해커들이 좋아하는 인증 환경은 따로 있다?

WHS 3기 Safe Us 팀

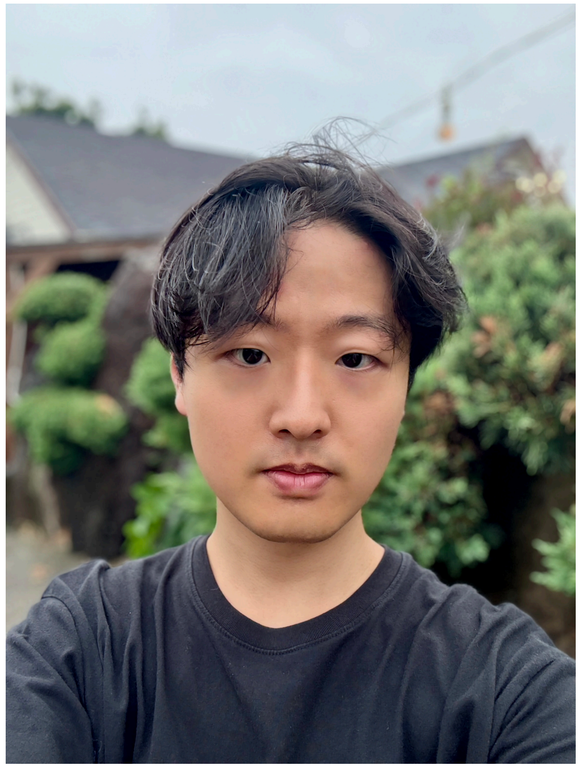
김민곤, 정민석, 길태균, 남현석, 오수진, 이규현, 정승연

팀원 소개

김민곤, 정민석, 길태균, 남현석, 오수진, 이규현, 정승연

발표자 소개

- 이름: 정민석
- 전공: 국어국문학, 철학
- 관심사
  - Security Engineering
  - FE, BE Engineering
  - Imbeded SW (모터 제어)
  - Philosophy (인식론, 관념론, 형이상학)
- 수상 이력
  - 창의적 종합설계 경진대회 - 산업통상자원부 장관상
  - 로봇 융합 페스티벌 지능형 창작로봇 경진대회 - 대전시장상



Blog: https://j93.es

LinkedIn: https://www.linkedin.com/in/j93es

발표자 소개

- 이름: 김민곤
- 전공: 컴퓨터소프트웨어공학과
- 관심사
  - Web Hacking
  - 모의해킹

OAuth 관련 보안 위협을 조기에 발견하여

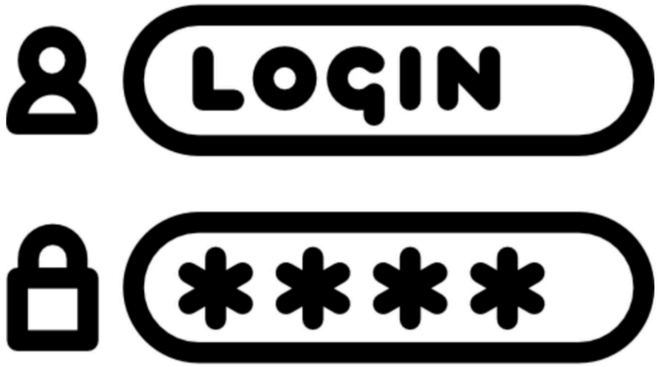
안전한 인증/인가 환경에 기여

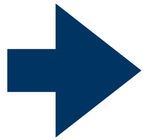
인증/인가란?

