

LLM에 로그인했더니 내 계정이 아니게 됐다???



| whoami



남현석



| me@imnya.ng

Information security

- 2026 ~ 선린인터넷고등학교 정보보안 동아리 Layer7 26기
- 2026 ~ 선린인터넷고등학교 정보보호과
- 2025 - 화이트햇스쿨 3기 이수
- 2025 - 2024 Sunrin Layer7 CTF 중등부 2위
- 2024 - 29회 해킹캠프 CTF 1위 (고민중독)

Software engineering

- 2025 - ADOFAI.gg Full Stack, Mod Developer
- 2026 - Effect Playing Contest 2025 : Finale



| LLM은 내 계정을 어떻게 접근할까?

우리가 계정을 접근하는 방법은 무엇이 있을까요?



| LLM은 내 계정을 어떻게 접근할까?

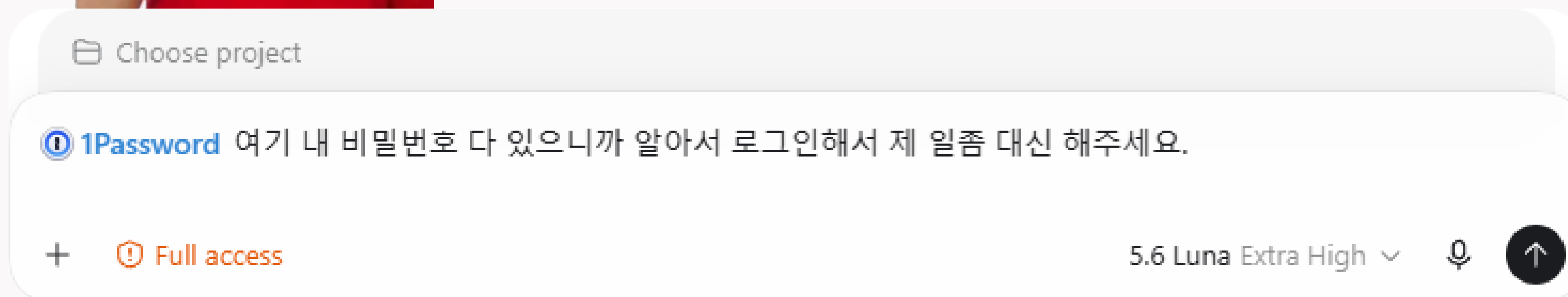
우리는 주로 사용자 이름, 비밀번호를 입력해서 토큰이나 세션을 받는 방식으로 접근해요.



| LLM은 내 계정을 어떻게 접근할까?

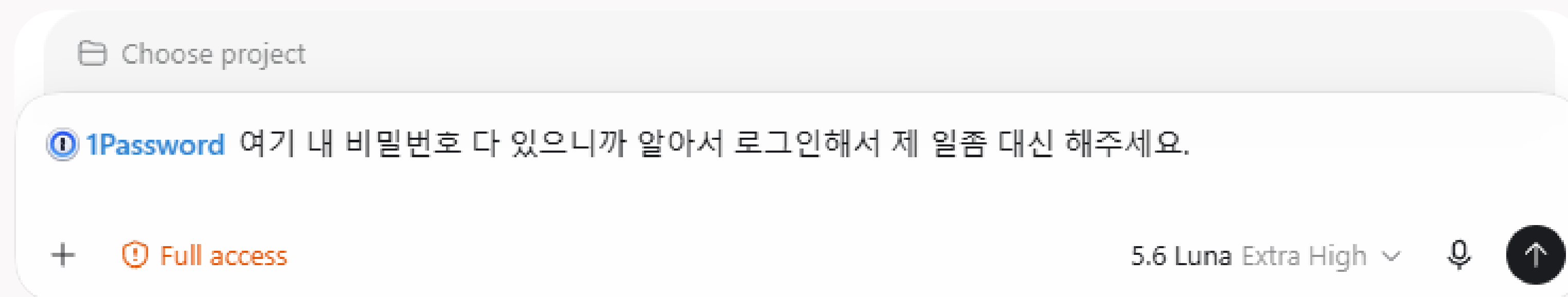


그럼 LLM한테 내 비밀번호를 주면 되겠구나!



| LLM은 내 계정을 어떻게 접근할까?

~~그럼 LLM한테 내 비밀번호를 주면 되겠구나!~~



| LLM은 내 계정을 어떻게 접근할까?

왜 내 비밀번호를 그냥 주는 방식을 쓰지 않을까?



| LLM은 내 계정을 어떻게 접근할까?

일단 권한이 너무 광범위적이고 관리가 어렵다



| LLM은 내 계정을 어떻게 접근할까?

그럼 어떤 다른 방법이 있을까?



| LLM은 내 계정을 어떻게 접근할까?

OAuth
API Key
Personal Access Token
...



| LLM은 내 계정을 어떻게 접근할까?

OAuth
API Key
Personal Access Token
...



| LLM은 내 계정을 어떻게 접근할까?

