Secure Hub

CY-TER

2371078 김수민 (기획, 백엔드)

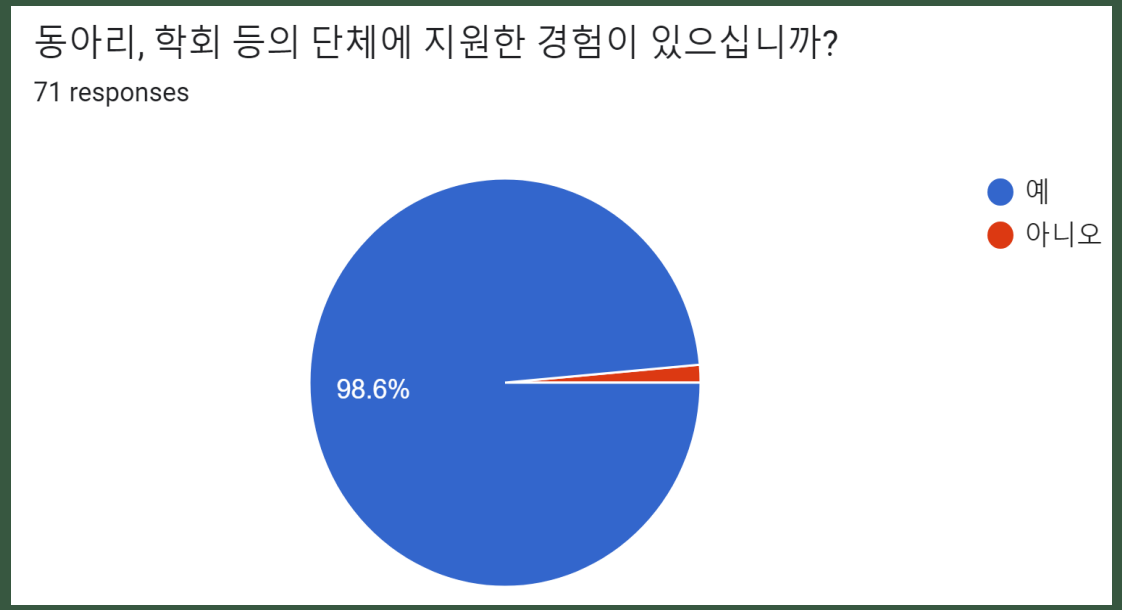
2371097 조휘정 (기술, 백엔드)

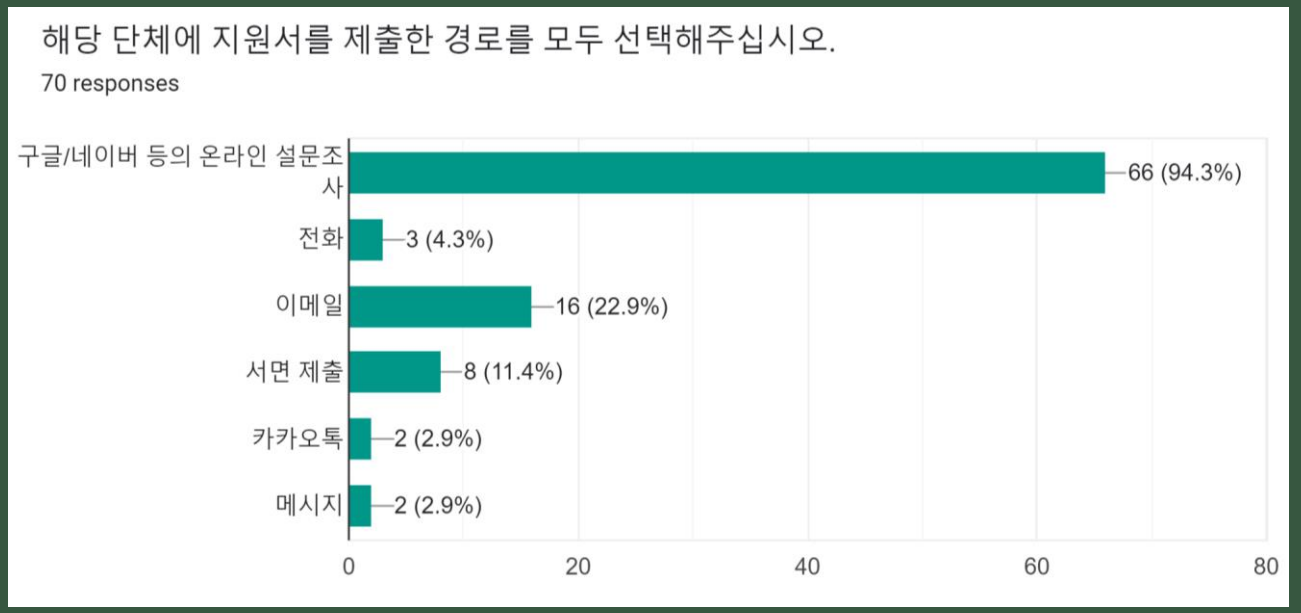
2371008 곽인정 (백엔드)

2371096 장예린 (프론트엔드)