내가 '나'임을 증명하고

나의 권한을 부여하는 것

인증/인가의 발전 과정



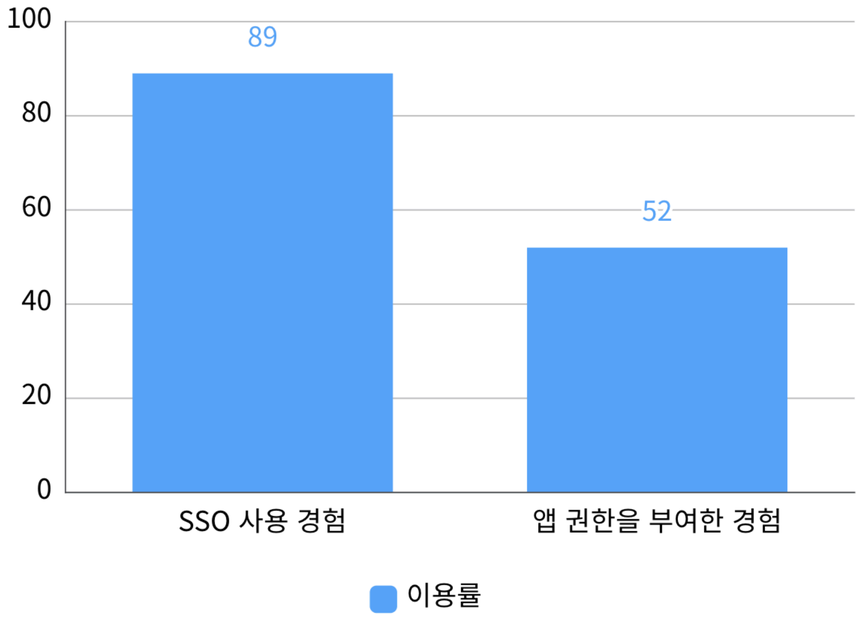


ID, PW 기반 로그인

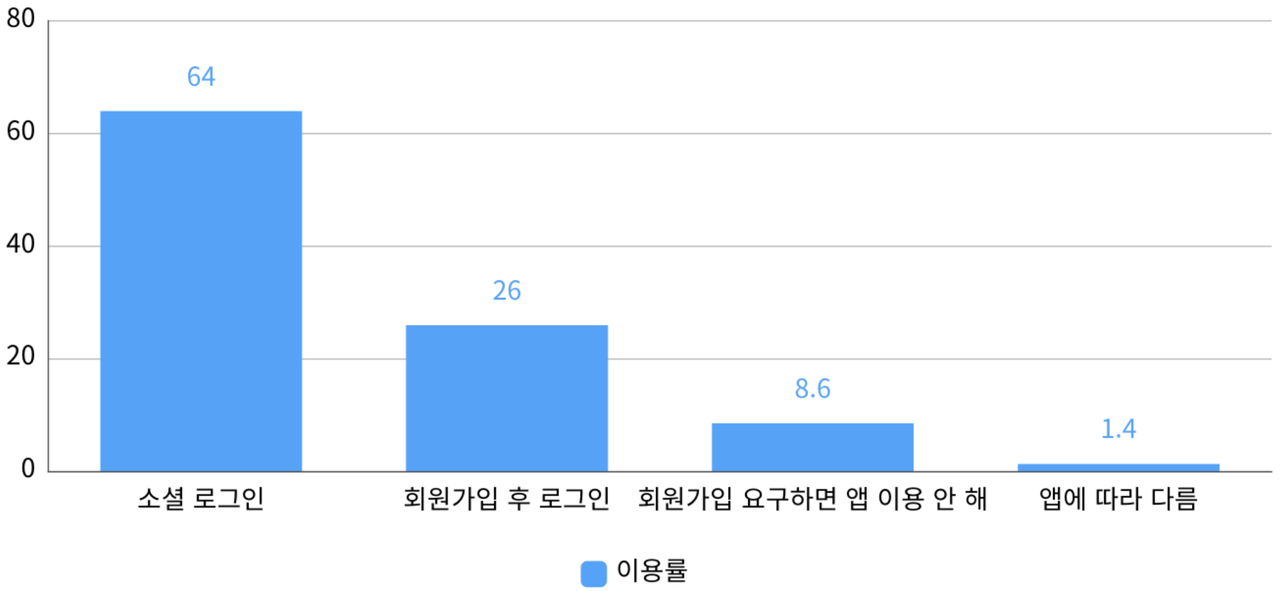
OAuth 기반 SSO 로그인

OAuth 기반 소셜 로그인의 현위치

구글 사용자 대상 SSO 이용률



소셜 로그인과 직접 회원가입 중 주로 사용하는 로그인 방법



D. G. Balash, X. Wu, M. Grant, I. Reyes, and A. J. Aviv, “Security and privacy perceptions of third-party application access for Google accounts (Extended Version),” *CoRR*, vol. abs/2111.03573, 2021.