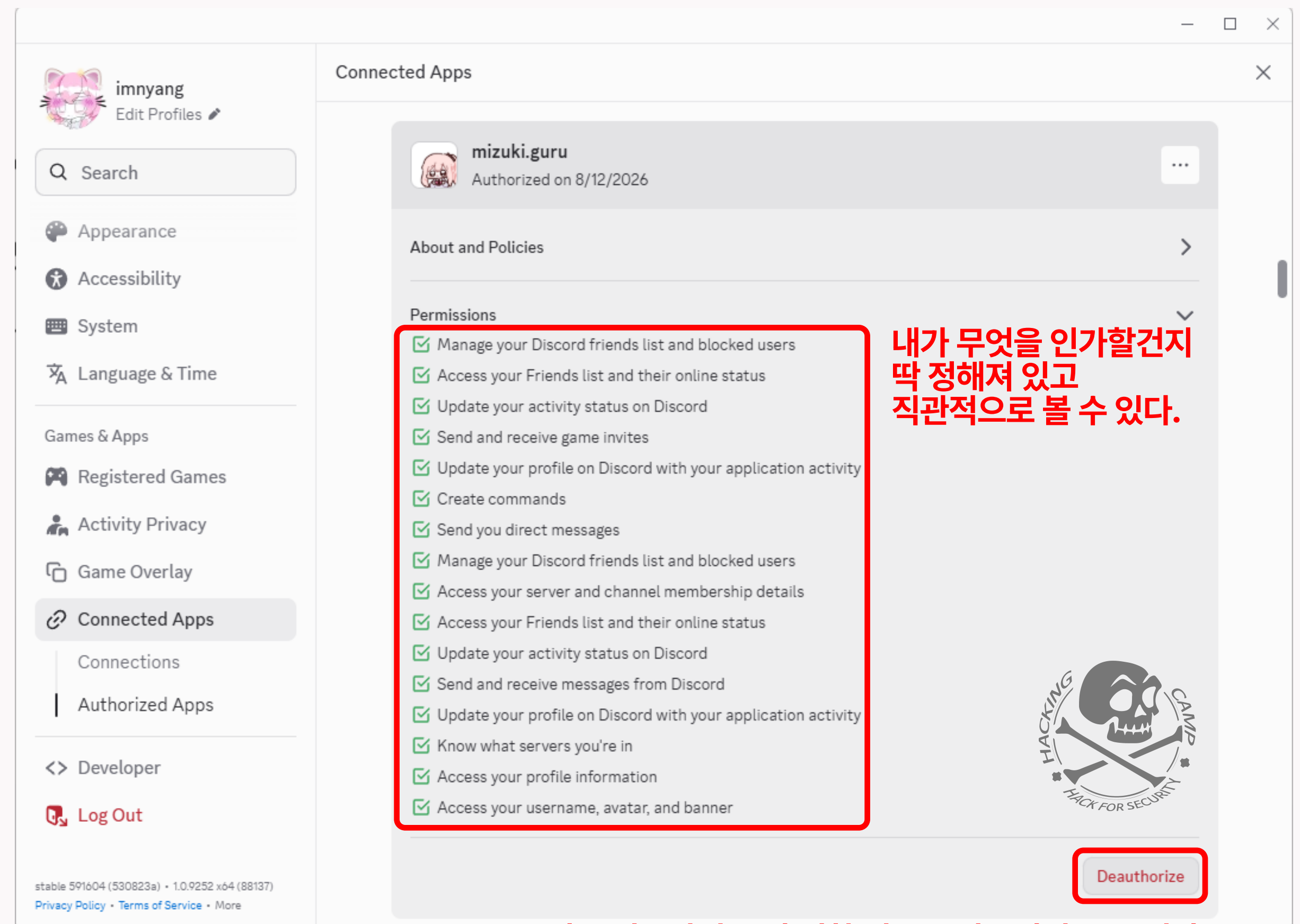
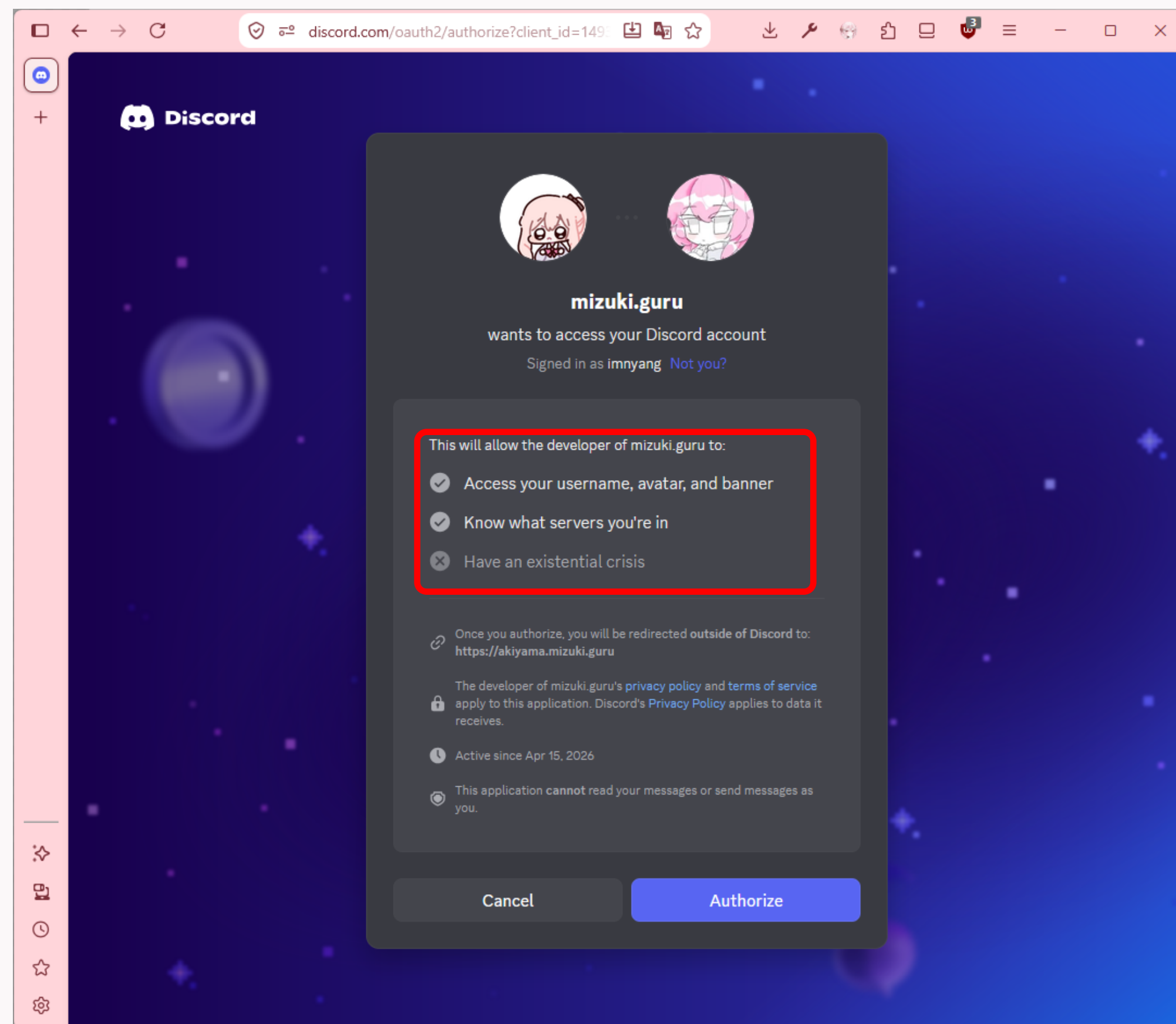
근데 왜 OAuth일까?



