공개출처정보(OSINT) 솔루션 개발

[최종 발표]

팀장 | 우제혁
팀원 | 신재형,이예준,송태현,이정호

목차

Ⅰ 프로젝트 소개

1. 팀 소개 및 프로젝트 관리
2. 프로젝트 주제 및 목표
3. 프로젝트 준비

Ⅱ 프로젝트 진행

1. OSINT 모듈 소개
2. 데이터 관리
3. OSINT 활용

Ⅲ 프로젝트 결과

1. 산출물 및 결과
2. 향후 계획

프로젝트 소개

Ⅰ 프로젝트 소개

1. 팀 소개 및 프로젝트 관리
2. 프로젝트 주제 및 목표
3. 프로젝트 준비

1. 팀 소개 및 프로젝트 관리

5명으로 구성

- 모의 기업서버 구축
- 도메인 모듈 담당
- CVE 1Day 담당
- 도메인 모듈 프론트
- 논문 작성(방법론)

이예준

- 검색 엔진 담당
- GPT 모듈 담당
- 검색 엔진 프론트
- 논문 작성(동향)

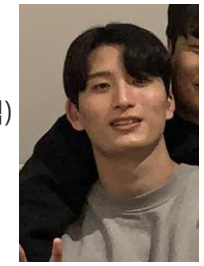
송태현

- Flask 프론트 담당
- SNS 모듈 담당
- 프로젝트 총괄
- SNS 모듈 프론트
- 논문 작성(제안 osint)

우제혁

- 네트워크 담당
- WHO IS 담당
- 네트워크 프론트
- 논문 작성(보안 위협)

신재형



- AWS 세팅
- Flask 기본 구성
- CVE 모듈 담당
- CVE 모듈 프론트
- 논문 작성(서론,결론)

이정호

노션으로 프로젝트 관리

Add cover Add comment

캡스톤 디자인 - OSINT (공개정보 출처)

WW(What-Work)

회의록 / 교수님과의 소통

교수님에게 질문 & 프로젝트 고민

공부내용

자료 조사

보고서 및 발표자료

7주차	각 URL 메인 화면 캡처 및 로깅 (v2.1)	이 이예준	2023년 4월 16일	SPA 웹 페이지 크롤링
	cve 2021-41773 1-day 구현	이 이예준	2023년 4월 19일	APM 서버 올리기 + 원데이
	중간발표 ppt 만들기(서버구축,도메인)	이 이예준	2023년 4월 21일	중간 점검 발표
	검색엔진 class화 v2	송 송태현	2023년 4월 22일	
	네트워크 class 수정 및 네트워크 + CVE 모듈 Class 화	신 신재형	2023년 4월 23일	네트워크 + CVE 클래스화
8주차	flask spa merge	우 우제혁_6804	2023년 4월 30일	flask 모듈 merge
	flask sns id pw 세팅 수정	우 우제혁_6804	2023년 5월 2일	flask 모듈 merge
	flask domain module	이 이예준	2023년 5월 2일	domain 모듈 플라스크 머지
9주차	검색엔진 프론트 엔드	송 송태현	2023년 5월 6일	검색엔진 프론트 엔드
	flask network	신 신재형	2023년 5월 7일	네트워크 플라스크
	논문 초안 작성	우 우제혁_6804	2023년 5월 7일	논문
10주차	논문 서론, joongsint 소개 작성	우 우제혁_6804	2023년 5월 12일	[제혁] 서론 / 우리의 osint
	논문 초기 틀 제작	우 우제혁_6804	2023년 5월 12일	논문 파일

2. 프로젝트 주제 및 목표

OSINT?

- 공개 출처 정보를 의미하는 'OSINT(Open Source Intelligence)'
- 사이버 보안, 범죄 조사, 전쟁 등 다양한 분야에도 사용되고 있음

OSINT를 활용하여 사이버 인텔리전스 수집을 수행할 수 있으며,
사이버 위협에 대한 보안을 강화할 수 있음

"OSINT를 활용한 기업 데이터 수집과 취약점을 제공하는 차별화 된 OSINT 솔루션 개발"

2. 프로젝트 주제 및 목표

현재 다양한 플랫폼에서는 OSINT를 활용하여 **사이버 위협에 효과적으로 대응**하고 있다.

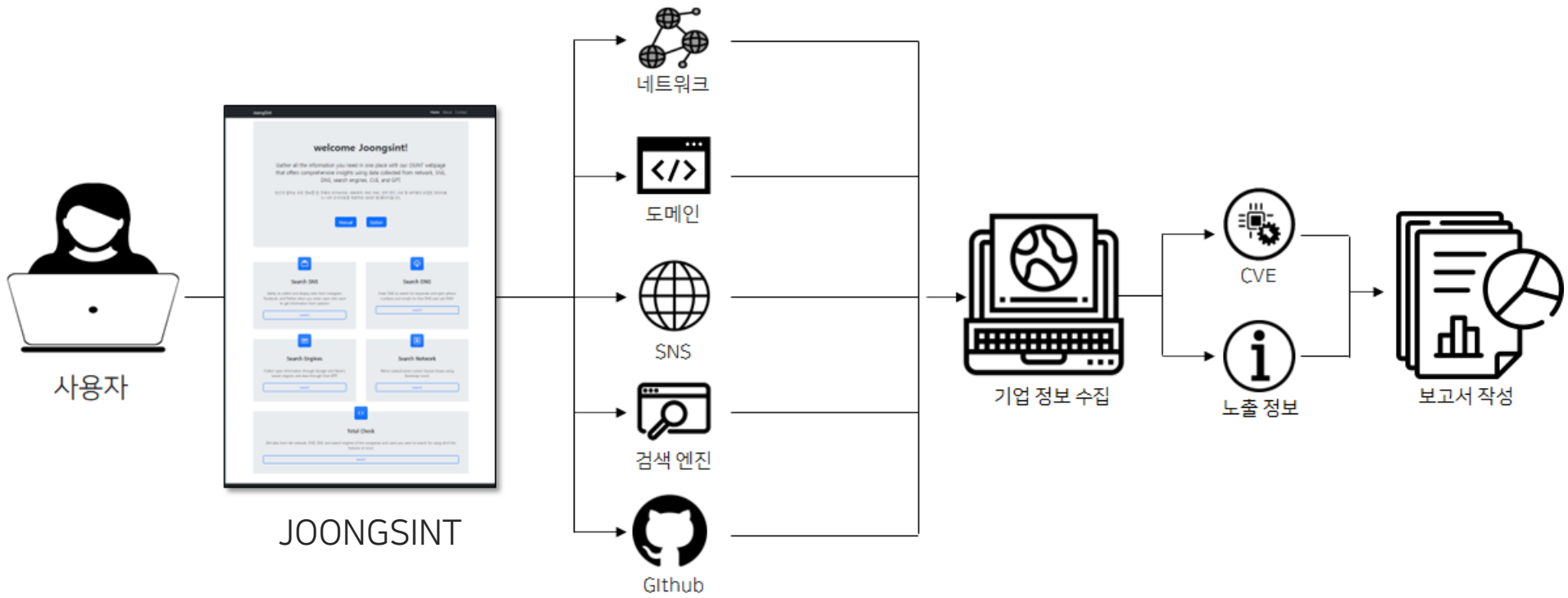
인터넷진흥원(KISA) 및 군사 안보 분야등 다수의 분야에서 OSINT를 활용하는 사실을 확인할 수 있었으며

OSINT로 정보 유출 정황을 수집한다면, **기업의 정보 유출로 인한 피해 최소화**에도 큰 도움이 될 수 있다.

2. 프로젝트 주제

JOONGSINT (OSINT 솔루션)?

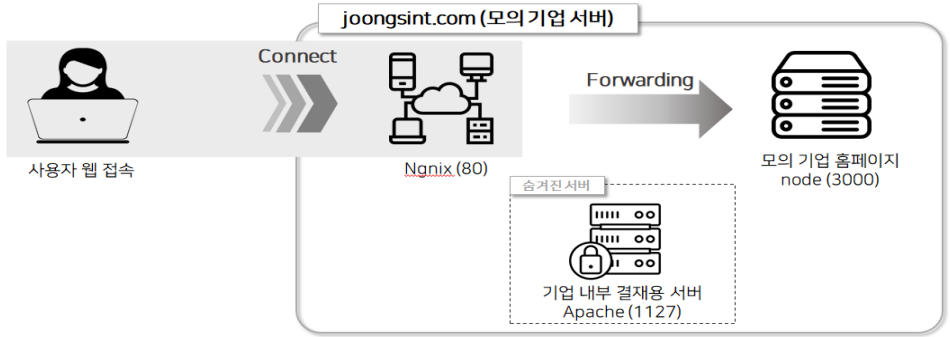
- 다양한 모듈을 통해 기업의 정보를 수집
- 수집된 정보를 분석 및 가공하여 외부로 노출된 기업의 내부 정보를 파악
- 기업 서버에 관련된 CVE 출력
- 기업의 보안 사고 예방



3. 프로젝트 준비

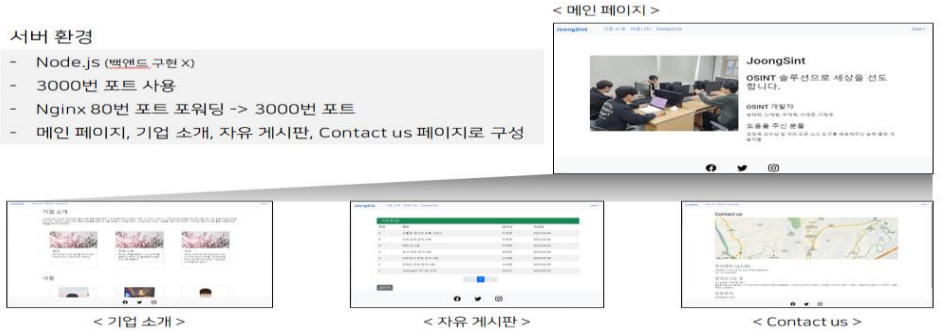
▶ 모의 기업 환경 구축

네트워크 구성도



모의 기업 홈페이지

서버 환경
- Node.js (백엔드 구현 X)
- 3000번 포트 사용
- Nginx 80번 포트 포워딩 -> 3000번 포트
- 메인 페이지, 기업 소개, 자유 게시판, Contact us 페이지로 구성



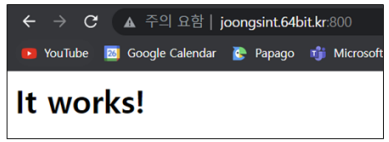
기업 내부 결재용 서버(숨겨진 서버)