한국 소비자 연맹(2020), 소셜 로그인 인식도 조사

OAuth의 장점

01

확장성 용이

OIDC 등과 함께 사용 가능

-> 다른 프로토콜을 통한 확장 용이

02

유연한 서비스 통합

Google, Naver 등 다양한 플랫폼과 연동 가능

-> 다양한 플랫폼과의 연동

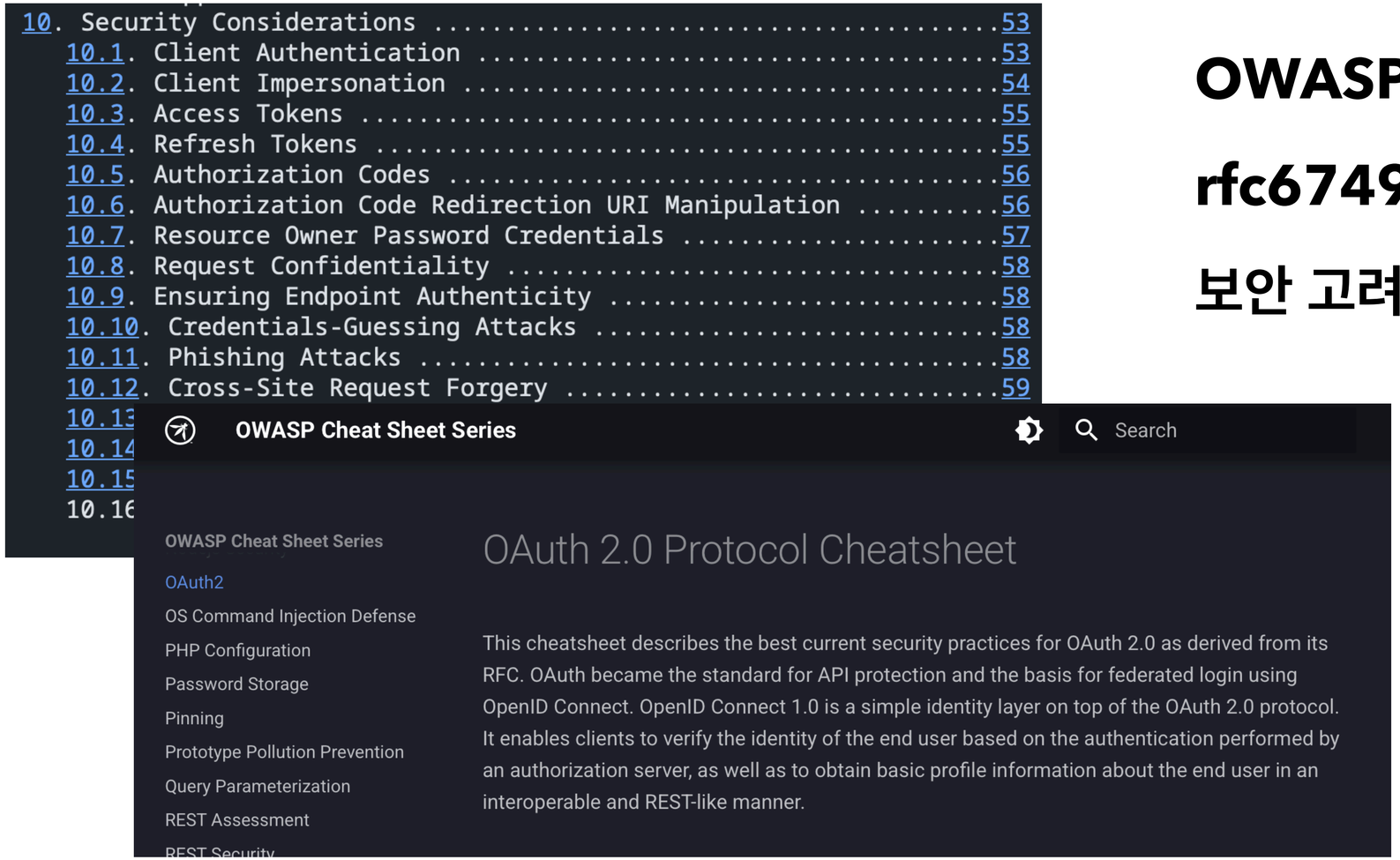
03

사용자 인증 정보 보호