| LLM은 내 계정을 어떻게 접근할까?

근데 왜 OAuth일까?

권한 관리가 다른 것에 비해 압도적으로 쉬움



그리고 필요하면 즉시 권한 접근을 만료시킬 수도 있다.

| LLM은 내 계정을 어떻게 접근할까?

근데 왜 OAuth일까?

권한 관리가 다른 것에 비해 압도적으로 쉬움
만약 API Key를 쓴다면?

dash.cloudflare.com/profile/api-tokens

Support

My Profile

Quick search... Ctrl K

Settings

Access Management

API Tokens

← Back to view all tokens

Create Custom Token

Token name

Give your API token a descriptive name.

Permissions

Select edit or read permissions to apply to your accounts or websites for this token.

Account Access: Apps and Policies Select...

Account Select Select...

+ Add more

Account Resources

Select accounts to include

Include

+ Add more

Access: Apps

Access: Apps and Policies

Access: Audit Logs

Access: Custom Pages

Access: Device Posture

Access: Groups

Client IP Address Filtering

Select IP addresses or ranges of IP addresses to filter. This filter limits the client IP addresses that can use the API token with Cloudflare. By default, this token will apply to all addresses.

Operator Value

Select e.g. 192.168.1.88 Use my IP

+ Add more



| LLM은 내 계정을 어떻게 접근할까?

근데 왜 OAuth일까?

권한 관리가 다른 것에 비해 압도적으로 쉬움
만약 API Key를 쓴다면?

보통 서비스들의 권한이 정말로 많이 있다...
사용자가 권한을 혼동해서
필요 이상으로 권한을 줄 수도 있어요.

그리고 개발자한테 편할 수도 있어도
일반 사용자한테 좀...

The screenshot shows the Cloudflare dashboard interface for creating a custom API token. The left sidebar contains navigation links for 'My Profile', 'Settings', 'Access Management', and 'API Tokens'. The main content area is titled 'Create Custom Token' and includes a 'Token name' field, a 'Permissions' section with a dropdown menu open showing various access options, and a 'Client IP Address Filtering' section with a table for adding IP addresses.