서버 환경
- Apache2 2.24.49
- 1127번 포트 사용
- PHP 7.4 (연동 오류로 인해 사용 X)
- Mysql (PHP 연동 오류로 인해 사용 X)

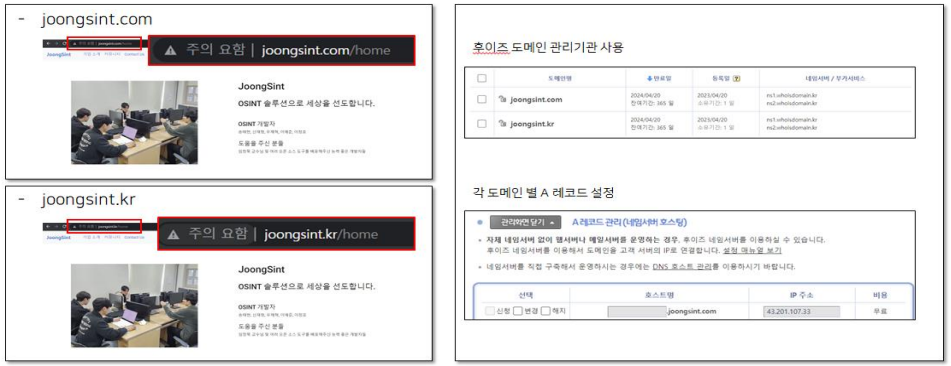
1 이전 버전 다운로드 후 수동 설치

```
./configure --prefix=/usr/local/apache2.4 \
--enable-module=so --enable-rewrite --enable-so \
--with-apr-util=/usr/local/apr-util \
--with-pcre=/usr/local/pcre \
--enable-mods-shared=all
```

2 구축 완료



도메인 등록



진행 상황

Ⅱ 프로젝트 진행

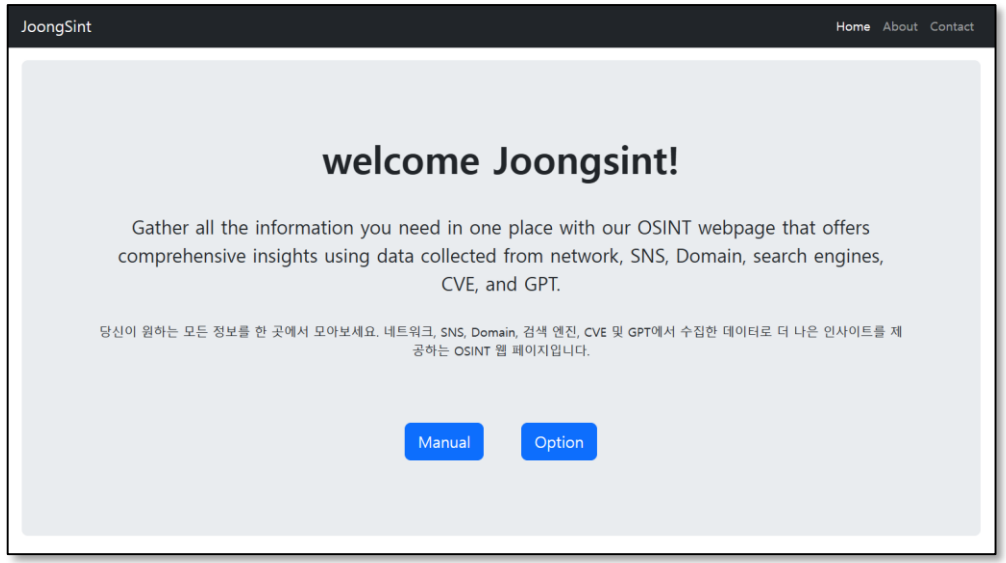
1. OSINT 모듈 소개
2. 데이터 관리
3. OSINT 활용

1. OSINT 모듈 소개 – 웹 서비스 개발

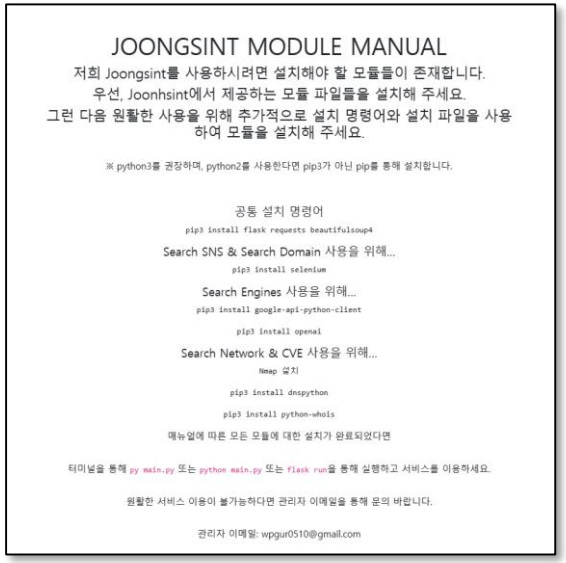
▶ 서비스 개발(Flask)

- Option 토글을 활용해 원하는 데이터를 입력한 뒤 쿠키 값에 저장하여 데이터 활용
- Manual 토글을 활용하여 기본 사용법 안내(api key값 및 설정 파일 안내)