어플리케이션이 사용자의 ID, PW를
직접 다루지 않음

-> 보안 위협을 최소화

OAuth 보안 고려사항

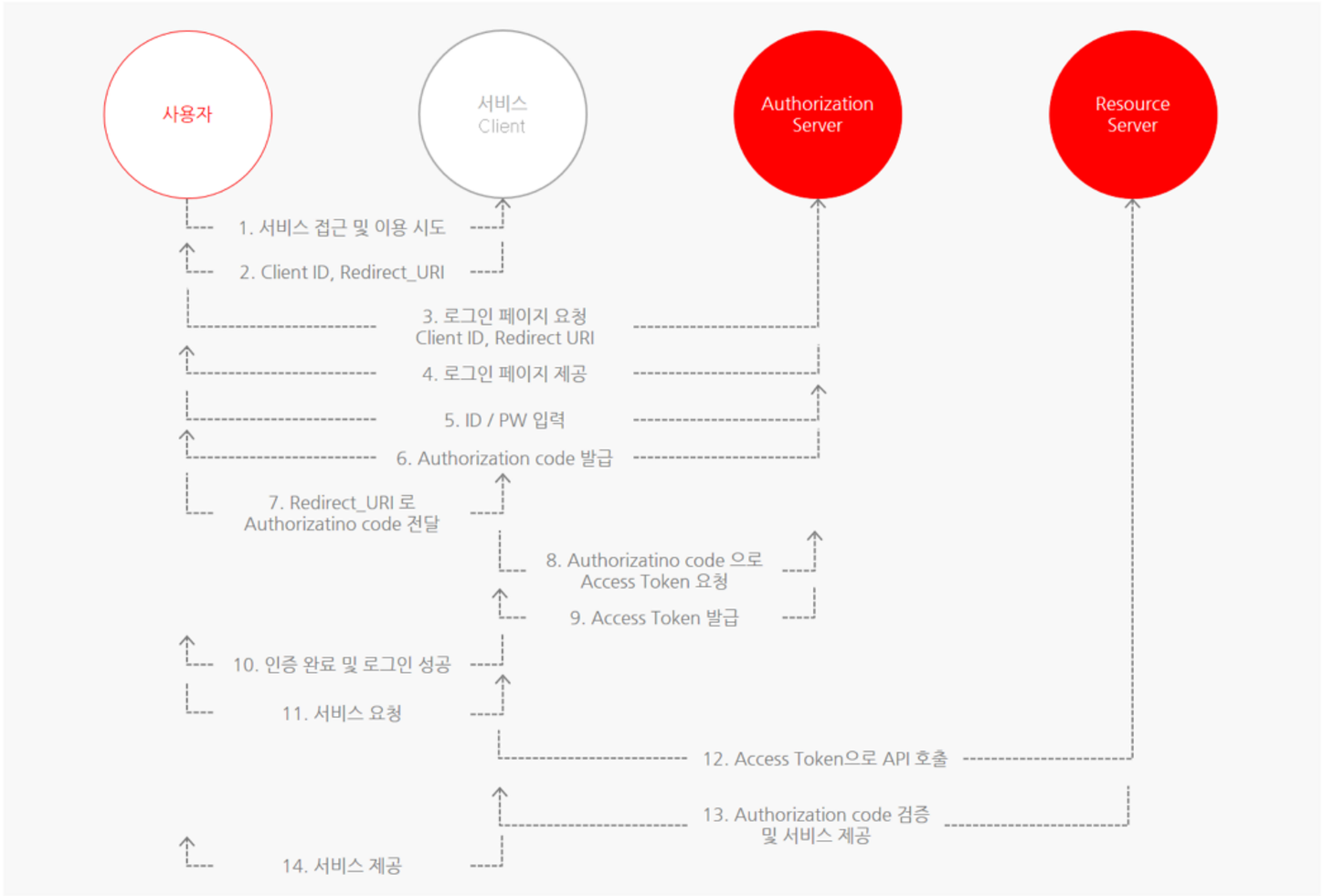


OWASP Cheatsheet,

rfc6749 등의 공식 문서를 통하여

보안 고려사항을 학습

OAuth의 복잡성



OAuth의 복잡성은

개발과정에서의 실수로 인한

보안 위협을 초래할 수 있습니다.