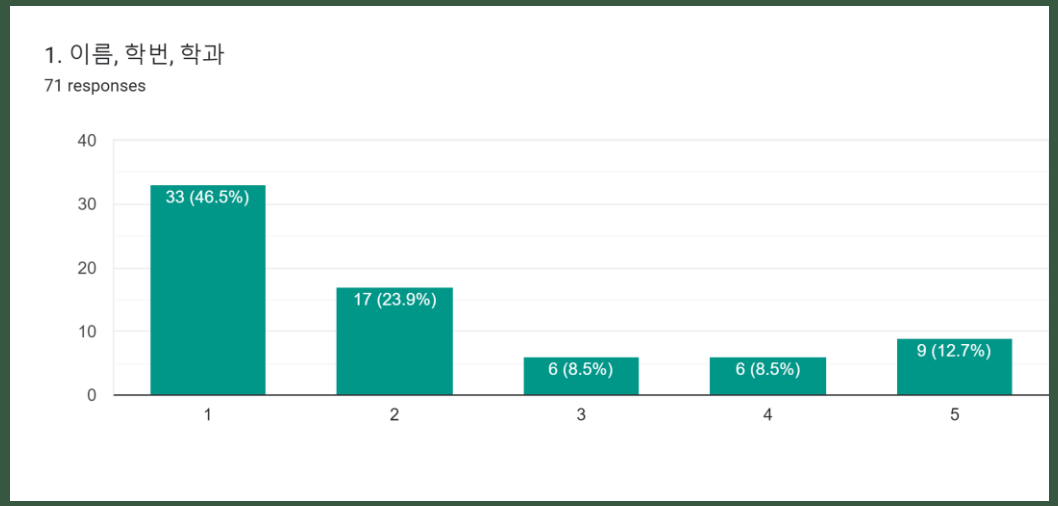
2371086 염혜선(프론트엔드)