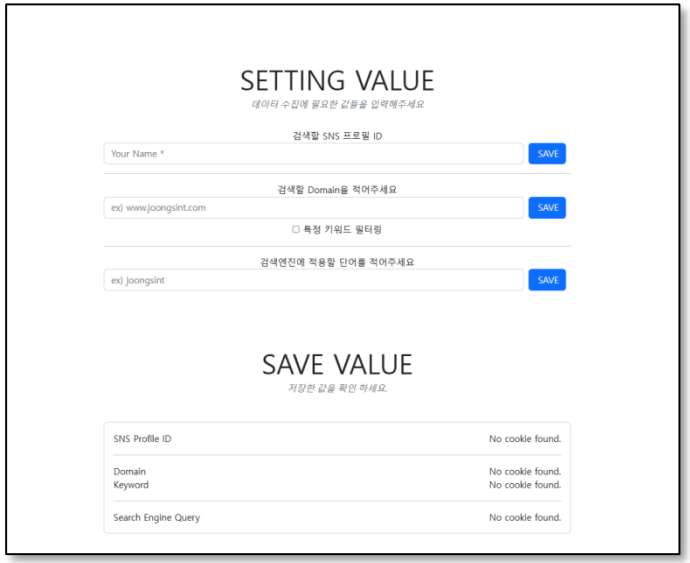
JoongSInt 서비스



Manual 토글

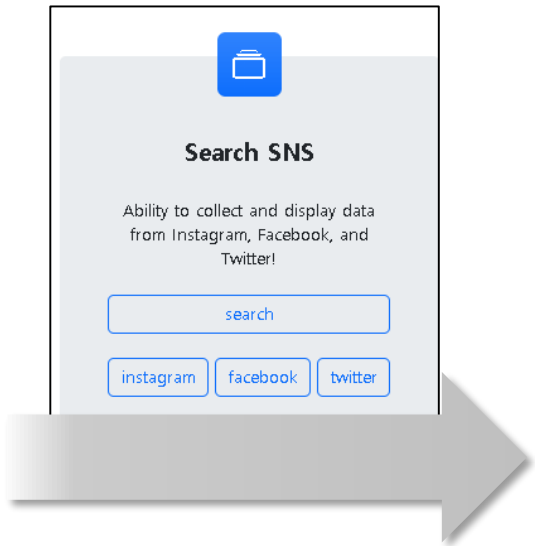


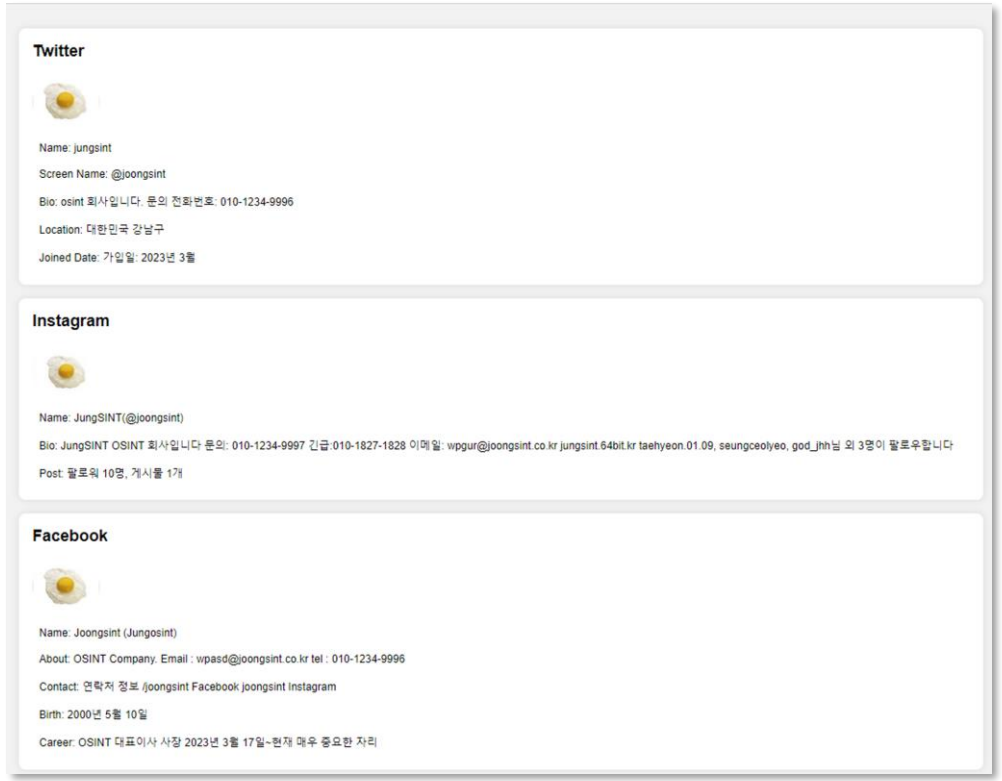
Option 토글



1. OSINT 모듈 소개 – SNS 모듈

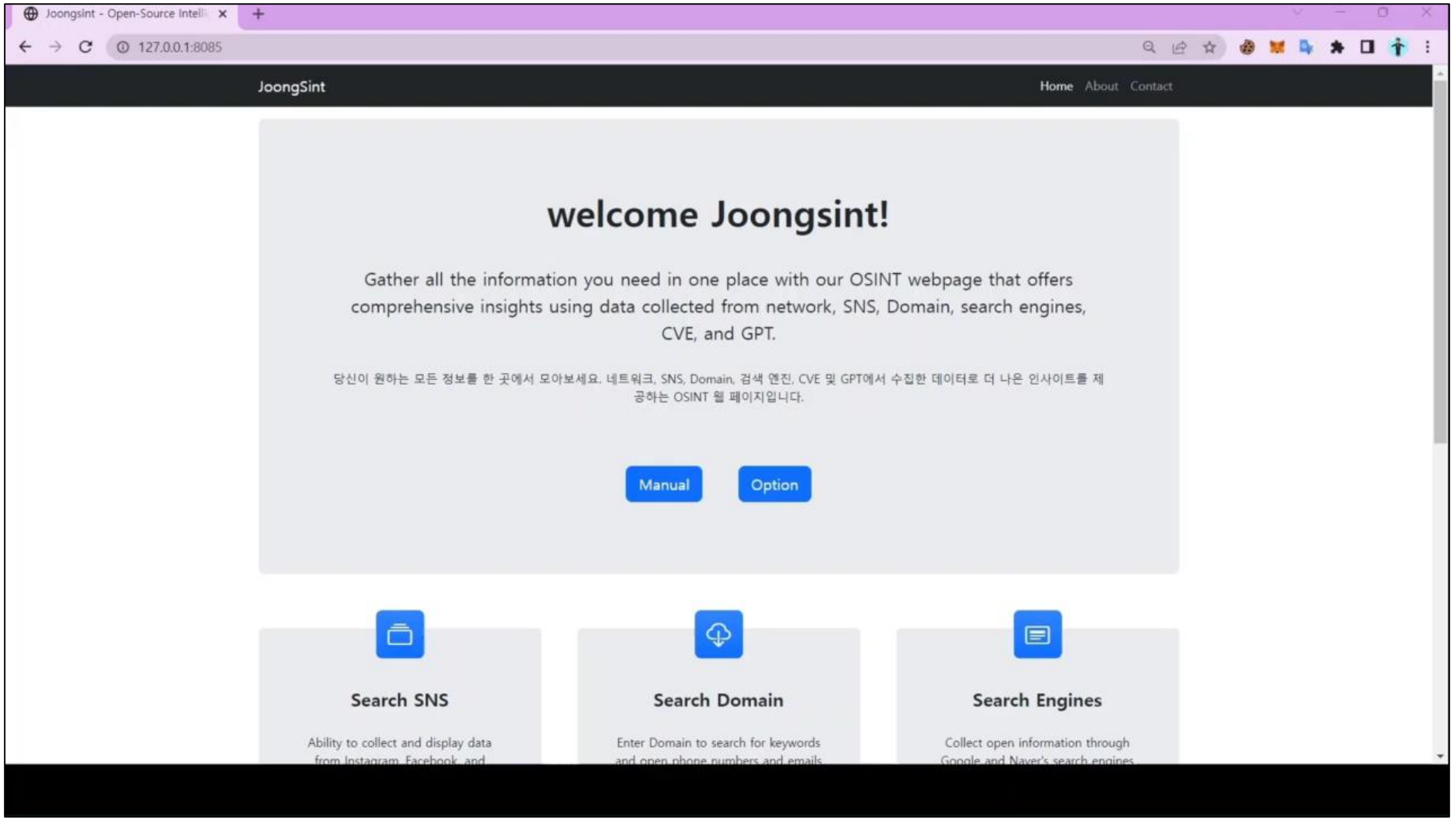
- Instagram, Facebook, Twitter의 사용자 정보를 가져온다.
- **사용자 이름 / 전화번호 / 주소 / 생일 / 이메일 / 기업정보 수집**





1. OSINT 모듈 소개 – SNS 모듈

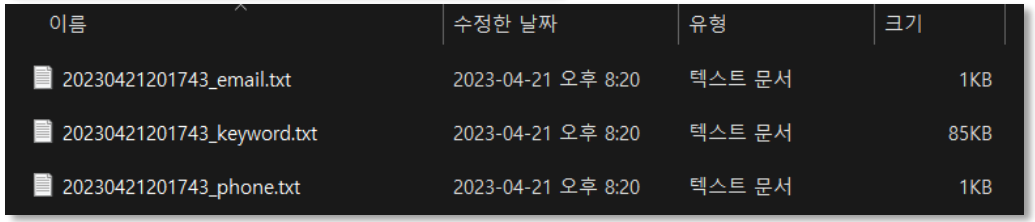
- SNS 시연 영상



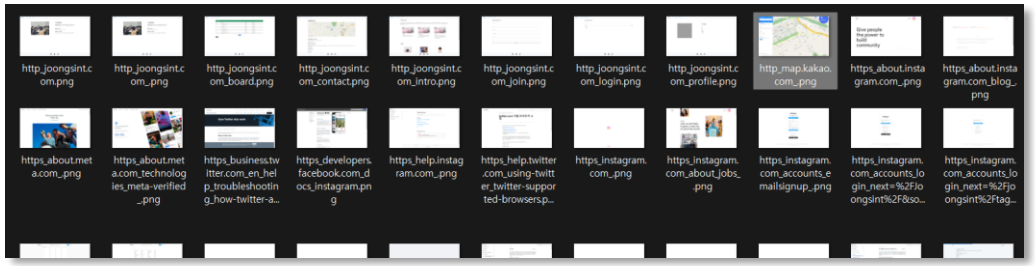
1. OSINT 모듈 소개 – 도메인 모듈

- Selenium을 이용한 도메인 기반 모듈
  - 입력 받은 URL을 기준으로 웹 페이지 크롤링을 진행함.
  - 해당 하는 URL 기준으로 <a> 태그를 수집하여 도메인 순회 깊이 처리를 함.
  - URL 안에 있는 모든 HTML 소스코드를 크롤링하여 정규식을 통해 **키워드/ 이메일 / 전화번호 / 웹페이지 첫 화면 수집**