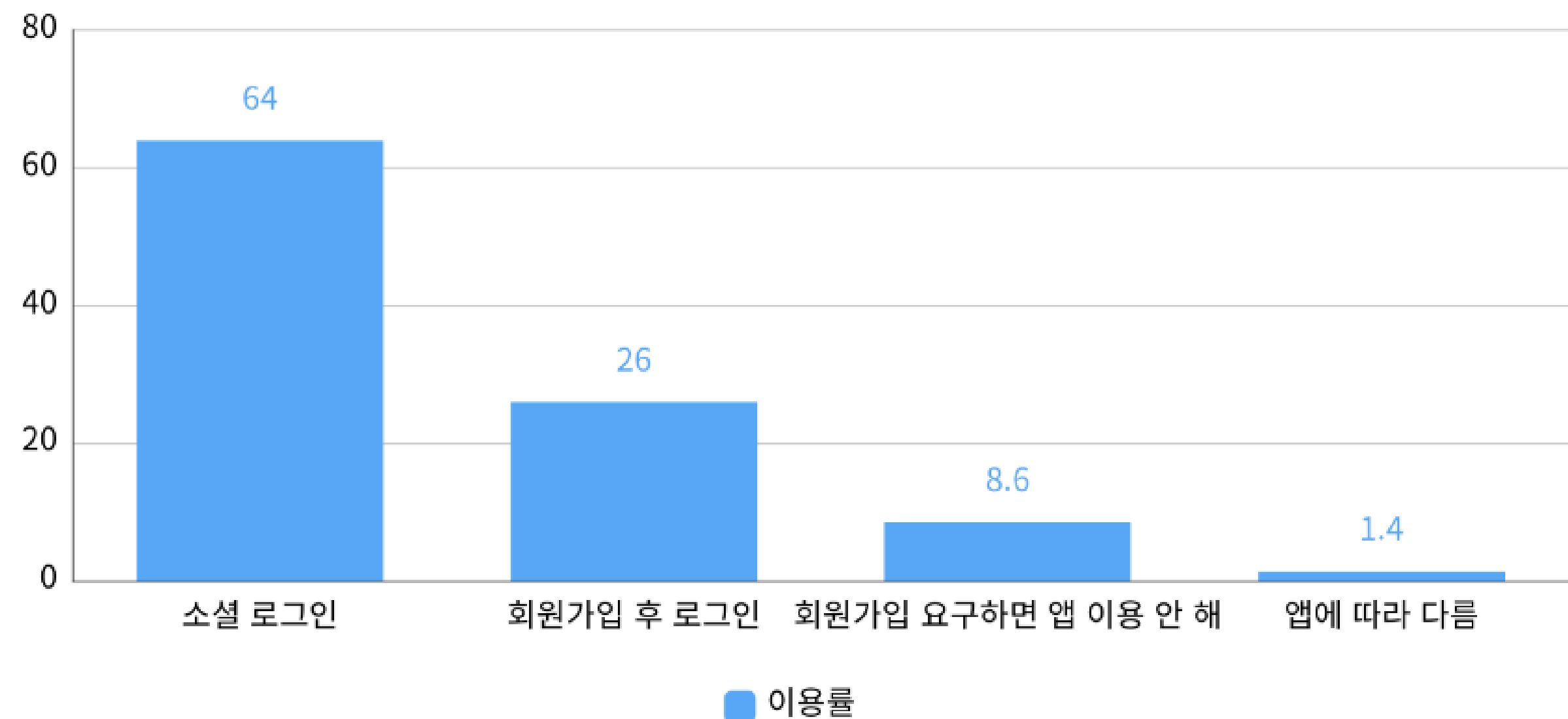
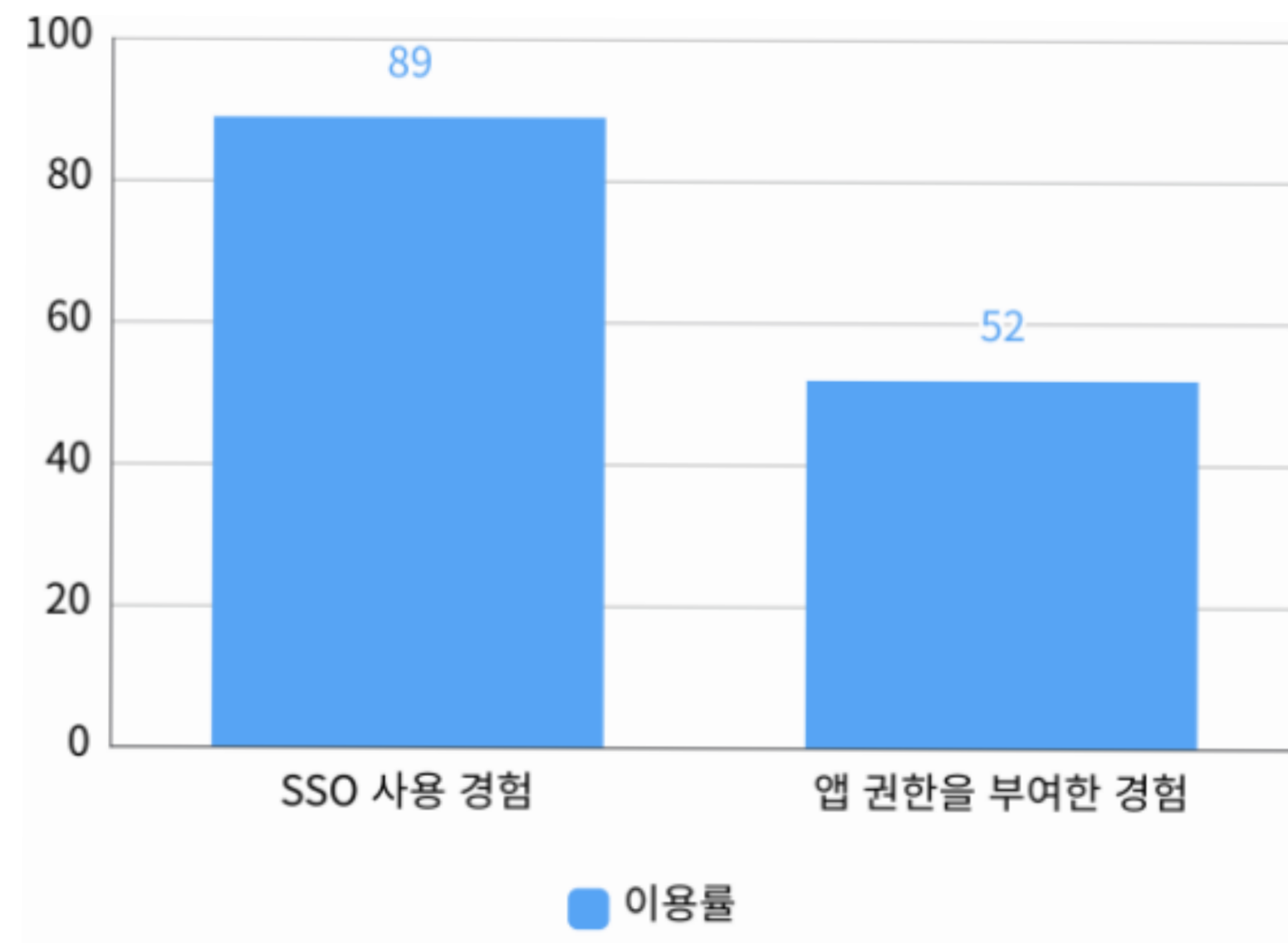


| OAuth란?

여러분은 OAuth를 써 보신 적이 있나요?



| OAuth란?



한국 소비자 연맹(2020), 소셜 로그인 인식도 조사,
[arxiv abs/2111.03573](https://arxiv.org/abs/2111.03573) Security and Privacy Perceptions of Third-Party Application Access for Google Accounts (Extended Version)



| OAuth란?

Sign up

Email

Auth0 may contact me with marketing communications
opt-out details in [Privacy Policy](#).

☐ I agree

By continuing, you agree to the [Self Service PSS](#) and
[Privacy Policy](#).

Continue

OR

 Continue with GitHub

 Continue with Google

 Continue with Microsoft

Google 로그인 = 보통 OAuth 2.0 + OpenID Connect



| OAuth란?

Sign up

Email

Auth0 may contact me with marketing communications
opt-out details in [Privacy Policy](#).

☐ I agree

By continuing, you agree to the [Self Service PSS](#) and
[Privacy Policy](#).