복잡한 문제를 간결하게 생각할 수는 없는가?

복잡한 문제를 깊이 파고

이를 다른 시각에서 간결하게 바라보자

OAuth의 구조

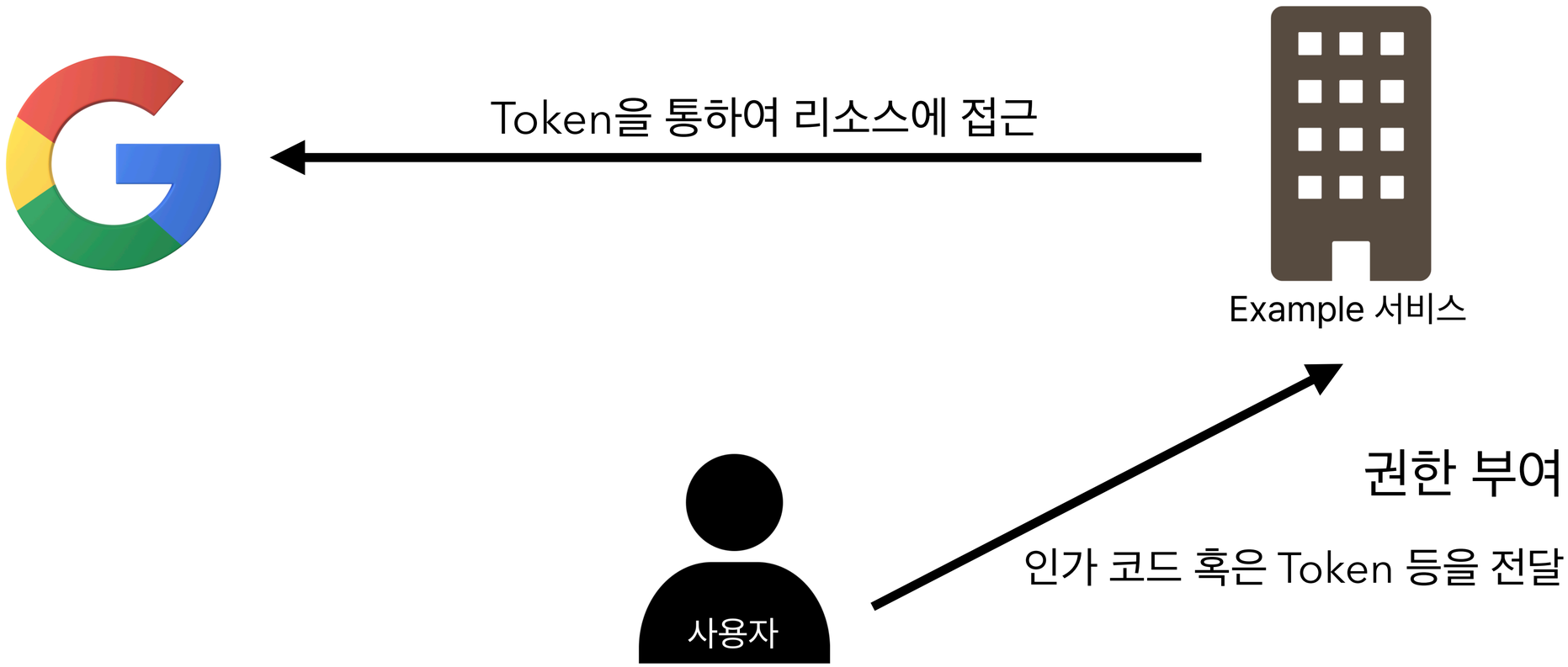
OAuth 흐름

Example 서비스에서 사용자의 Google 리소스에 접근할 수 있게 만드는 것

OAuth 흐름

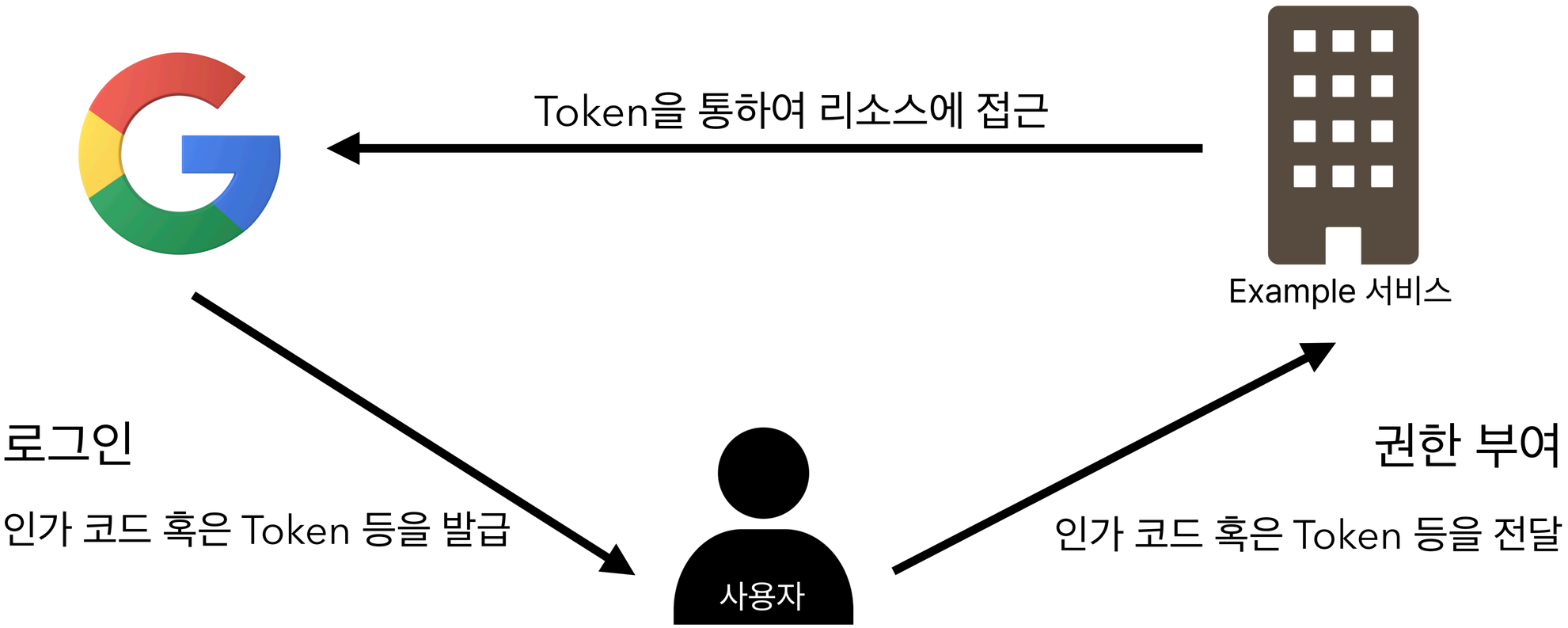
Example 서비스에서 Token을 통하여 사용자의 Google 리소스에 접근