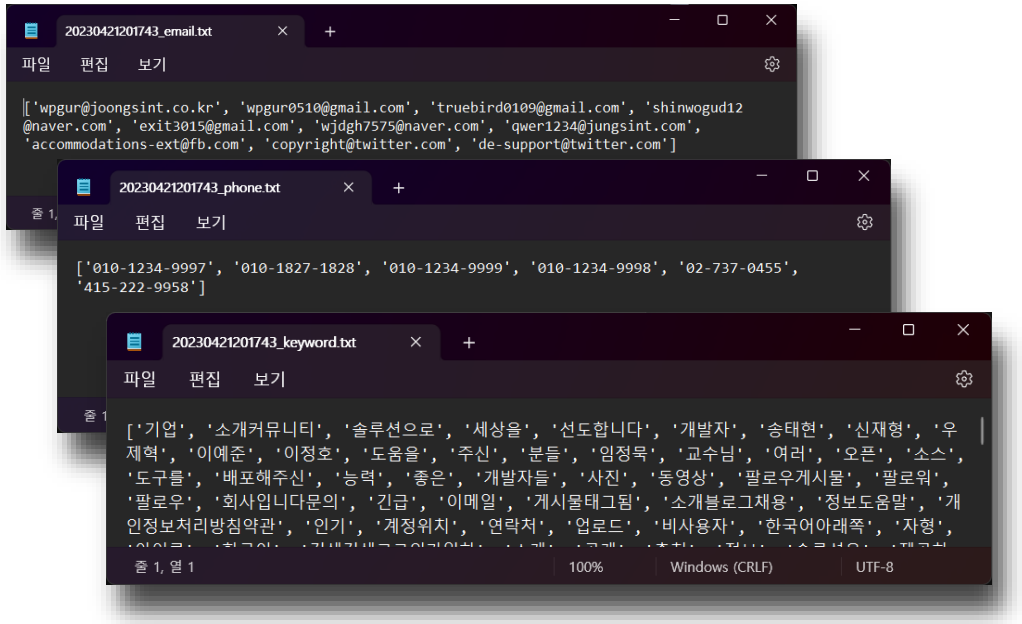
crawling_log 폴더 생성 후 저장



page_capture 폴더 생성 후 저장



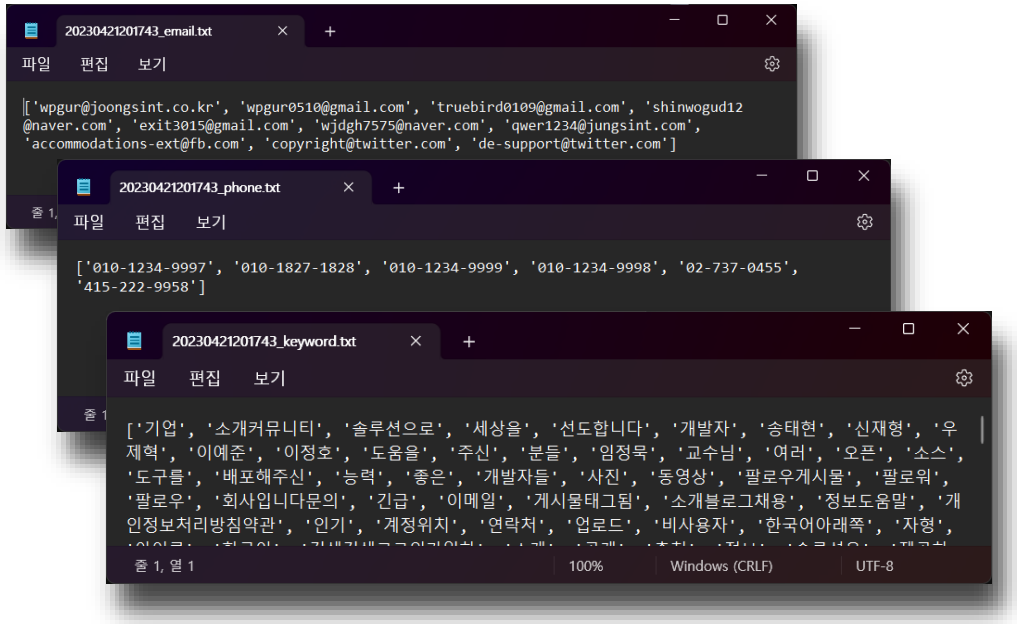
crawling_log 파일 저장 결과



1. OSINT 모듈 소개 – 도메인 모듈

- 도메인 프론트앤드 구현
- 키워드 필터링 및 수집 결과 저장 가능

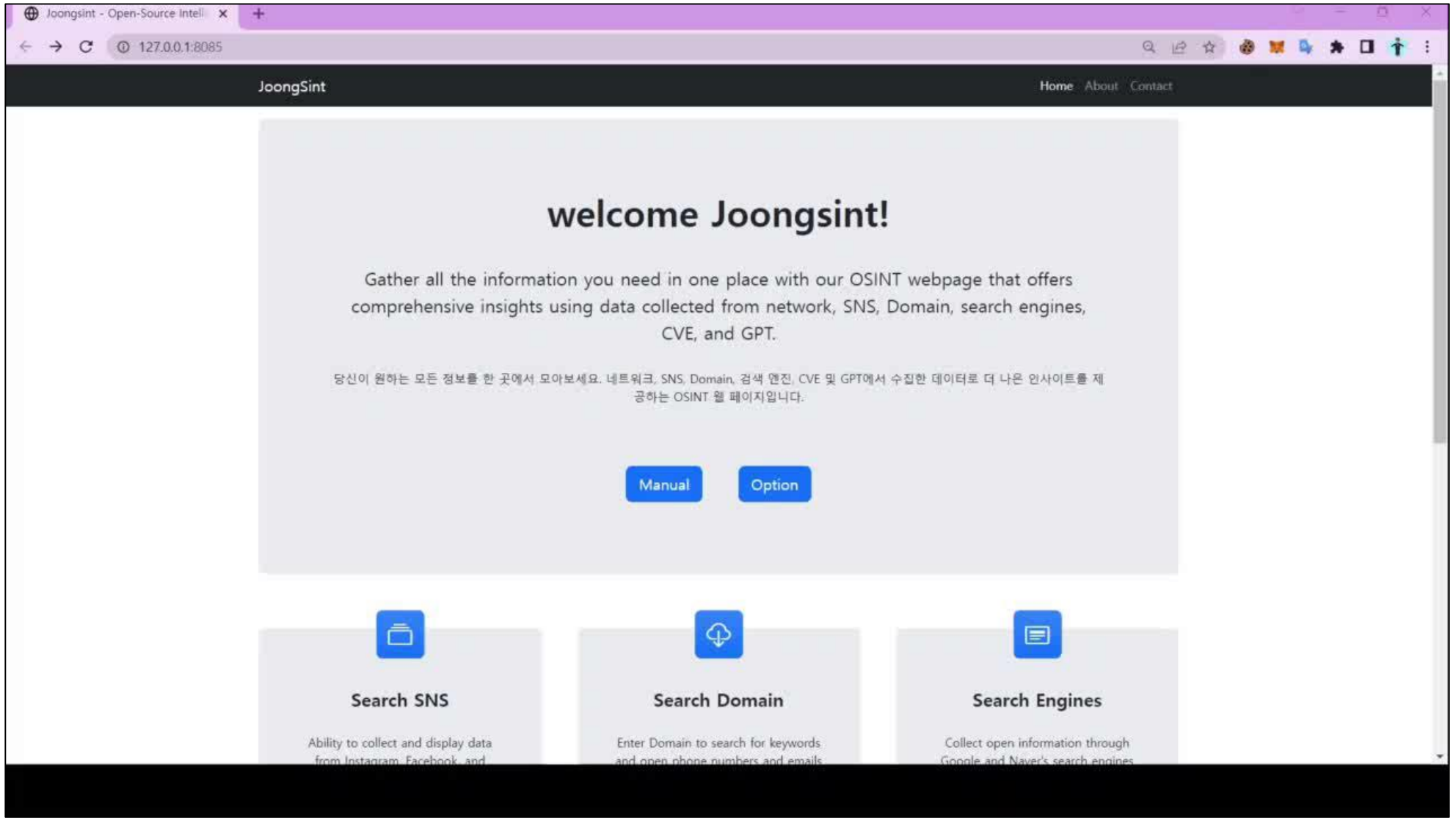
도메인 출력 결과



[domain_result.html]

1. OSINT 모듈 소개 – 도메인 모듈

- 도메인 시연 영상



1. OSINT 모듈 소개 – 검색엔진 모듈

- 검색 엔진(Naver,google) API를 이용해서 검색을 한다.

검색할 단어 입력

Google

검색 페이지 설정

```python
def google_search(self, search_term, page):
    # 검색 시작 인덱스 계산
    start_index = (page - 1) * 10 + 1

    # 검색 API를 이용해 검색
    try:
        service = build("customsearch", "v1", developerKey=self.google_api_key)
        res = service.cse().list(q=search_term, cx=self.google_cse_id, start=start_index).execute(
```

NAVER

```python
def naver_search(self, search_term, page):
    # 검색 시작 인덱스 계산
    start_index = (page - 1) * 10 + 1

    # 검색어 인코딩
    query = urllib.parse.quote(search_term)

    # 네이버 검색 API를 이용해 검색
    url = f"https://openapi.naver.com/v1/search/webkr?query={query}&display=10&start={start_index}"
    headers = {"X-Naver-Client-Id": self.naver_client_id, "X-Naver-Client-Secret": self.naver_client_secret}
```

1. OSINT 모듈 소개 – 검색엔진 모듈

- URL에 접속해서 크롤링하여 원하는 정보를 수집한다.

```python
try:
    # URL에서 HTML 가져오기
    res = requests.get(url)
    html = res.text

    # 이메일 찾기
    email_regex = r"[a-zA-Z0-9._%+-]+@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,}"
    email_match = re.search(email_regex, html)
    if email_match:
        email = email_match.group()
    else:
        email = None

    # 전화번호 찾기
    phone_regex = r"\d{3}-\d{3,4}-\d{4}"
    phone_match = re.search(phone_regex, html)
    if phone_match:
        phone = phone_match.group()
    else:
        phone = None

# 이메일이나 전화번호가 있는 경우 결과 리스트에 추가
    if email or phone:
        self.search_results.append([res.url, [phone, email]])
```

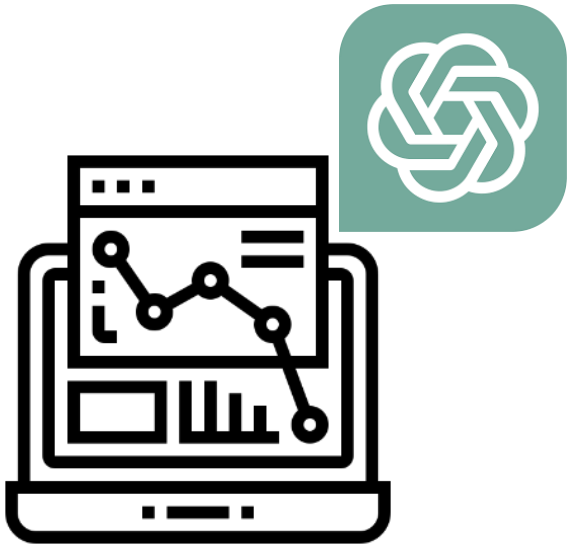
정규 표현식으로 이메일 수집

정규 표현식으로 전화번호 수집

```
[['중부대학교', 'https://www.joongbu.ac.kr/', ['042-750-6219', 'hgr9120@joongbu.ac.kr']
```

1. OSINT 모듈 소개 – 검색엔진 모듈

- gpt-3 API를 이용해서 gpt로 추가 검색



Chat gpt 추가 검색

검색할 단어 + "에 대해 알려줘"

```
def gpt_search(self, search_term):
    question = search_term

    response = self.openai.Completion.create(
        model="text-davinci-002",
        prompt=f"질문: {question}에 대해서 알려줘\n답변:",
        max_tokens=2048
    )

# 생성된 답변을 출력합니다.
    answer = response.choices[0].text.strip()
    print("답변:", answer)
```

1. OSINT 모듈 소개 – 검색엔진 모듈

- 출력 결과
- **관련 도메인 / 이메일 / 전화번호 / GPT 데이터 수집**

```
C:\Users\qkdrn\Desktop\SCP\OSIN>python chat.py
검색어를 입력하세요: 중부대학교
[['중부대학교', 'https://www.joongbu.ac.kr/', ['042-750-6219', 'hgr9120@joongbu.ac.kr']], ['중부대학교 LMS', 'https://edu.joongbu.ac.kr/', ['041-750-6845', None]], ['입학 홈페이지 - 중부대학교', 'https://www.joongbu.ac.kr/ipsi/', ['041-750-6807', 'jechun@joongbu.ac.kr']], ['중부대학교 학생성장교육혁신원', 'https://inedu.joongbu.ac.kr/', ['041-750-6848', 'nam33@joongbu.ac.kr']], ['중부대학교 원격대학원', 'https://cyber.joongbu.ac.kr/', ['031-8075-1164', None]], ['중부대학교', 'https://www.joongbu.ac.kr/', ['042-750-6219', 'hgr9120@joongbu.ac.kr']], ['중부대학교 LMS', 'https://edu.joongbu.ac.kr/', ['041-750-6845', None]], ['입학 홈페이지 - 중부대학교', 'https://www.joongbu.ac.kr/ipsi/', ['041-750-6807', 'jechun@joongbu.ac.kr']], ['중부대학교 학생성장교육혁신원', 'https://inedu.joongbu.ac.kr/', ['041-750-6848', 'nam33@joongbu.ac.kr']], ['중부대학교 원격대학원', 'https://cyber.joongbu.ac.kr/', ['031-8075-1164', None]], ['https://www.joongbu.ac.kr/', ['042-750-6219', 'hgr9120@joongbu.ac.kr']], ['https://www.joongbu.ac.kr/ipsi/', ['041-750-6807', 'jechun@joongbu.ac.kr']], ['https://www.joongbu.ac.kr/undergradList.es?mid=a10202010000&campus_cd=1', ['041-750-6500', None]], ['https://www.joongbu.ac.kr/index.es?sid=a6', ['041-750-6807', 'jechun@joongbu.ac.kr']]]

FINISH

chat_gpt를 사용해 추가 검색 해보시겠습니까? y/n : y
답변: 중부대학교는 대한민국 중부지방에 위치한 6대 출신 대학 중 하나로 명문 대학으로 알려져 있습니다. 현재 재학생은 약 1,000명을 나타내며, 전공 분야는 경영학과, 미디어커뮤니케이션학과, 컴퓨터공학과, 금융학과 등 다양합니다.

중부대학교는 1929년 중부감원대학수학전문대학으로 설립되었으며, 현재는 박영찬 총장의 지도를 받으며 오사카 교토대학교와 공동 교육 협력을 통해 4년제 교육을 하고 있습니다.
```