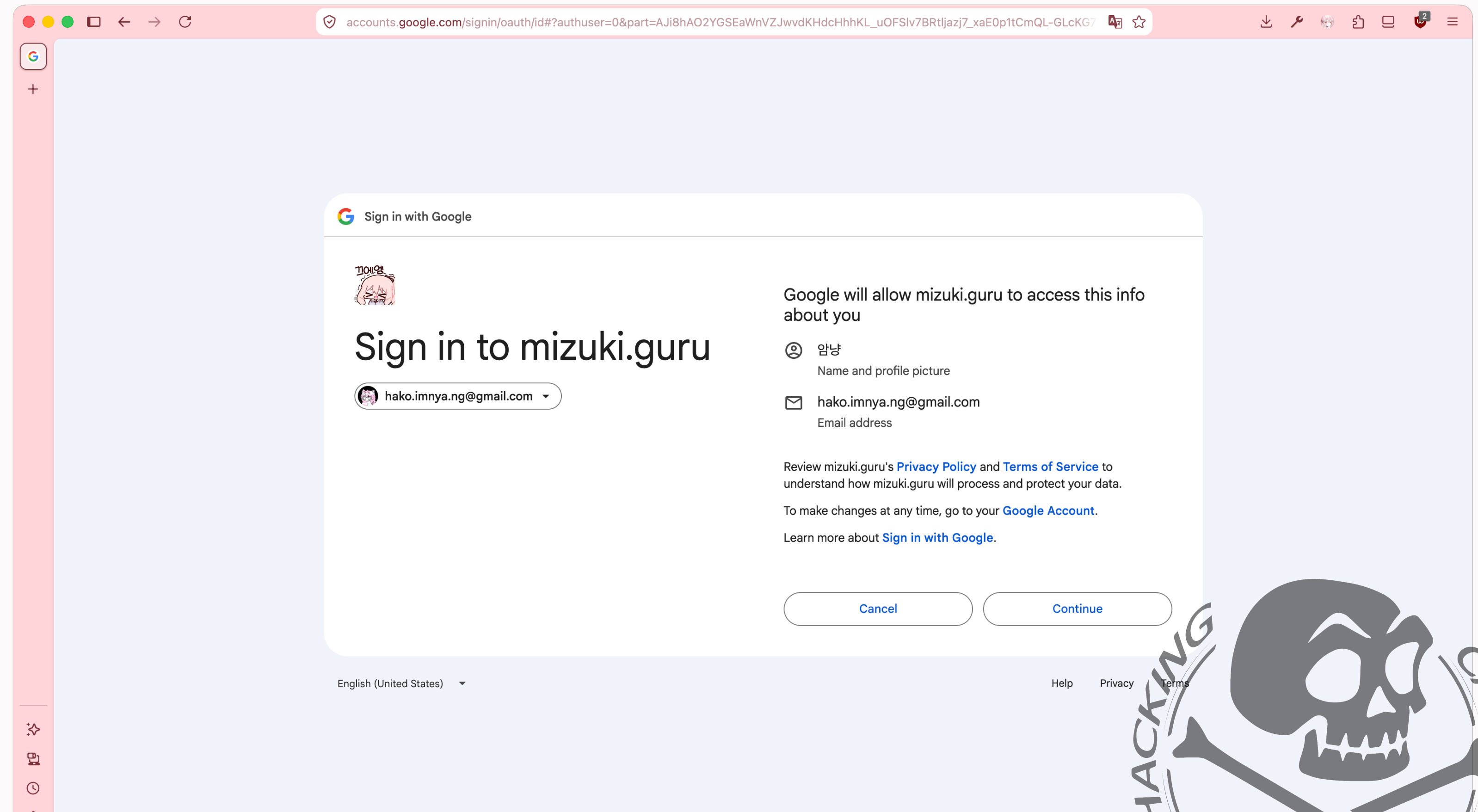
Continue

OR

 Continue with GitHub

 Continue with Google

 Continue with Microsoft



비밀번호는 Google에만 입력 · 앱은 code/token을 받음



| OAuth란?

OAuth는 처음부터 제3자 앱에
제한된 API 접근 권한을 위임하기 위해 설계됨



| OAuth란?

OpenID Connect가 OAuth 위에 인증 계층을 더해 소셜 로그인을 표준화했고,
LLM Agent는 OAuth의 원래 목적인 API 권한 위임을 적극적으로 사용