OAuth 흐름



사용자의 권한 부여를 통하여, Example 서비스가 Token을 획득

OAuth 흐름

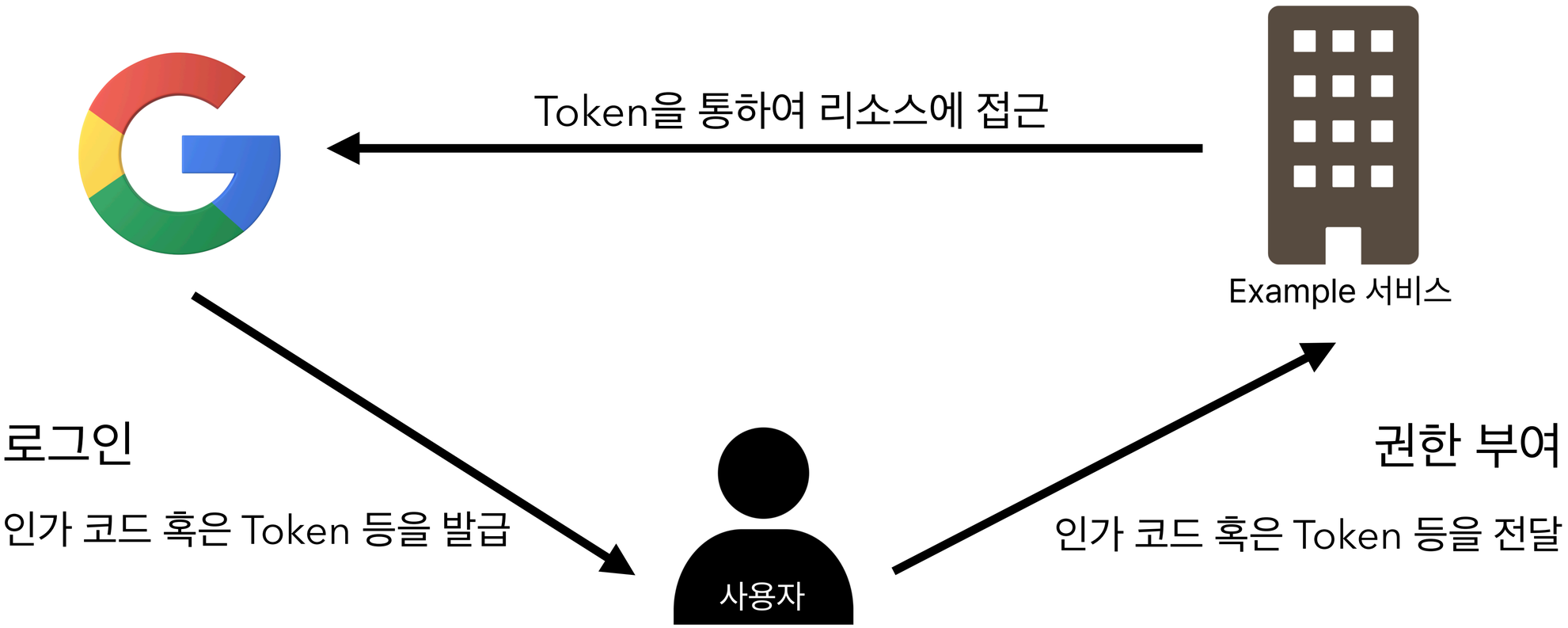


사용자는 구글에 로그인하여 인가 코드 혹은 Token 등을 발급받음

기술의 궁극적인 목적을 파악하고

목적을 달성하기 위하여 필요한 기능을 파악

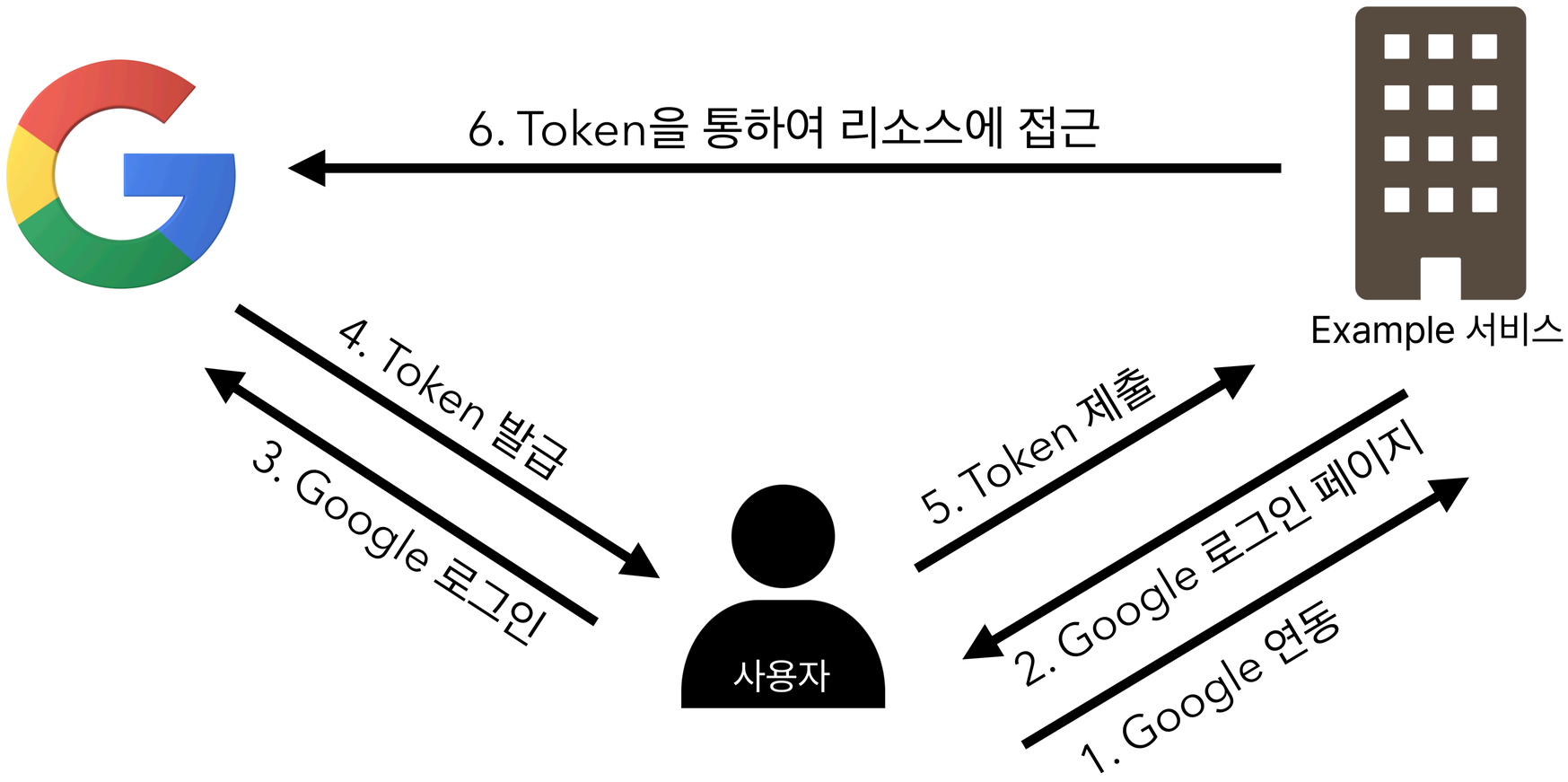
권한 부여란?



인가 코드 혹은 Token? 권한 부여?