1. OSINT 모듈 소개 – 검색엔진 모듈

- 검색 엔진 프론트앤드 구현

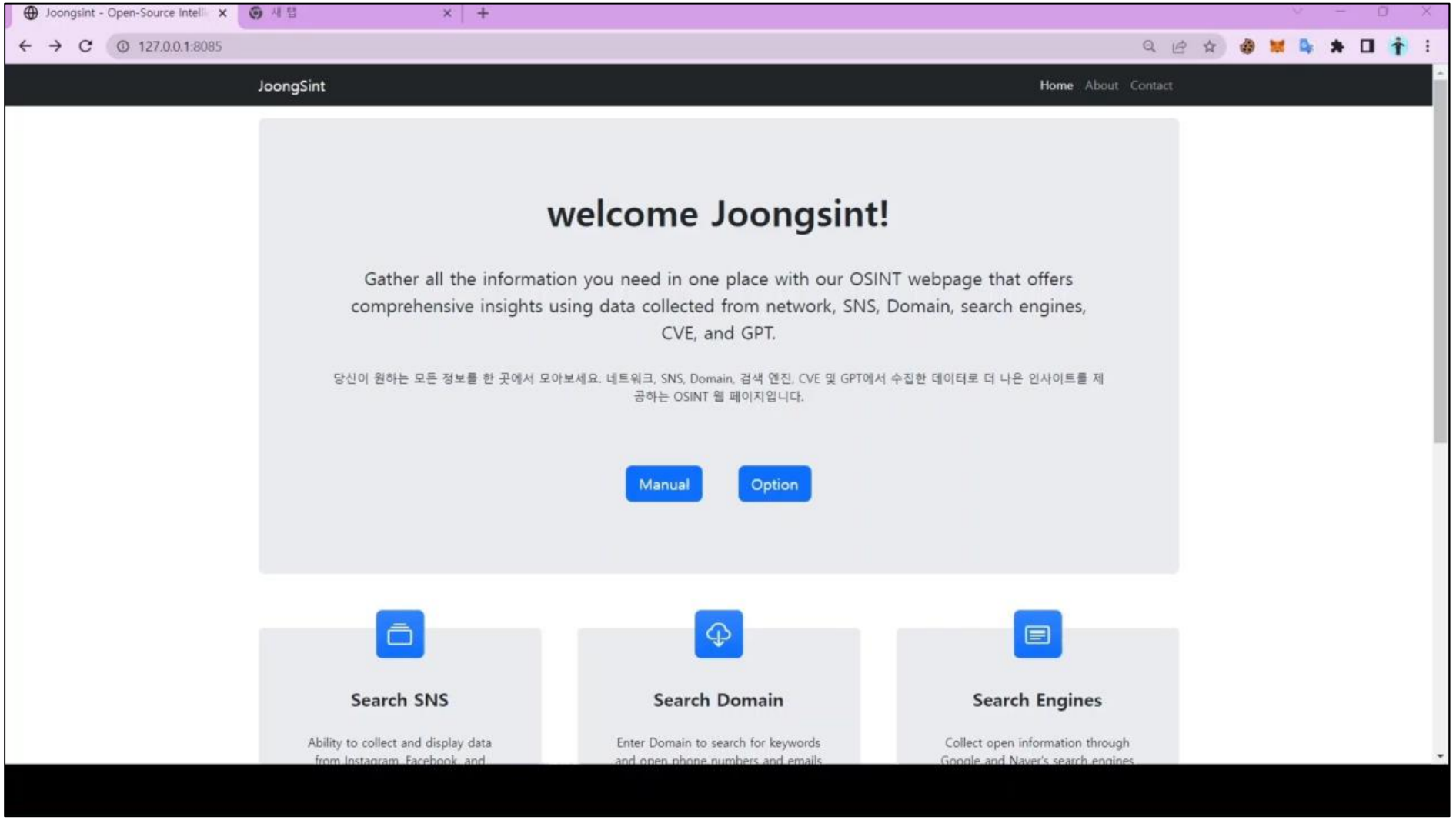
검색 엔진 출력 결과

```
C:\Users\qkdrn\Desktop\SCP\OSIN>python chat.py
검색어를 입력하세요: 중부대학교
[['중부대학교', 'https://www.joongbu.ac.kr/', ['042-750-6219', 'hgr9120@joongbu.ac.kr']], ['중부대학교 LMS', 'https://edu.joongbu.ac.kr/', ['041-750-6845', None]], ['입학 홈페이지 - 중부대학교', 'https://www.joongbu.ac.kr/ipsi/', ['041-750-6807', 'jechun@joongbu.ac.kr']], ['중부대학교 학생성장교육혁신원', 'https://inedu.joongbu.ac.kr/', ['041-750-6848', 'nam33@joongbu.ac.kr']], ['중부대학교 원격대학원', 'https://cyber.joongbu.ac.kr/', ['031-8075-1164', None]], ['중부대학교', 'https://www.joongbu.ac.kr/', ['042-750-6219', 'hgr9120@joongbu.ac.kr']], ['중부대학교 LMS', 'https://edu.joongbu.ac.kr/', ['041-750-6845', None]], ['입학 홈페이지 - 중부대학교', 'https://www.joongbu.ac.kr/ipsi/', ['041-750-6807', 'jechun@joongbu.ac.kr']], ['중부대학교 학생성장교육혁신원', 'https://inedu.joongbu.ac.kr/', ['041-750-6848', 'nam33@joongbu.ac.kr']], ['중부대학교 원격대학원', 'https://cyber.joongbu.ac.kr/', ['031-8075-1164', None]], ['https://www.joongbu.ac.kr/', ['042-750-6219', 'hgr9120@joongbu.ac.kr']], ['https://www.joongbu.ac.kr/ipsi/', ['041-750-6807', 'jechun@joongbu.ac.kr']], ['https://www.joongbu.ac.kr/undergradList.es?mid=a10202010000&campus_cd=1', ['041-750-6500', None]], ['https://www.joongbu.ac.kr/index.es?sid=a6', ['041-750-6807', 'jechun@joongbu.ac.kr']]]

FINISH

chat_gpt를 사용해 추가 검색 해보시겠습니까? y/n : y
답변: 중부대학교는 대한민국 중부지방에 위치한 6대 출신 대학 중 하나로 명문 대학으로 알려져 있습니다. 현재 재학생은 약 1,000명을 나타내며, 전공 분야는 경영학과, 미디어커뮤니케이션학과, 컴퓨터공학과, 금융학과 등 다양합니다.

중부대학교는 1929년 중부감원대학수학전문대학으로 설립되었으며, 현재는 박영찬 총장의 지도를 받으며 오사카 교토대학교와 공동 교육 협력을 통해 4년제 교육을 하고 있습니다.
```

[search_result.html]

1. OSINT 모듈 소개 – 검색엔진 모듈

- 검색 엔진 시연 영상

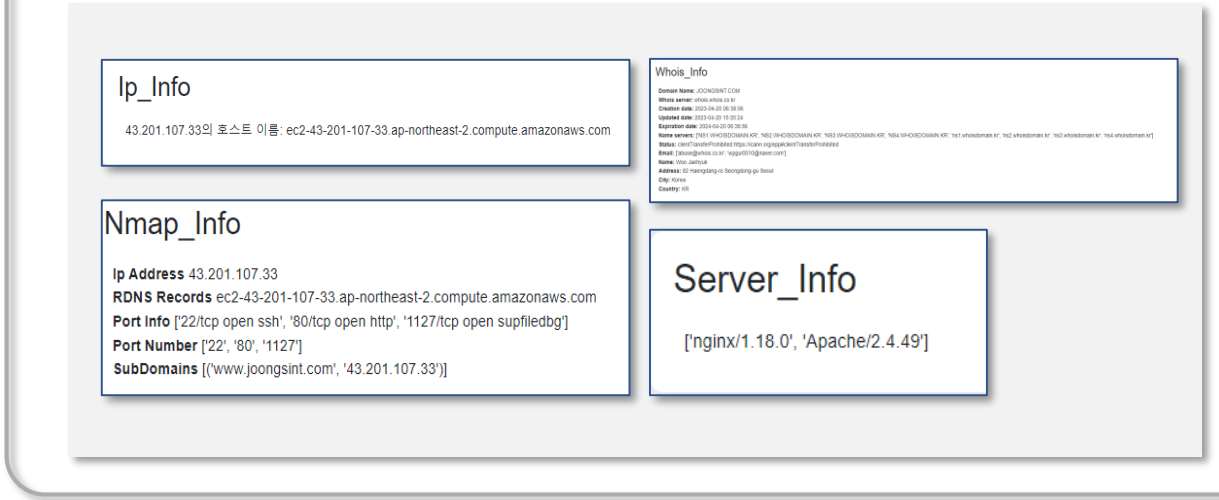


1. OSINT 모듈 소개 – 네트워크 & CVE

네트워크 출력 결과

Whois, Nmap, CVE 등각종 네트워크 관련 정보 스캔

도메인 등록기관 / 등록일 / 네임서버 / 등록자 이름, 이메일 ,주소 / IP / RDNS / Open PORT / SUB domain / Server info 수집



1. OSINT 모듈 소개 – 네트워크 & CVE

- 네트워크 & CVE 프론트앤드 구현
- CVE_ID, CVE 설명, CVSS 점수, CWE 정보 수집

서버 정보 관련 CVE 출력

Server_Info

['nginx/1.18.0', 'Apache/2.4.49']

CVE_Info

CVE ID: CVE-2021-33193
Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.
CVSS Score: 7.5
Category: NVD-CWE-Other

CVE ID: CVE-2021-41773
Description: A flaw was found in a change made to path normalization in Apache HTTP Server 2.4.49. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default configuration "require all denied", these requests can succeed. If CGI scripts are also enabled for these aliased pathes, this could allow for remote code execution. This issue is known to be exploited in the wild. This issue only affects Apache 2.4.49 and not earlier versions. The fix in Apache HTTP Server 2.4.50 was found to be incomplete, see CVE-2021-42013.
CVSS Score: 7.5
Category: CWE-22