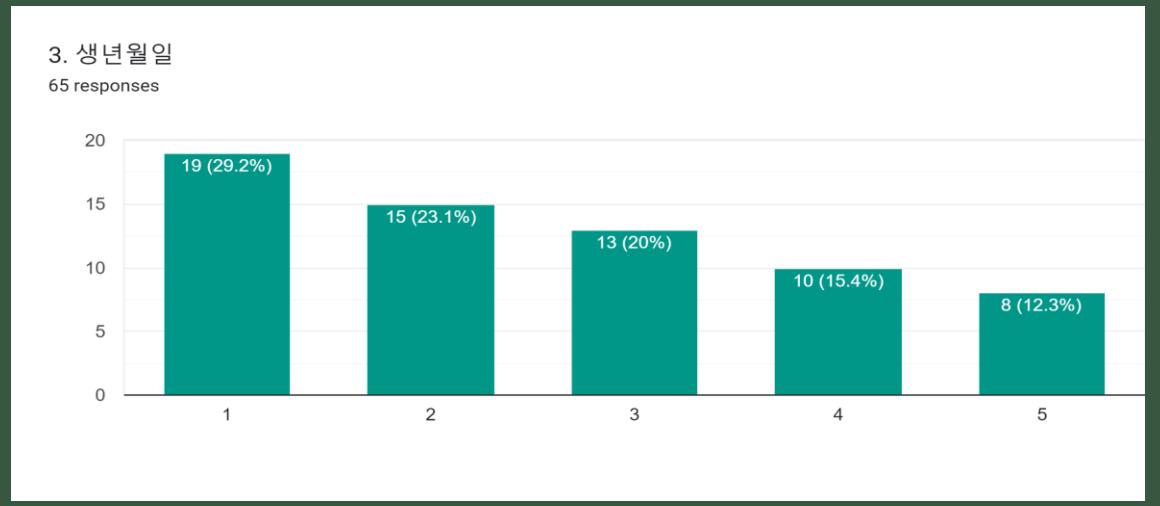
교내 설문조사 실시

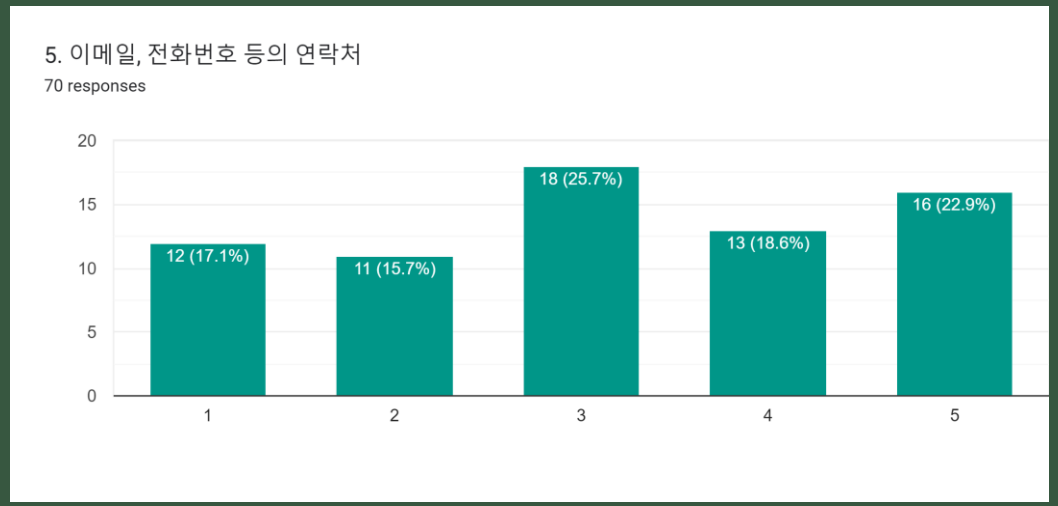


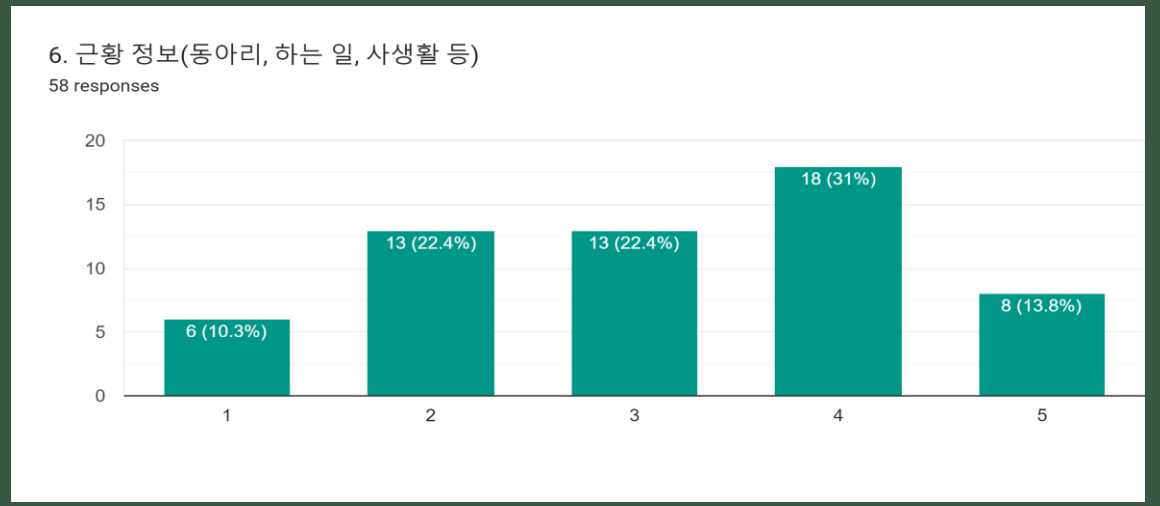


많은 이화인들이 동아리와 학회 지원을 위해
구글폼 과 네이버폼 형태의 온라인 설문조사를 이용





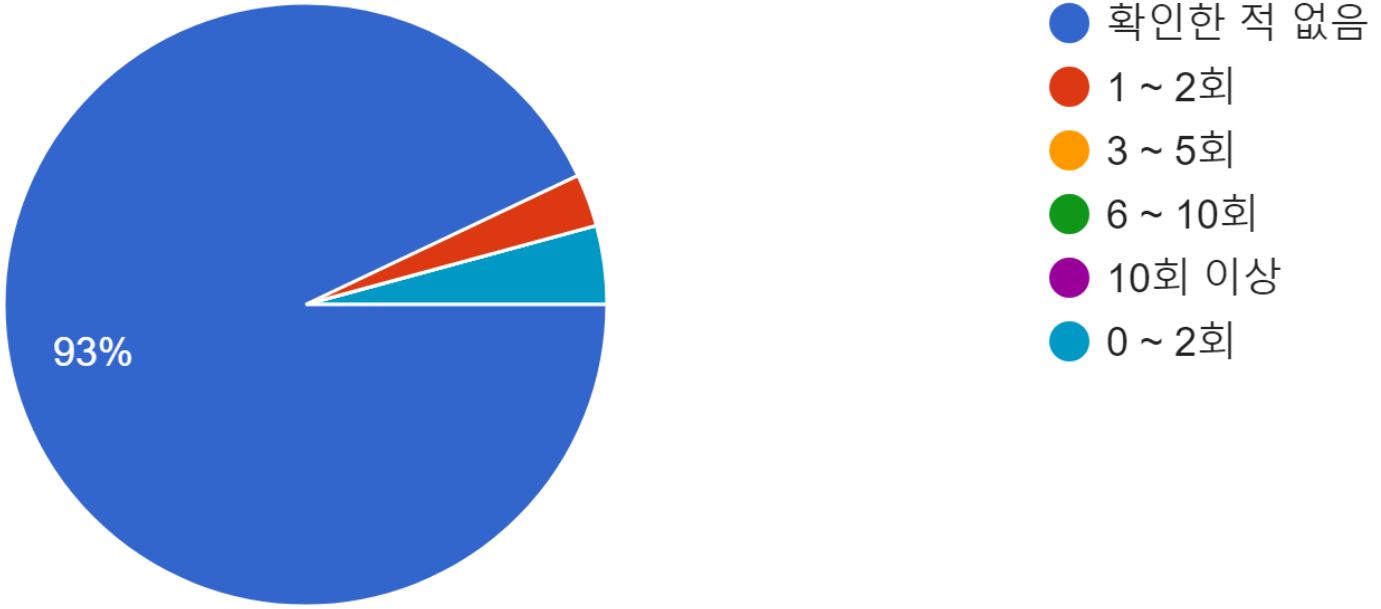




얼굴 사진, 연락처, 주소와 같은 개인정보 제공 시 많은 이화인들이
정보 유출의 부담을 느낀다고 답변

본인의 정보가 폐기되었다는 사실을 실제로 확인한 사례가 있습니까?