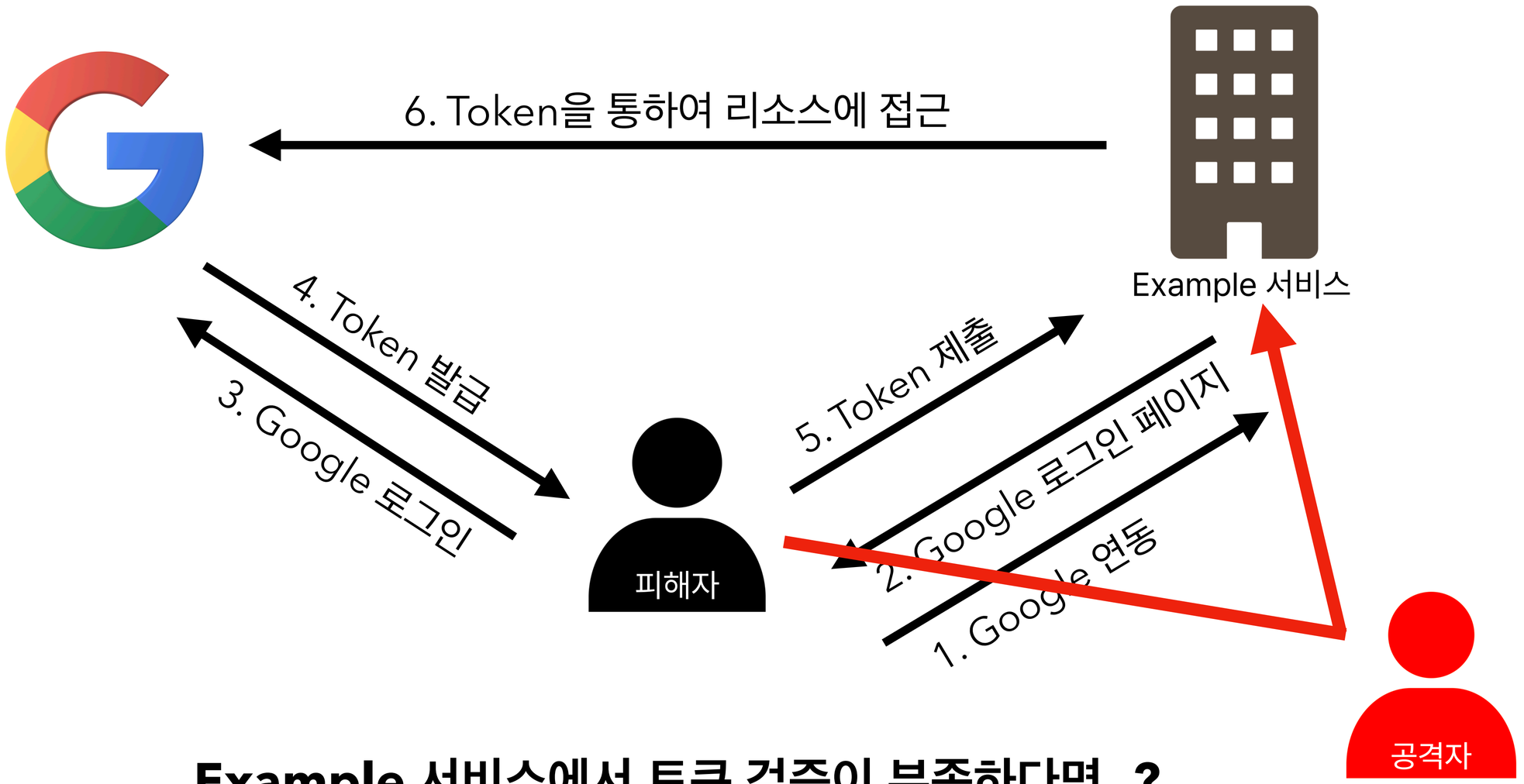
OAuth 권한 부여 방식

Implicit Grant Type



Token을 직접 발급받는 방식

What if …?



Example 서비스에서 토큰 검증이 부족하다면..?