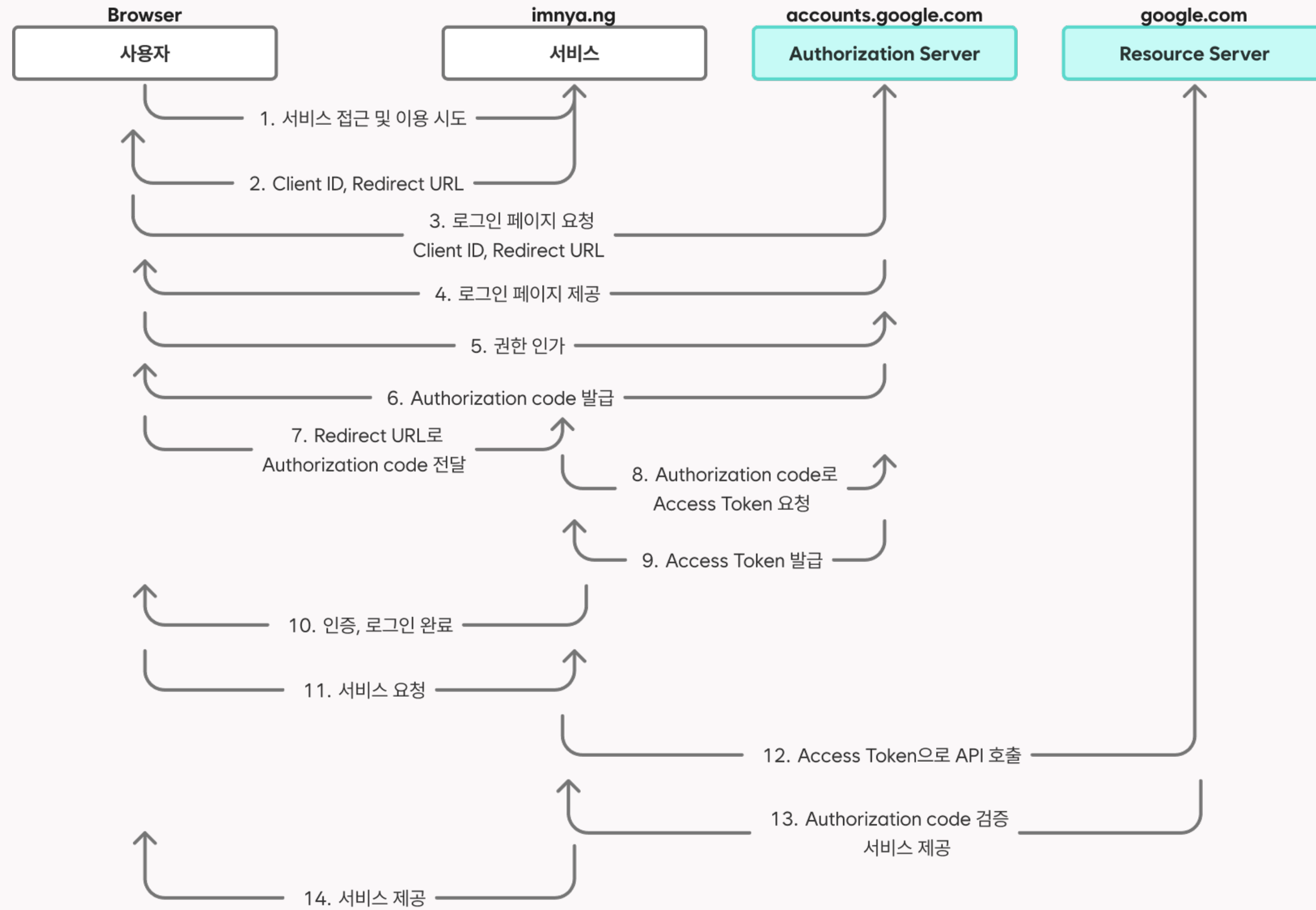


| OAuth란?

Agent의 자동화 속도와 권한 범위가 커져
OAuth 구현의 정확성이 더욱 중요해짐



| OAuth란?



| OAuth란?

1. OAuth는 지켜야 할 값이 많다



| OAuth란?

1. OAuth는 지켜야 할 값이 많다
- 2. 복잡성은 구현 실수의 가능성을 높인다**



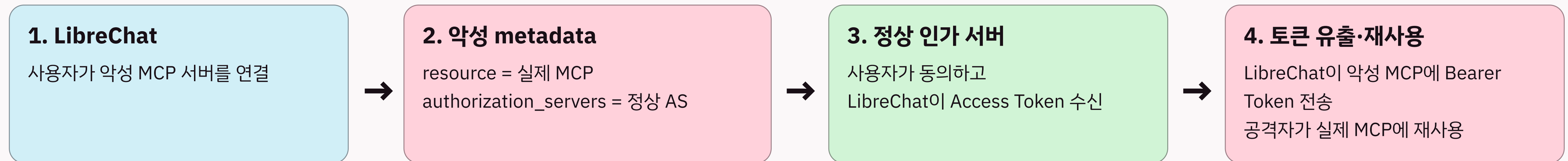
| OAuth란?

1. OAuth는 지켜야 할 값이 많다
2. 복잡성은 구현 실수의 가능성을 높인다
- 3. 구현에서의 실수는 취약점으로 이어질 수도 있다**



| LibreChat: CVE-2026-54030

토큰이 이동하는 실제 경로



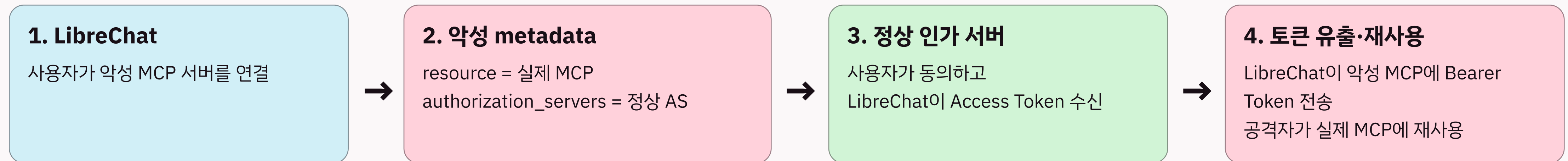
metadata.resource <https://real.mcp.mizuki.guru>
authorization_servers <https://auth.mizuki.guru>

토큰은 인가 서버에서 악성 MCP로 직접 전달되지 않는다.



| LibreChat: CVE-2026-54030

토큰이 이동하는 실제 경로



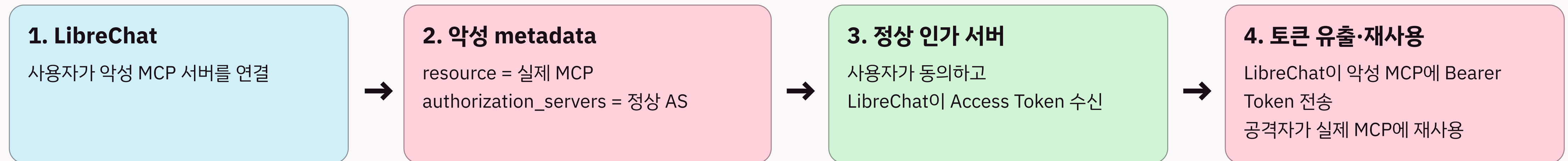
metadata.resource <https://real.mcp.mizuki.guru>
authorization_servers <https://auth.mizuki.guru>

연결한 MCP URL과 metadata.resource가 정확히 일치해야 한다.



| LibreChat: CVE-2026-54030

토큰이 이동하는 실제 경로



metadata.resource <https://real.mcp.mizuki.guru>
authorization_servers <https://auth.mizuki.guru>

불일치하면 metadata만 버리는 것이 아니라 OAuth 흐름 전체를 중단

GHSA-gvpj-vm2f-2m23 · LibreChat < 0.8.5 · fixed in 0.8.5 · High 8.0



Access Token이 비밀번호보다 피해 범위를 제한하기 쉬운 이유는?