71 responses



설문이 이루어진 후
자신이 제공한 정보가 폐기되었음을 확인한 사례는 6퍼센트 미만

동아리 및 학회, 공동구매의 홍보가 이루어지는 에브리타임에는

이화여대 학생이 아닌 외부인이 있는 경우도 허다

동아리 또한 종교단체나 이익추구 단체가 만든 경우도 존재

또한 연합 동아리와 학회 중 학교의 승인이 없거나 운영주체 불분명한 경우가 다수 존재

문제 해결을 위해 Secure Hub 필요

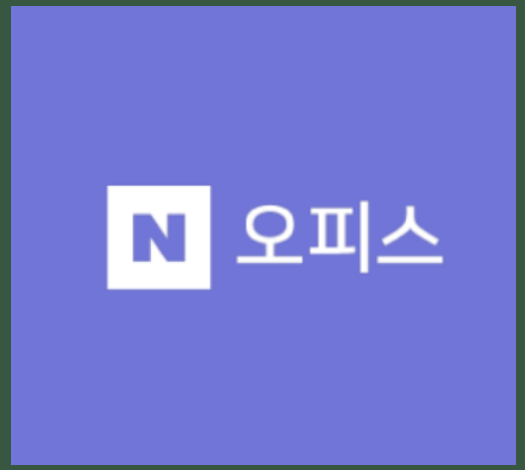
Cy-ter 방향성

Secure Hub는 이화인의 개인정보 노출 걱정 없는 안전한 대학생활

언제나 익명성을 보장받으며 의견을 제시할 수 있는 권리 보장

다양하고 직접적인 피드백을 통한 학교 생활의 질 향상에 도움이 되고 싶습니다

웹 구현 목적



온라인 설문 서비스를 통해 지원자의 개인정보를 전달할 때

정보에 제한적으로 접근하거나 민감한 정보를 필요시에만

열람할 수 있는 방법에 대해 고안

웹 기능 구상

- 개인정보 암호화

설문 응답자가 폼 형태의 설문을 제출하는 즉시 암호화

- 상호 동의 후 복호화

동아리 합격, 공동구매 확정 등과 같이 결과가 발표 후 설문 작성자와 응답자의 상호 동의가 있어야 개인정보를 복호화 가능

-데이터 즉시 폐기

복호화 되지 않은 모든 데이터들은 설문 기간이 끝나는 즉시 폐기하여 개인정보 노출 방지

Secure Hub "안전한 중심지"