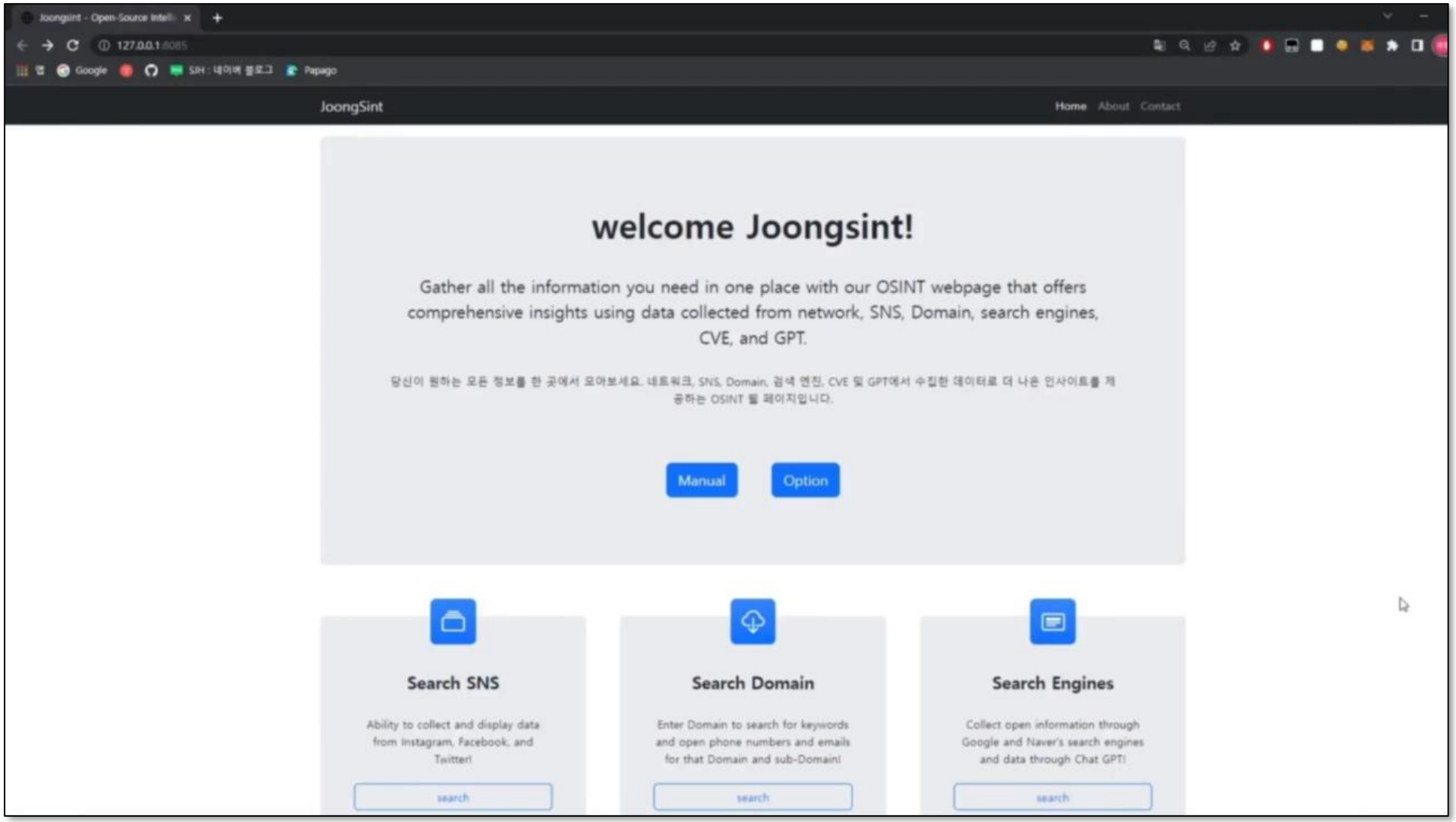
CVE ID: CVE-2021-41524
Description: While fuzzing the 2.4.49 httpd, a new null pointer dereference was detected during HTTP/2 request processing, allowing an external source to DoS the server. This requires a specially crafted request. The vulnerability was recently introduced in version 2.4.49. No exploit is known to the project.
CVSS Score: 7.5
Category: CWE-476

CVE ID: CVE-2021-34798
Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.
CVSS Score: 7.5
Category: CWE-476

CVE ID: CVE-2021-36160
Description: A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).
CVSS Score: 7.5

1. OSINT 모듈 소개 – 네트워크 & CVE

- 네트워크 & CVE 시연 영상



1. OSINT 모듈 소개 – 깃허브 모듈

- 회사 및 사원의 깃허브를 검색하여 내부 코드가 노출 되어있는지 검색

수집 방법

1. 사원 프로필과 찾고자 하는 키워드 입력
2. 해당 키워드의 히스토리 및 래퍼들을 순회하며 해당 키워드 검색
3. 수집된 정보 분석 후 웹 페이지 전달

who	repository	path	content
songtaehyeon	SCP_mentoring	test.md	email : truebird@gmail.com
songtaehyeon	SCP_mentoring	test.md	phone : 010-0101-0101
songtaehyeon	SCP_mentoring	test.md	iP : 112.32.112.53
songtaehyeon	SCP_mentoring	test.md	api : testinday
songtaehyeon	SCP_mentoring	test.md	id : test
songtaehyeon	SCP_mentoring	test/tistory/may.py	#bimil_api : im_bimil
songtaehyeon	SCP_mentoring	test/tistory/truebird/OMG.C	//sEcond_ID : QueenCArd
songtaehyeon	SCP_mentoring	test/tistory/truebird/OMG.C	TEST_PW : P car CHU
songtaehyeon	SCP_mentoring	test/tistory/truebird/test.md	api : jaaja
songtaehyeon	SCP_mentoring	test/tistory/truebird/test.md	pw : sadsada
songtaehyeon	test	README.md	api = test
songtaehyeon	test	README.md	nu = 010-7749-4724

[키워드 기반으로 수집된 github 소스 정보]

2. 데이터 관리 - 보고서

Report - test1

Path: ./crawling_log/test1/ PDF로 변환

LOG - Domain Module

URL	Filter Keyword	Emails	Phones	Keywords
http://www.joongsint.com/intro	wpgur	['wpgur0510@gmail.com', 'truebird0109@gmail.com', 'shinwogud12@naver.com', 'exit3015@gmail.com', 'wjdgh7575@naver.com']	[]	['기업', '소개커뮤니티', '기업', '소개', '공개', '출처', '정보', '솔루션을', '제공하기', '위해']... 더보기
http://www.joongsint.com/contact	정보보호	['qwer1234@jungsint.com']	['010-1234-9999', '010-1234-9998']	['기업', '소개커뮤니티', '창의캠퍼스', '고양', '경기도', '고양시', '덕양구', '통헌로', '찾아오시는', '오시는']... 더보기

LOG - Network Module

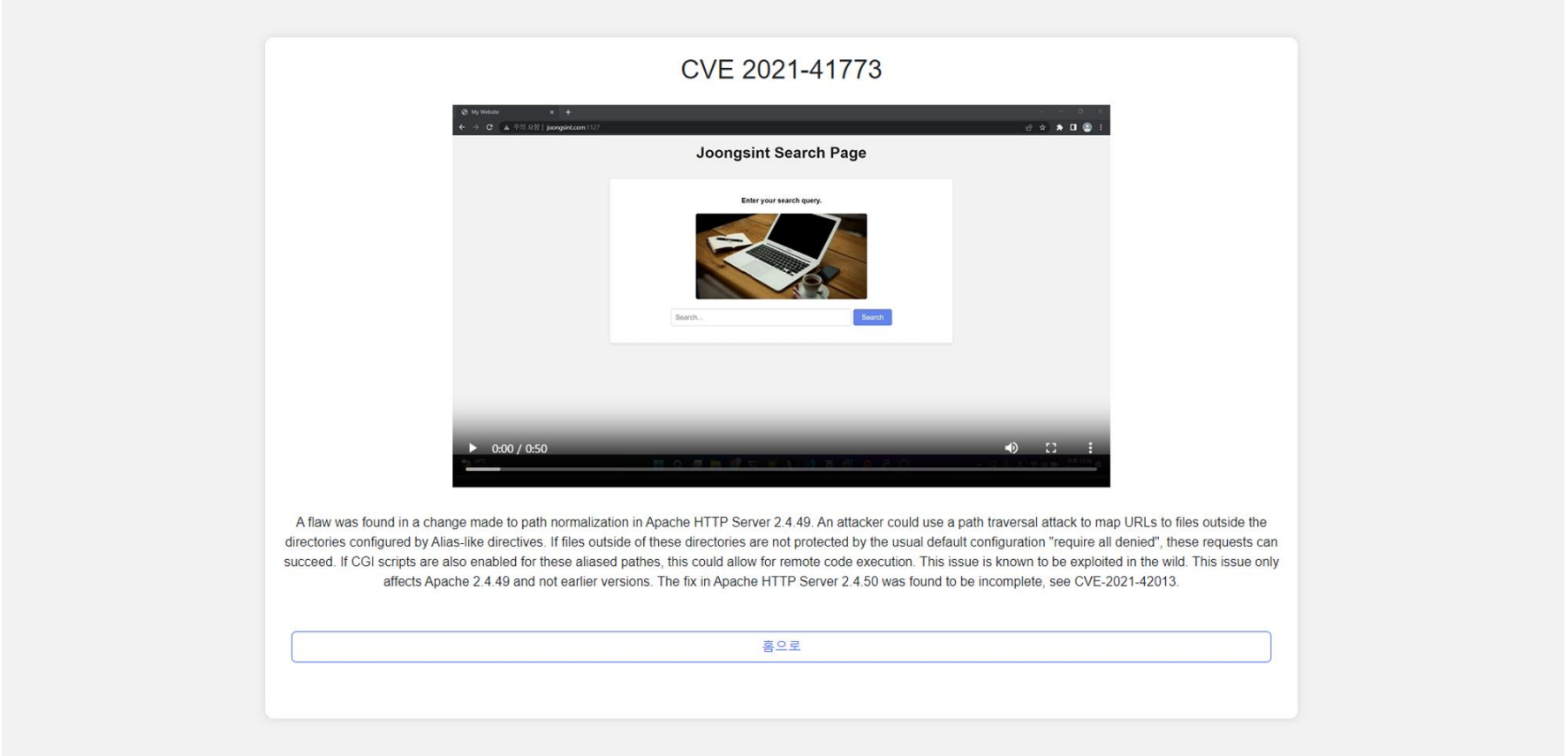
ip	hostname	open port	server version	CVE
43.201.107.33	ec2-43-201-107-33.ap-northeast-2.compute.amazonaws.com	['22/tcp open ssh', '80/tcp open http', '1127/tcp open supfiledbg']	['nginx/1.18.0']	
43.201.107.33	ec2-43-201-107-33.ap-northeast-2.compute.amazonaws.com	['22/tcp open ssh', '80/tcp open http', '1127/tcp open supfiledbg']	['nginx/1.18.0', 'Apache/2.4.49']	CVE-2021-33193 CVE-2021-41773 CVE-2021-41524 CVE-2021-34798 CVE-2021-36160 CVE-2021-42013 CVE-2021-39275 CVE-2021-40438