1. 토큰은 절대 탈취될 수 없기 때문에
2. scope·만료·폐기로 피해 범위를 제한할 수 있기 때문에
3. 토큰은 자동으로 암호화되어 저장되기 때문에



Access Token이 비밀번호보다 피해 범위를 제한하기 쉬운 이유는?

1. 토큰은 절대 탈취될 수 없기 때문에
2. scope·만료·폐기로 피해 범위를 제한할 수 있기 때문에
3. 토큰은 자동으로 암호화되어 저장되기 때문에



| Whitehat School 3rd

이 발표 주제를 정한 가장 큰 이유 중 하나
WhiteHat School 3기

기초 이론 교육 → 팀 프로젝트 → 선택형 심화 교육

이 발표에서는 Safe Us 팀의 현대 인증·인가 프로젝트를 소개



| Whitehat School 3rd

‘현대 인증/인가 깊이 파기’를 주제로 Safe Us 팀 프로젝트 진행
허가된 버그바운티 범위와 로컬 Lab에서만 분석



| Whitehat School 3rd

그래서 프로젝트로는 무엇을 했는가?



| Whitehat School 3rd

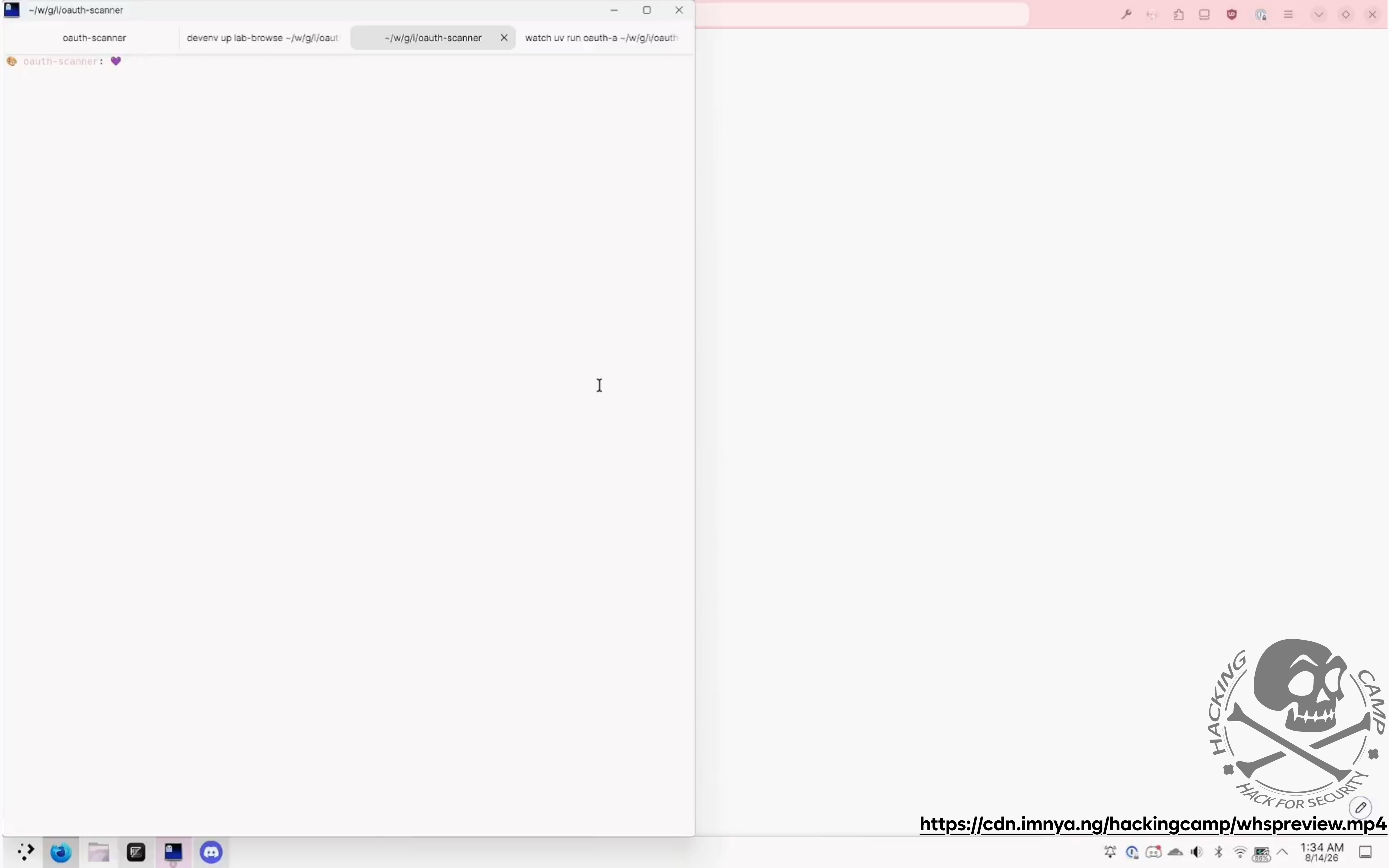
기존 방식

- 수동 로그인과 반복적인 캡처
- 기능 추가 때마다 코드 수정
- 분석가가 전체 흐름을 수행

프로젝트 방식

- 브라우저 탐색과 네트워크 기록 자동화
- 규칙 탐지와 LLM 후속 검토 분리
- 결과는 사람이 재현·검증





| Whitehat School 3rd

허용된 범위 · 정적 탐지 · 비결정적 후속 검토를 분리

1. 수집·탐색

HackerOne에 있던 버그바운티 도메인
자동화 도구를 통해 HackerOne에 있던 것을 추출



Chromium + browser-use
로그인·OAuth 화면 탐색



mitmproxy addon
HTTP(S) 요청·응답 기록

2. 검출·저장

Passive detectors
state · redirect · issuer · resource 검사



CSV Storage
사람이 읽기 쉬운 형태로 정리

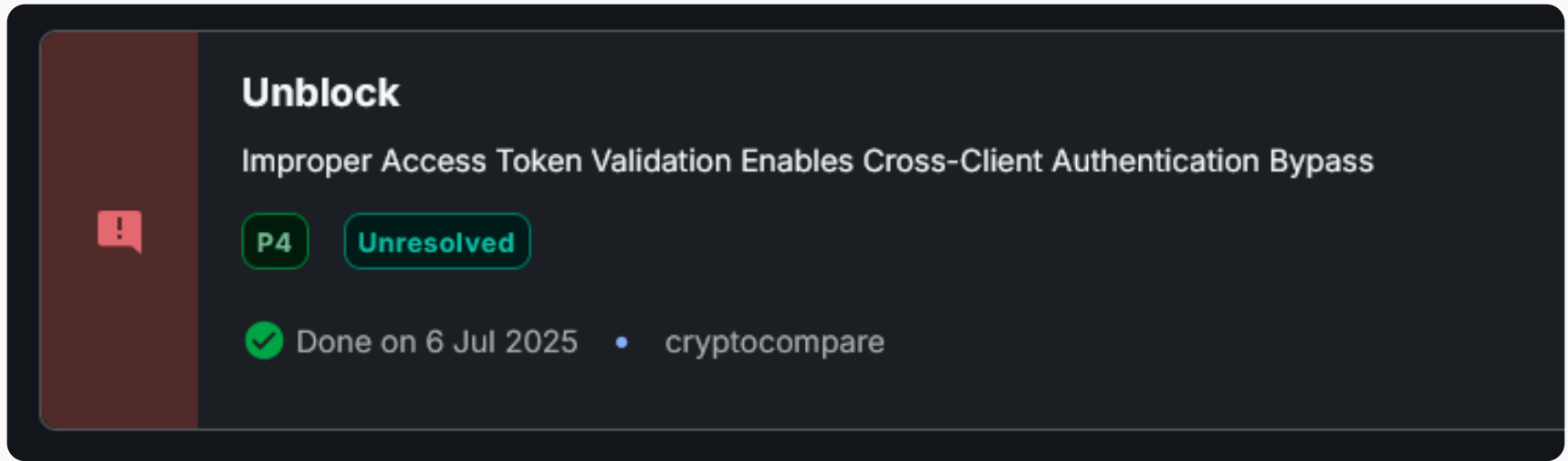


직접 검토
사람이 직접적으로 검토하여 정리



| Whitehat School 3rd

WhiteHat School 프로젝트 결과