: 사이트를 사용하는 이화인이라면
누구나 자신의 정보를 안전하게 관리할 수 있다는 의미

Secure Hub

메뉴 버튼을 클릭하여

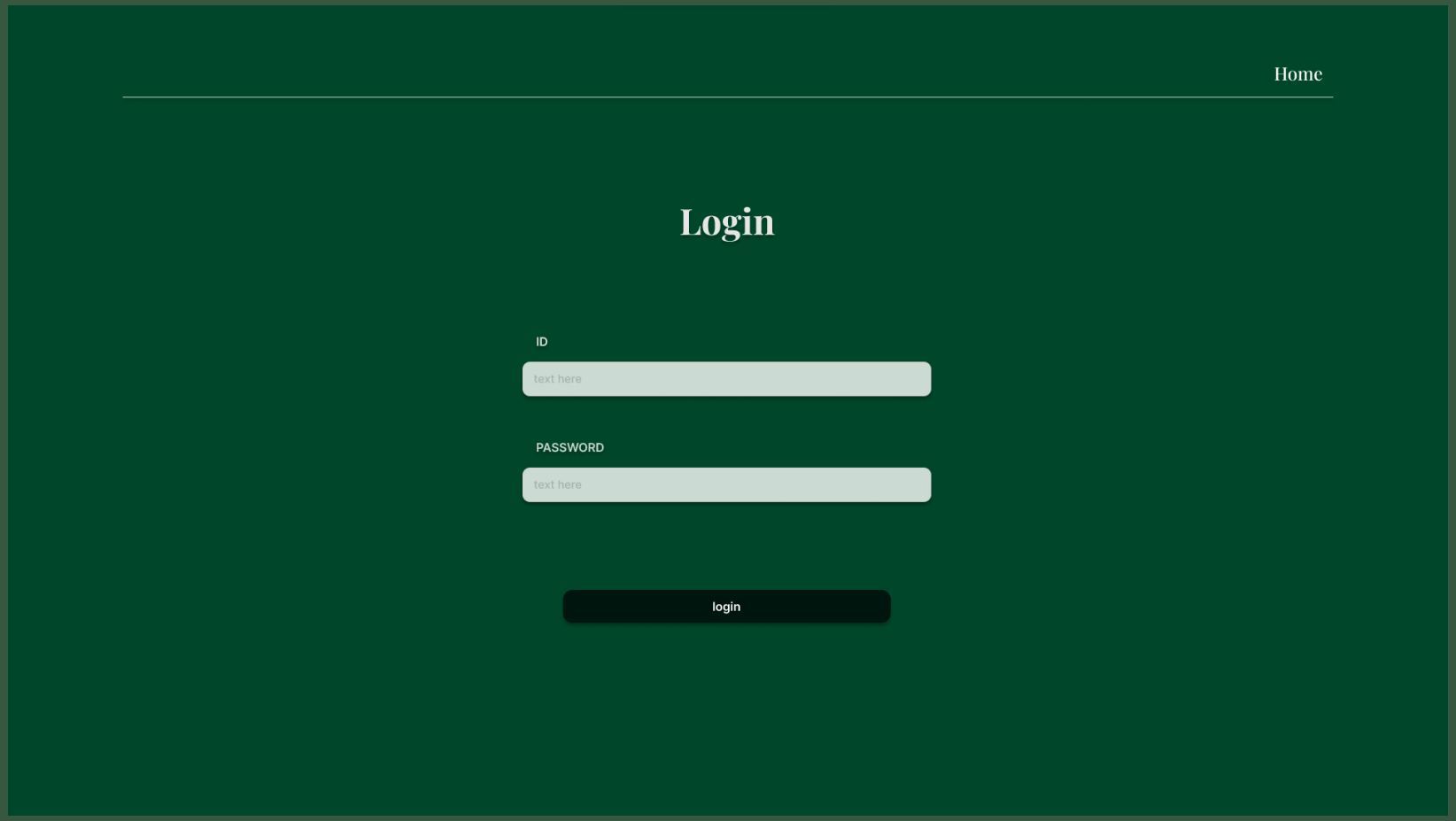
Secure Hub

welcome to ewha

Login
Search
Mypage

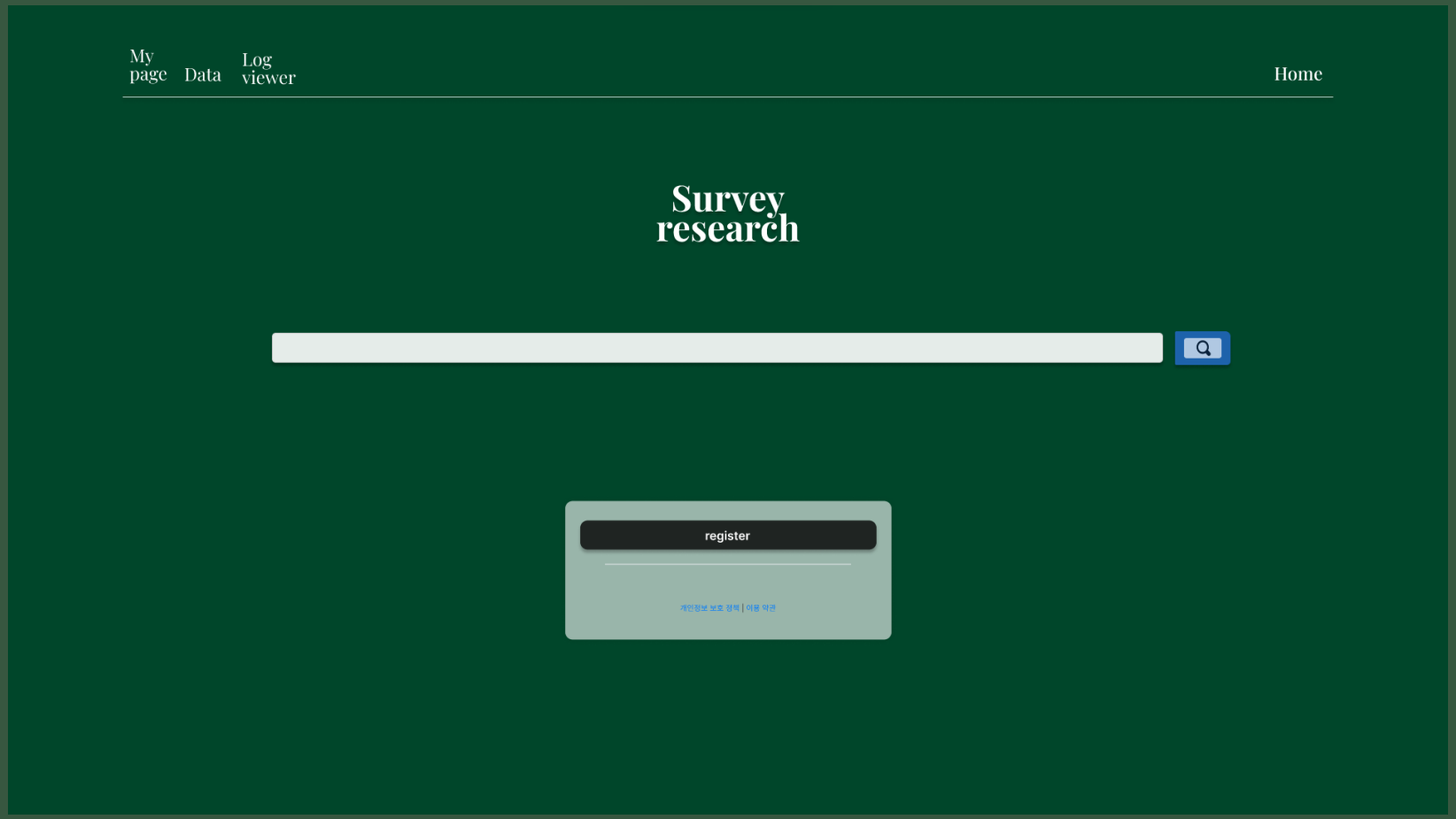
로그인, 설문 찾기, 마이페이지 기능으로 이동 가능

Secure Hub



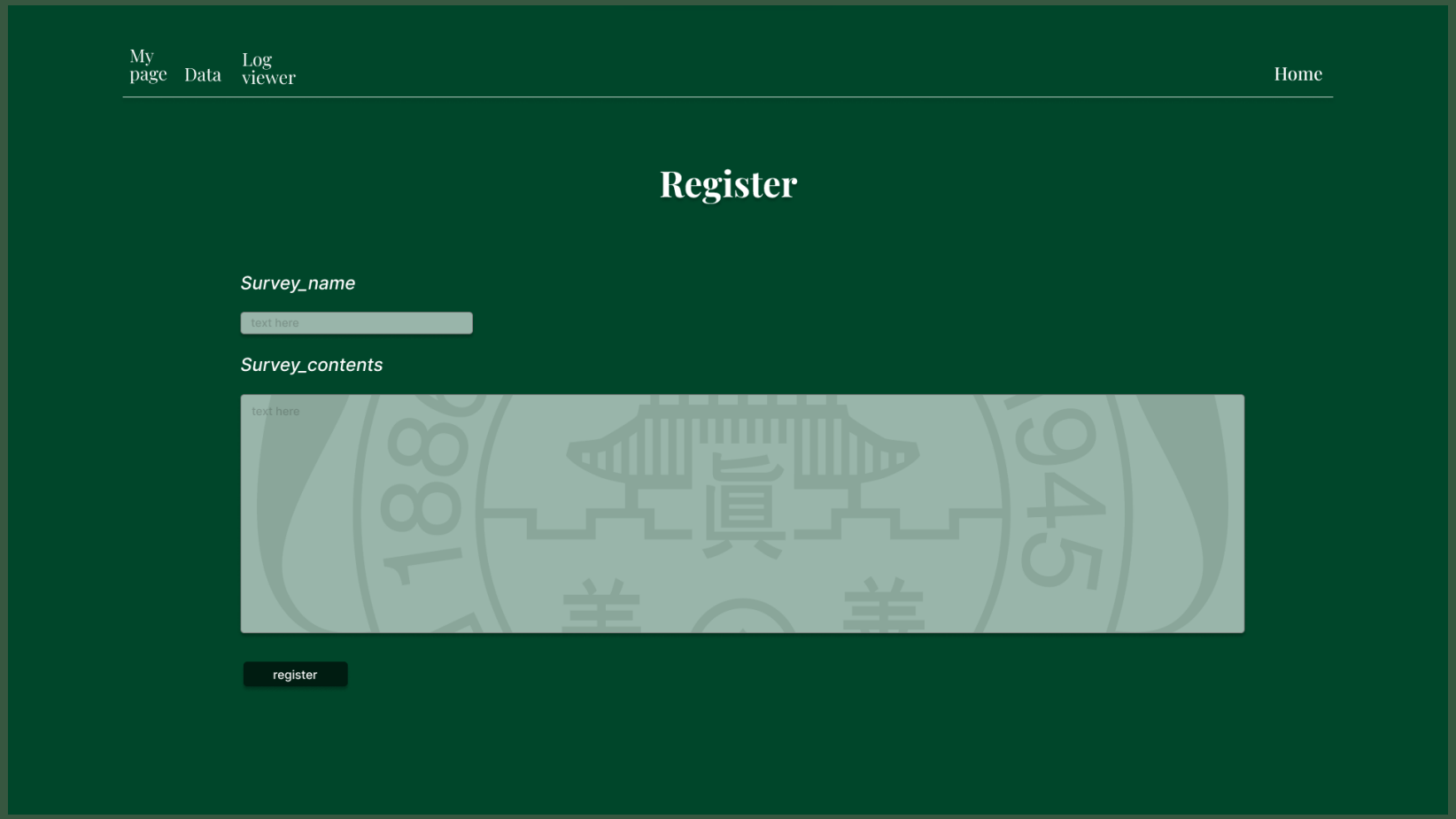
사용자 로그인

Secure Hub



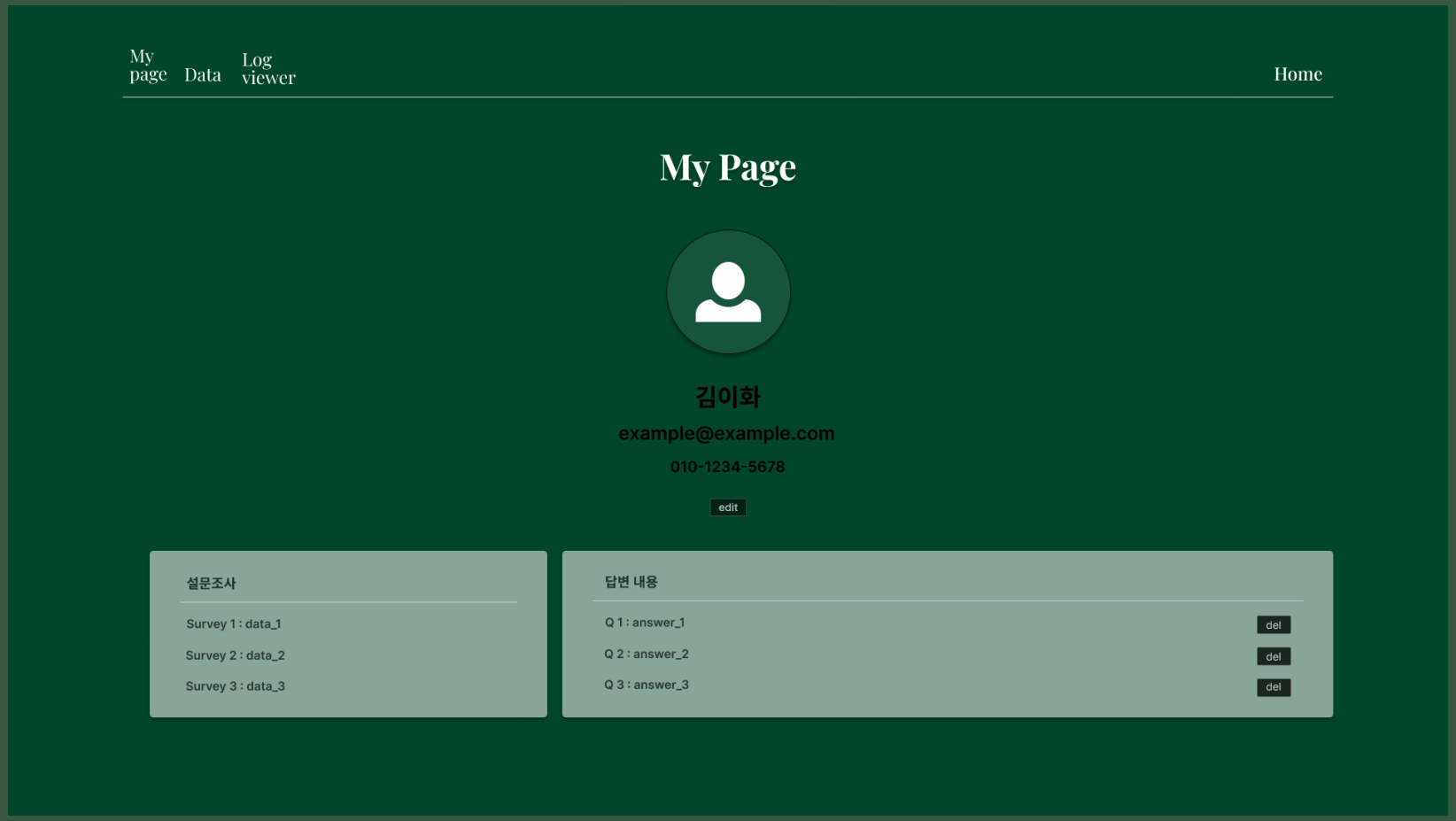
필요한 설문을 찾거나 나의 설문을 등록 가능

Secure Hub



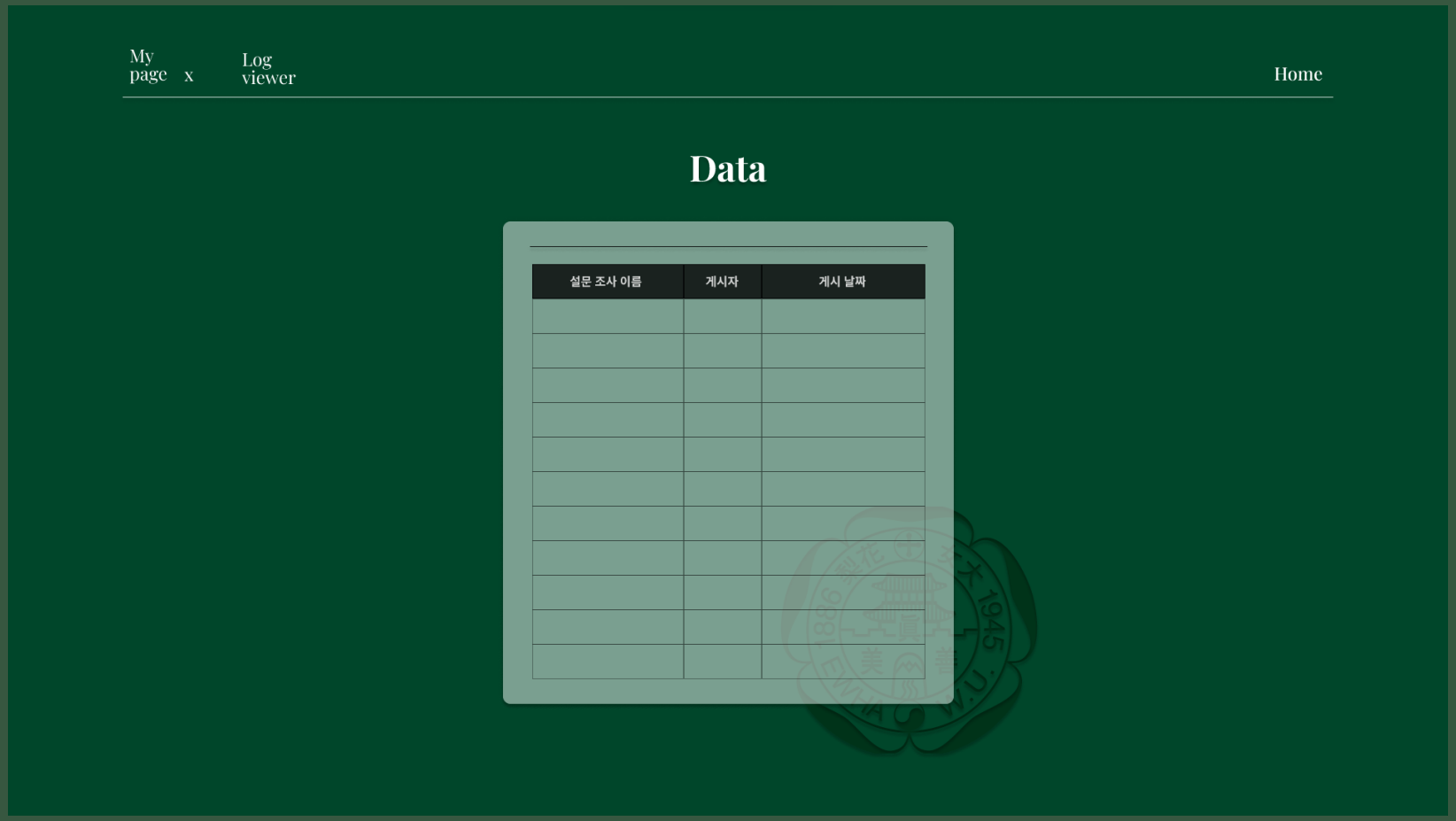
자유롭게 설문 등록 가능

Secure Hub



마이페이지에서 본인이 작성한 설문에 대한 답변과
본인이 응답한 설문(암호화된 형태) 확인 가능

Secure Hub



암호화된 답변들은 설문 기간 종류 후 설문 작성자와 응답자의 상호 동의 후 복호화 되어 제공

설문 작성자에게 채택되지 않았거나 동의를 받지 못한 정보들은 암호화된 상태에서 폐기

사용한 암호화 알고리즘

AES 암호화 알고리즘

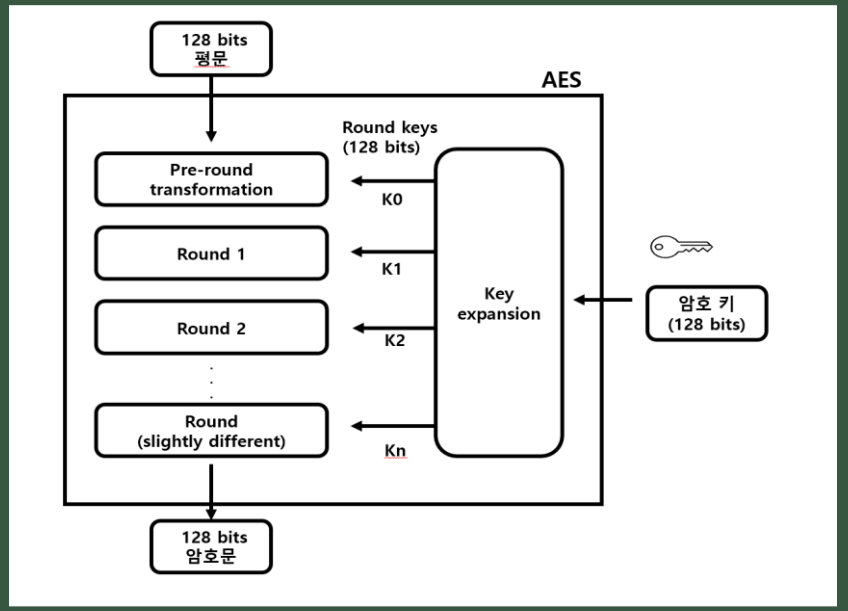
: 암호화 복호화 과정에서 동일한 키를 사용하는 대칭 키 알고리즘

선택 이유 :

대량의 데이터를 빠른 속도로 암호화 , 복호화 가능