LOG - Github Module

who	repository	path	content
woojaehyuk	SCP_mentoring	test.md	email : truebird@gmail.com
woojaehyuk	SCP_mentoring	test.md	phone : 010-0101-0101
woojaehyuk	SCP_mentoring	test.md	IP : 112.32.112.53

3. OSINT 활용

- CVE를 통한 서버 익스플로잇 영상 제공



3. OSINT 활용

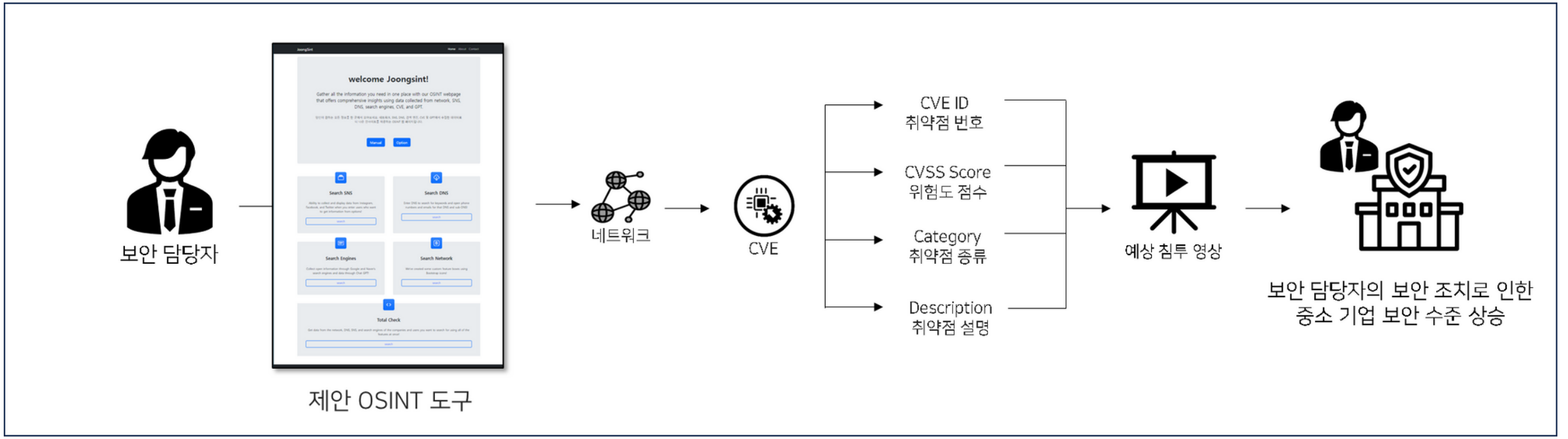
- CVE를 통한 서버 익스플로잇 영상 제공

1-day 공격 시현을 통해 위협에 노출될 수 있는 것을 확인

보안 경각심을 높여 기업 보안을 강화

3. OSINT 활용

- CVE 활용 로직 도식화



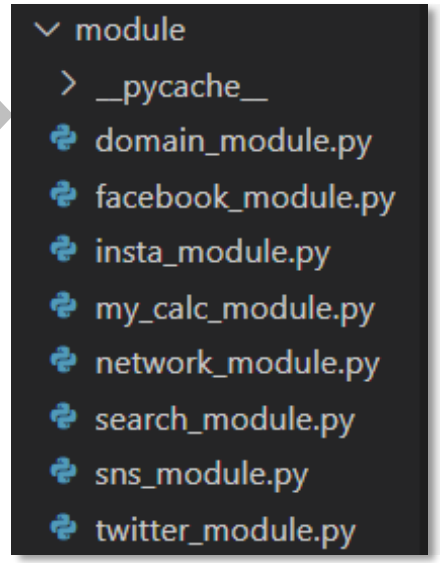
향후 수행계획

Ⅲ 프로젝트 결과

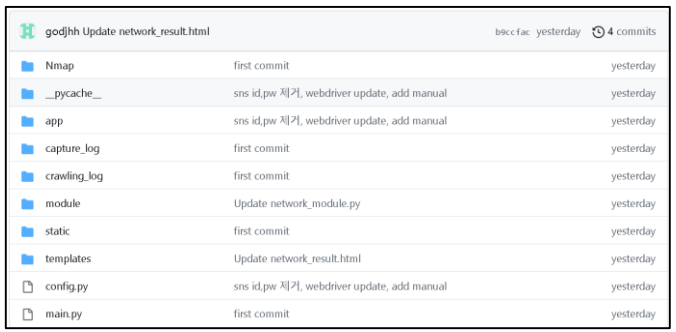
1. 산출물 및 결과
2. 향후 계획

1. 산출물 및 결과

- OSINT 솔루션 도구



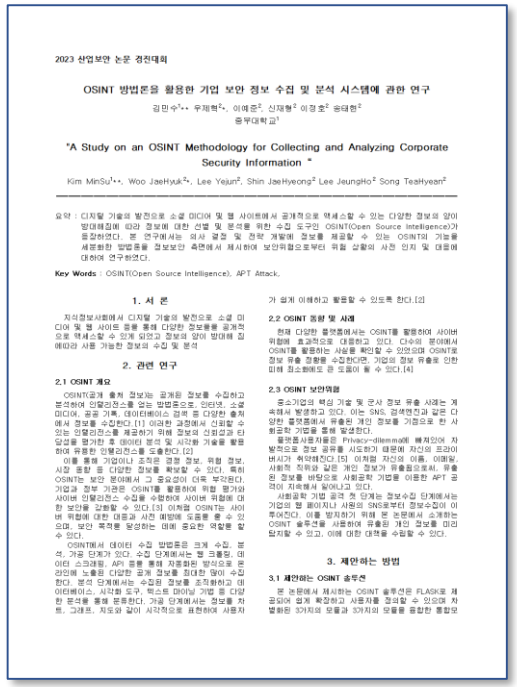

```python
from flask import Flask, render_template
from module.my_calc_module import my_calc_module
from module.sns_module import sns_module
from module.insta_module import insta_module
from module.facebook_module import facebook_module
from module.twitter_module import twitter_module
from module.search_module import search_module
from module.domain_module import domain_module
from module.network_module import network_module
import config as config


app = Flask(__name__)
app.register_blueprint(my_calc_module)
app.register_blueprint(sns_module)
app.register_blueprint(insta_module)
app.register_blueprint(facebook_module)
app.register_blueprint(twitter_module)
app.register_blueprint(search_module)
app.register_blueprint(domain_module)
app.register_blueprint(network_module)
```



1. 산출물 및 결과

- 2023 한국융합보안학회 하계학술대회
- SNS와 도메인 모듈을 중점으로 활용 방법론에 대한 내용을 논문으로 준비

OSINT 방법론을 활용한 기업 보안 정보 수집 및 분석 시스템에 관한 연구



2023 산업보안 논문 경진대회

OSINT 방법론을 활용한 기업 보안 정보 수집 및 분석 시스템에 관한 연구

김민수[1]*, 우제혁[2], 이예준[2], 신재형[2] 이정호[2] 송태현[2]
중부대학교[1]

"A Study on an OSINT Methodology for Collecting and Analyzing Corporate Security Information "

Kim MinSu[1]*, Woo JaeHyuk[2], Lee Yejun[2], Shin JaeHyeong[2] Lee JeungHo[2] Song TaeHyean[2]

요약 : 디지털 기술의 발전으로 소셜 미디어 및 웹 사이트에서 공개적으로 액세스할 수 있는 다양한 정보의 양이 방대해짐에 따라 정보에 대한 선별 및 분석을 위한 수집 도구인 OSINT(Open Source Intelligence)가 중요해졌다. 본 연구에서는 의사 결정 및 전략 개발에 정보를 제공할 수 있는 OSINT의 기능을 세분화한 방법론을 정보보안 측면에서 제시하여 보안위협으로부터 위협 상황의 사전 인지 및 대응에 대하여 연구하였다.

Key Words : OSINT(Open Source Intelligence), APT Attack,

1. 서 론

자식정보사회에서 디지털 기술의 발전으로 소셜 미디어 및 웹 사이트 등을 통해 다양한 정보들을 공개적으로 액세스할 수 있게 되었고 정보의 양이 방대해 짐에따라 사용 가능한 정보의 수집 및 분석

2. 관련 연구

2.1 OSINT 개요

OSINT(공개 출처 정보)는 공개된 정보를 수집하고 분석하여 인텔리전스를 얻는 방법론으로, 인터넷, 소셜 미디어, 공공 기록, 데이터베이스 검색 등 다양한 출처에서 정보를 수집한다 [1] 이러한 과정에서 신뢰할 수 있는 인텔리전스를 제공하기 위해 정보의 신뢰성과 타당성을 평가한 후 데이터 분석 및 시각화 기술을 활용하여 유용한 인텔리전스를 도출한다 [2]

이를 통해 기업이나 조직은 경쟁 정보, 위협 정보, 시장 동향 등 다양한 정보를 확보할 수 있다. 특히 OSINT는 보안 분야에서 그 중요성이 더욱 부각되고 있다. 기업과 정부 기관은 OSINT를 활용하여 위협 평가와 사이버 인텔리전스 수집을 수행하여 사이버 위협에 대한 보안을 강화할 수 있다.[3] 이처럼 OSINT는 사이버 위협에 대한 대응과 사전 예방에 도움을 줄 수 있으며, 보안 목적을 달성하는 데에 중요한 역할을 할 수 있다.

OSINT에서 데이터 수집 방법론은 크게 수집, 분석, 가공 단계가 있다. 수집 단계에서는 웹 크롤링, 데이터 스크래핑, API 등을 통해 자동화된 방식으로 온라인에 노출된 다양한 공개 정보를 최대한 많이 수집한다. 분석 단계에서는 수집된 정보를 조직화하고 데이터베이스, 시각화 도구, 텍스트 마이닝 기법 등 다양한 분석을 통해 분류한다. 가공 단계에서는 정보를 차트, 그래프, 지도와 같이 시각적으로 표현하여 사용자가 쉽게 이해하고 활용할 수 있도록 한다.[2]

2.2 OSINT 동향 및 사례

현재 다양한 플랫폼에서는 OSINT를 활용하여 사이버 위협에 효과적으로 대응하고 있다. 다수의 분야에서 OSINT를 활용하는 사실을 확인할 수 있었으며 OSINT로 정보 유출 경향을 수집한다면, 기업의 정보 유출로 인한 미래 잠소원해도 큰 도움이 될 수 있다.[4]

2.3 OSINT 보안위협

중소기업의 핵심 기술 및 군사 정보 유출 사례는 계속해서 발생하고 있다. 이는 SNS, 검색엔진과 같은 다양한 플랫폼에서 유출한 개인 정보를 기업으로 한 사회공학 기법을 통해 발생한다.