국내 OAuth 제공자 관련 보안 이슈 신고 →

← 버그바운티 프로그램을 운영하는 서비스에서
OAuth Client 검증 누락 후보를 신고·검증

N 버그바운티

더 보기 ▾

Issues

Rewards

취약점 제보

safe-us ▾

명예의 전당

🔍 검색

2025 ▾

번호	닉네임	웹사이트
1		
2		
3		
4	safe-us	웹사이트 방문



| Whitehat School 3rd

프로젝트에서 어려웠던 점

1. 이땐 LLM이 그렇게 똑똑하지 않았다

gemini-2.5-flash 나왔을 때의 시절

프롬프트에 진짜 모든 과정을 적어도 그 그대로 하지 않고 LLM이라 작동 방식의 디버깅도 어려움

LLM이기에 결과가 항상 같다고 보장할 수 없음



| Whitehat School 3rd

프로젝트에서 어려웠던 점

2. 썼던 라이브러리의 미성숙성

2025년 2분기만 해도 LLM이라는게 이제 막 발전할 시기였었다고 생각
그렇기 때문에 이런 LLM으로 자동화해서 브라우징하는 도구가 생소했던 시기

이런 기능 하는 도구 찾으려고 직접 검색도 많이 해보고
여기서 문서화가 이땐 잘 안되어 있었어서 직접 개발자랑 컨택도 해보고 많이 찾아봤던 시기...
지금은 Browser Use 문서가 진짜 굉장히 잘되어 있어서
여러분들도 웹 자동화가 필요하면 써보시는 걸 추천합니다.



| Whitehat School 3rd

만약 지금 한다면?

1. 지금의 LLM은...

OpenAI의 가장 저렴한 모델인 GPT-5.6 Luna만해도 속도도 준수하고 정확도도 굉장히 높아진 느낌이 들었음



| Whitehat School 3rd

만약 지금 한다면?

2. 지금 Browser Use 라이브러리

지금은 프로젝트가 안정화되고 Cloud라는 상업화 모델까지 나와서 문서화가 굉장히 잘된 편임
만약 다른 웹 관련 자동화 프로젝트를 한다면 다음에도 쓰는 걸 고려해보고 싶을 정도...



감사합니다

 | [@imnyang](https://discord.com/invite/imnyang)
 | [@imnya.ng](https://www.instagram.com/imnya.ng)
 | [@imnya_ng](https://twitter.com/imnya_ng)
 | imnya.ng
 | me@imnya.ng