무차별 대입 공격에 강함

미국 국가안보국 1급비밀에 승인된 알고리즘



```python
@app.route('/encrypt', methods=['POST'])
def encrypt():
    data = request.form['data'].encode('utf-8')
    cipher = AES.new(key, AES.MODE_CBC)
    ct_bytes = cipher.encrypt(pad(data, AES.block_size))
    iv = base64.b64encode(cipher.iv).decode('utf-8')
    ct = base64.b64encode(ct_bytes).decode('utf-8')

    # Save encrypted data and IV to the database
    c.execute("INSERT INTO users (username, encrypted_data, iv) VALUES (?, ?, ?)", ('user', ct, iv))
    conn.commit()

    return render_template('encrypted.html', iv=iv, ct=ct)
```

```python
@app.route('/encrypt', methods=['POST'])
def encrypt():
    data = request.form['data'].encode('utf-8')
    cipher = AES.new(key, AES.MODE_CBC)
    ct_bytes = cipher.encrypt(pad(data, AES.block_size))
    iv = base64.b64encode(cipher.iv).decode('utf-8')
    ct = base64.b64encode(ct_bytes).decode('utf-8')

    # Save encrypted data and IV to the database
    c.execute("INSERT INTO users (username, encrypted_data, iv) VALUES (?, ?, ?)", ('user', ct, iv))
    conn.commit()

    return render_template('encrypted.html', iv=iv, ct=ct)
```

AES 대칭키 암호화 방식으로 암호화 객체 생성

'key'는 미리 정의된 암호화 키 사용

암호화 객체 사용
데이터를 AES 블록크기에 맞춰 패딩 후 암호화

암호화된 템플릿을 렌더링 하여 사용자에게 보여줌

이름 암호화

- IV: mV6VqH65jkytT4fPTD9kqQ==
- CT: 1GBirzgAogKA0ltlqeJOpg==

김이화

주소 암호화

- IV: 0mdss14FD7rcXpwJlftw/w==
- CT: jirN7Ekz6NGlXm8xZapLwl4aEqz/v982L1sRf+6SHgg=

서울시 서대문구

전화번호 암호화 (학번, 주민등록번호도 가능)

- IV: j+uwuQyciXiqXMf4RQwS8A==,
- CT: SQ61/HX4QTjRe3TZfsTZhA

010-1234-5678

복호화

```python
@app.route('/decrypt', methods=['POST'])
def decrypt():
    user_id = request.form['user_id']
    c.execute("SELECT * FROM users WHERE id=?", (user_id,))
    user_data = c.fetchone()
    if user_data:
        iv = base64.b64decode(user_data[3])
        ct = base64.b64decode(user_data[2])
        cipher = AES.new(key, AES.MODE_CBC, iv)
        pt = unpad(cipher.decrypt(ct), AES.block_size).decode('utf-8')
        return render_template('decrypted.html', pt=pt)
    else:
        return 'User not found'
```

IV를 사용하여 AES암호화 객체 생성

암호화된 데이터 디코딩하여 바이너리 형태로 변환하여 ct에 저장

데이터 복호화 후 패딩 제거
UTF-8형식으로 디코딩하여 pt에 저장

복호화된 템플릿을 렌더링 하여 사용자에게 보여줌

Secure Hub 추가 기능 구상

채팅 기능 추가

화면 캡쳐 감지 기술

Secure Hub의 비전

개인 정보 보호
익명성 보장

참여도 상승
설설문문 다양성 기대
직접적인 피드백 가능
양질의 의견 취합가능

감사합니다