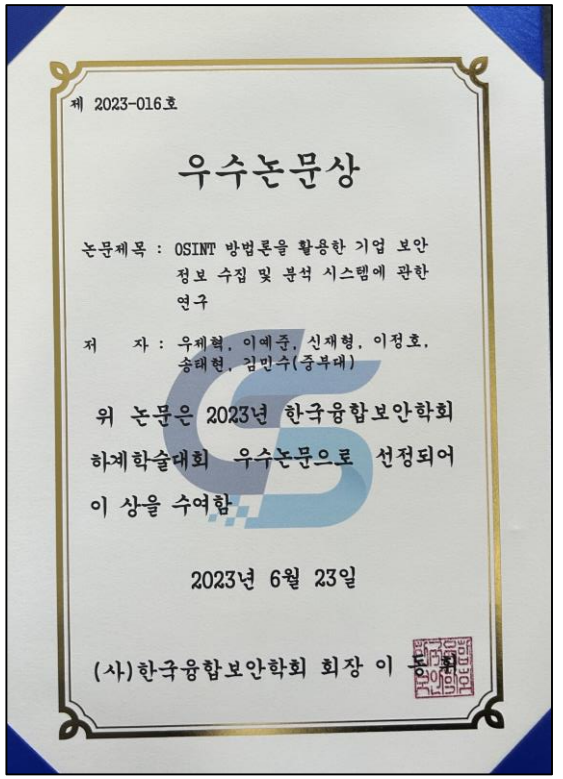
플랫폼사용자들은 Privacy-dilemma에 빠지면서 자발적으로 정보 공유를 시도한다 때문에 자신의 프라이버시가 취약해진다.[5] 이처럼 자신의 이름, 이메일, 사회적 직위와 같은 개인 정보가 유출됨으로써, 유출된 정보를 바탕으로 사회공학 기법을 이용한 APT 공격이 자행돼 일어나고 있다.

사회공학 기법 공격 첫 단계는 정보수집 단계에서는 기업의 웹 페이지나 사원의 SNS로부터 정보수집이 이루어진다. 이를 방지하기 위해 본 논문에서 소개하는 OSINT 솔루션을 사용하여 유출된 개인 정보를 미리 탐지할 수 있고, 이에 대한 대책을 수립할 수 있다.

3. 제안하는 방법

3.1 제안하는 OSINT 솔루션

본 논문에서 제시하는 OSINT 솔루션은 FLASK로 제공되어 쉽게 확장하고 사용자를 정의할 수 있으며 차별화된 3가지의 모듈과 3가지의 모듈을 융합한 통합모



제 2023-016호

우수논문상

논문제목 : OSINT 방법론을 활용한 기업 보안 정보 수집 및 분석 시스템에 관한 연구

저 자 : 우제혁, 이예준, 신재형, 이정호, 송태현, 김민수(중부대)

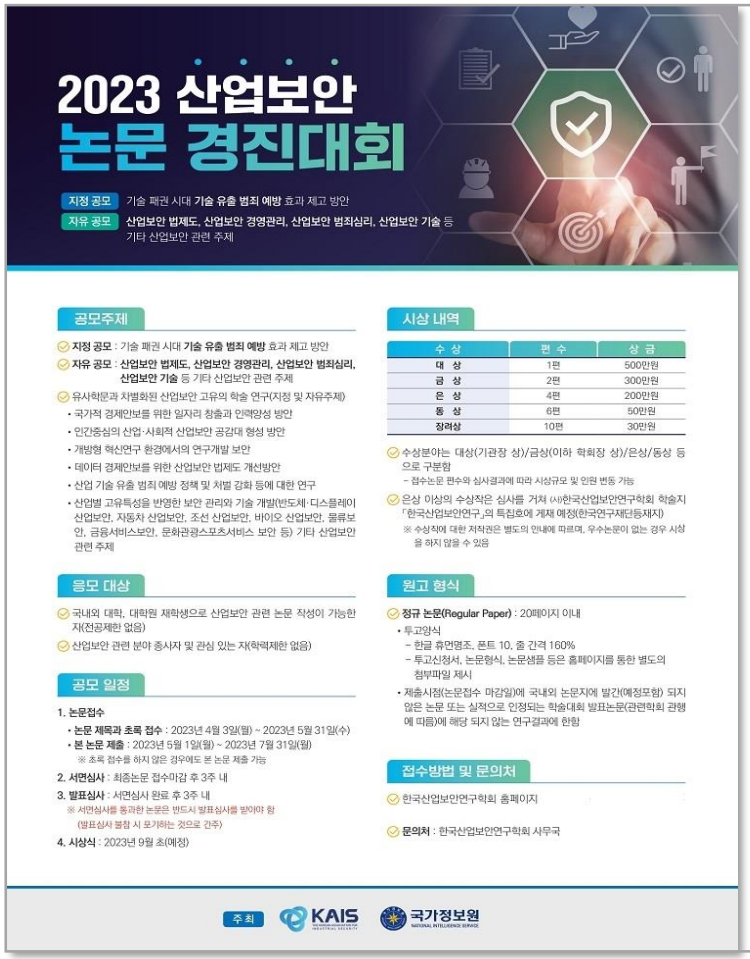
위 논문은 2023년 한국융합보안학회 하계학술대회 우수논문으로 선정되어 이 상을 수여함.

2023년 6월 23일

(사)한국융합보안학회 회장 이 용 [illegible]

1. 산출물 및 결과

- 2023 산업보안 논문경진대회
- 네트워크 정보를 통해 1-day 공격 가능성 제시와 github osint를 통해 위협 가능성 제시 논문 투고 예정



2023 산업보안 논문 경진대회

지정 공모 기술 패권 시대 **기술 유출 범죄 예방** 효과 제고 방안

자유 공모 **산업보안 법제도, 산업보안 경영관리, 산업보안 범죄심리, 산업보안 기술** 등 기타 산업보안 관련 주제

공모주제

- **지정 공모** : 기술 패권 시대 **기술 유출 범죄 예방** 효과 제고 방안
- **자유 공모** : **산업보안 법제도, 산업보안 경영관리, 산업보안 범죄심리, 산업보안 기술** 등 기타 산업보안 관련 주제
- 유사학문과 차별화된 산업보안 고유의 학술 연구(지정 및 자유주제)
  - 국가적 경제안보를 위한 일자리 창출과 인력양성 방안
  - 인간중심의 산업·사회적 산업보안 공감대 형성 방안
  - 개방형 혁신연구 환경에서의 연구개발 보안
  - 데이터 경제안보를 위한 산업보안 법제도 개선방안
  - 산업 기술 유출 범죄 예방 정책 및 처벌 강화 등에 대한 연구
  - 산업별 고유특성을 반영한 보안 관리와 기술 개발(반도체·디스플레이 산업보안, 자동차 산업보안, 조선 산업보안, 바이오 산업보안, 물류보안, 금융서비스보안, 문화관광스포츠서비스 보안 등) 기타 산업보안 관련 주제

응모 대상

- 국내외 대학, 대학원 재학생으로 산업보안 관련 논문 작성이 가능한 자(전공제한 없음)
- 산업보안 관련 분야 종사자 및 관심 있는 자(학력제한 없음)

공모 일정

1. **논문접수**
   - **논문 제목과 초록 접수** : 2023년 4월 3일(월) ~ 2023년 5월 31일(수)
   - **본 논문 제출** : 2023년 5월 1일(월) ~ 2023년 7월 31일(월)
     ※ 초록 접수를 하지 않은 경우에도 본 논문 제출 가능
2. **서면심사** : 최종논문 접수마감 후 3주 내
3. **발표심사** : 서면심사 완료 후 3주 내
   ※ 서면심사를 통과한 논문은 반드시 발표심사를 받아야 함
   (발표심사 불참 시 포기하는 것으로 간주)
4. **시상식** : 2023년 9월 초(예정)

시상 내역

수 상	편 수	상 금
대 상	1편	500만원
금 상	2편	300만원
은 상	4편	200만원
동 상	6편	50만원
장려상	10편	30만원

- 수상분야는 대상(기관장 상)/금상(이하 학회장 상)/은상/동상 등으로 구분함
  - 접수논문 편수와 심사결과에 따라 시상규모 및 인원 변동 가능
- 은상 이상의 수상작은 심사를 거쳐 (사)한국산업보안연구학회 학술지 「한국산업보안연구」의 특집호에 게재 예정(한국연구재단등재지)
  ※ 수상작에 대한 저작권은 별도의 안내에 따르며, 우수논문이 없는 경우 시상을 하지 않을 수 있음

원고 형식

- **정규 논문(Regular Paper)** : 20페이지 이내
  - 투고양식
    - 한글 휴먼명조, 폰트 10, 줄 간격 160%
    - 투고신청서, 논문형식, 논문샘플 등은 홈페이지를 통한 별도의 첨부파일 제시
  - 제출시점(논문접수 마감일)에 국내외 논문지에 발간(예정포함) 되지 않은 논문 또는 실적으로 인정되는 학술대회 발표논문(관련학회 관행에 따름)에 해당 되지 않는 연구결과에 한함

접수방법 및 문의처

- 한국산업보안연구학회 홈페이지
- **문의처** : 한국산업보안연구학회 사무국

주최 KAIS 국가정보원

중소 기업 보안 위협 탐지를 위해 분석 단계를 체계적으로 활용한 포괄적인 OSINT 솔루션

- 주최 및 주관: KAIS THE KOREAN ASSOCIATION FOR INDUSTRIAL SECURITY 국가정보원 NATIONAL INTELLIGENCE SERVICE
- 논문 초록 제출 완료
- 본 논문 제출 일정: 23.05.1 ~ 23.07.31
- 원고 형식: 정규 논문 20페이지 이내

2. 향후 계획

- 추후 프로젝트를 보완하여 많은 컨퍼런스 발표 계획

Black Hat

Hack In The Box

CodeGate

발표 들어주셔서 감사합니다.

CCIT
CULTURE CONTENTS & INFORMATION TECHNOLOGY