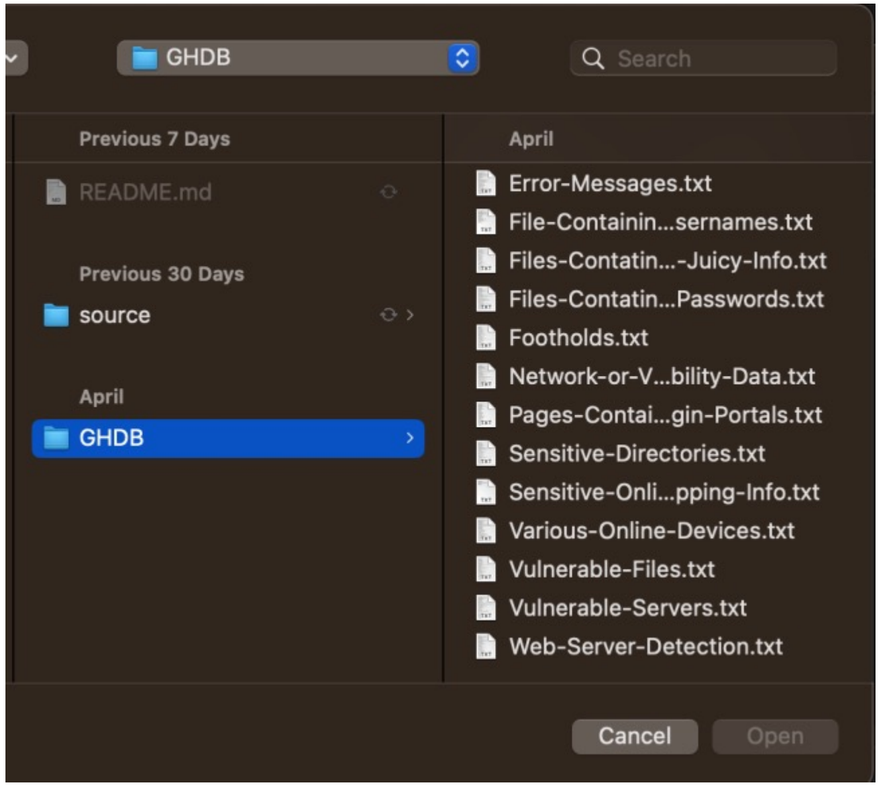
Python 모듈 설치 목록:

```
$ pip3.x install PyQt5
$ pip3.x install bs4
$ pip3.x install selenium
```

1. URL 입력

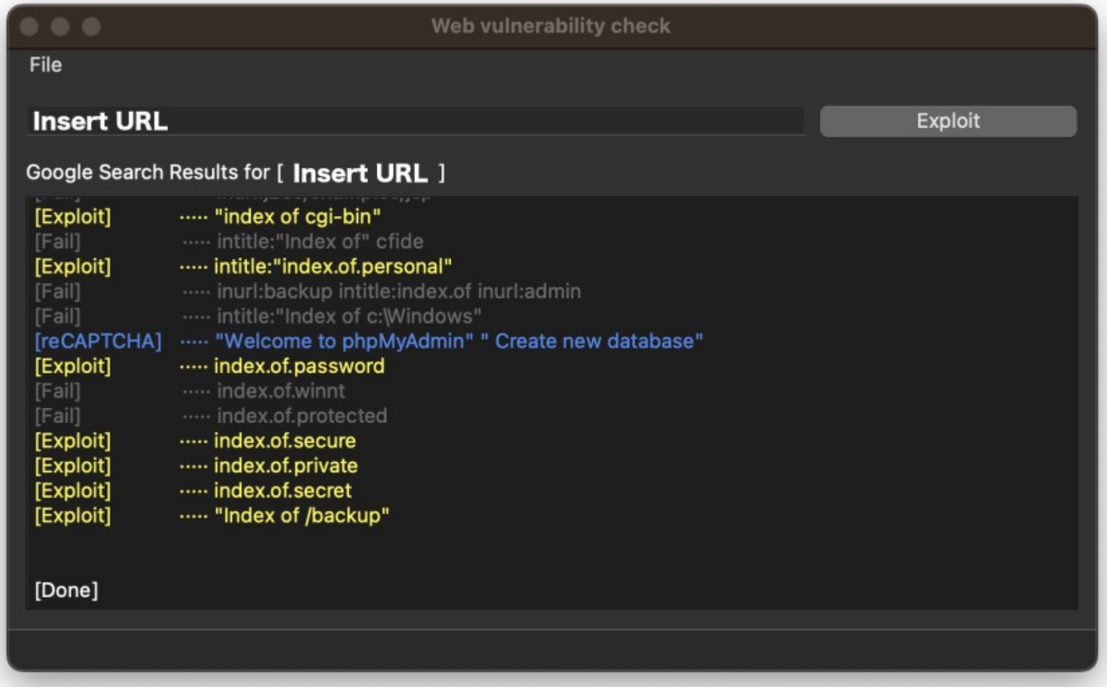

Web vulnerability check
File
Enter your website URL
Exploit

2. GHDB에서 카테고리 선택



3. 진단 결과 대기 중

[Exploit] : 검색 결과가 있습니다.
[Fail] : 검색 결과가 없습니다.
[reCAPTCHA] : Google reCAPTCHA 감지되었습니다.



reCAPTCHA를 우회하는 방법

대부분의 reCAPTCHA는 Safari 웹 브라우저를 사용하기 때문에 우회되지만 아래 방법을 추가로 사용하면 보다 효과적으로 우회할 수 있습니다.

```
1. Use a VPN
reCAPTCHA can be bypassed by using a VPN to change your country or region.

2. Restart your MAC
reCAPTCHA can be bypassed by restarting the Mac.
```

위의 두 가지 방법 중 어떤 방법을 사용하든 상관없지만 Mac을 다시 시작하는 것이 좋습니다.

향후 과제

04 향후 과제

- 현재 reCAPTCHA 우회를 적용 중이지만, 추후 패치를 예상하여 향상된 우회 방법 업데이트 예정
- Safari를 제외한 다른 웹 브라우저 호환성 업데이트 예정

REFERENCE

05 REFERENCE

- Reference URL : https://github.com/accio3014/JMT#reference

Q & A

감사합니다.

팀장 : 1821032 정 석 천 | 팀원 : 1921011 김 은 혜