Implicit Grant Type 보안 위협

브라우저 기반 노출 위험

→ 토큰이 URL, 히스토리, 로그 등에 저장될 수 있음

→ 의도치 않게 토큰이 노출될 위험

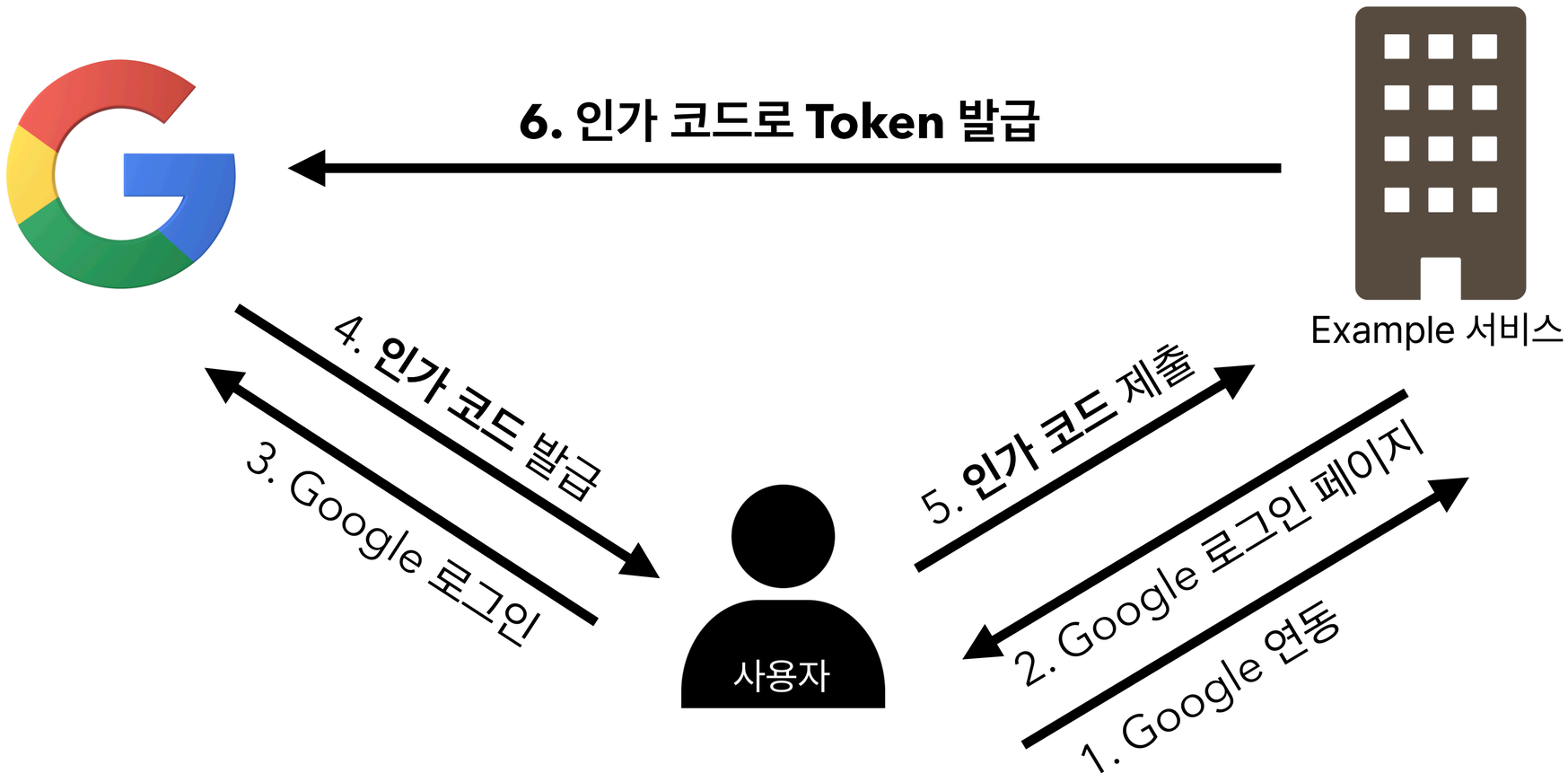
Access Token 보안 위험

→ 탈취 시, 공격자가 토큰을 재사용할 수 있기에 피해자 리소스에 무단으로 접근하기 쉬움

→ Access Token에 대한 검증이 부족할 수 있음

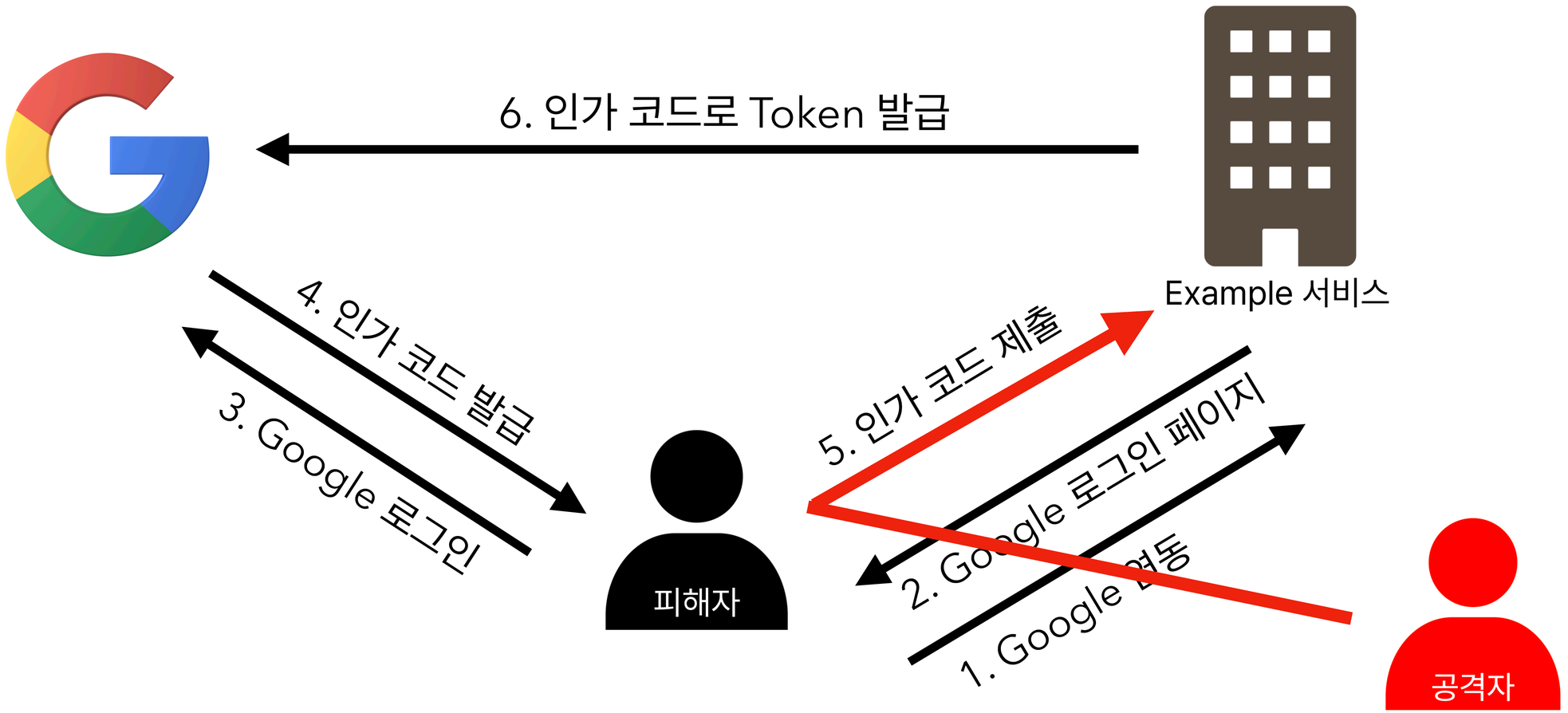
Implicit Grant Type은 새로 도입될 표준인 OAuth 2.1에서 공식적으로 제거

Authorization Code Grant Type



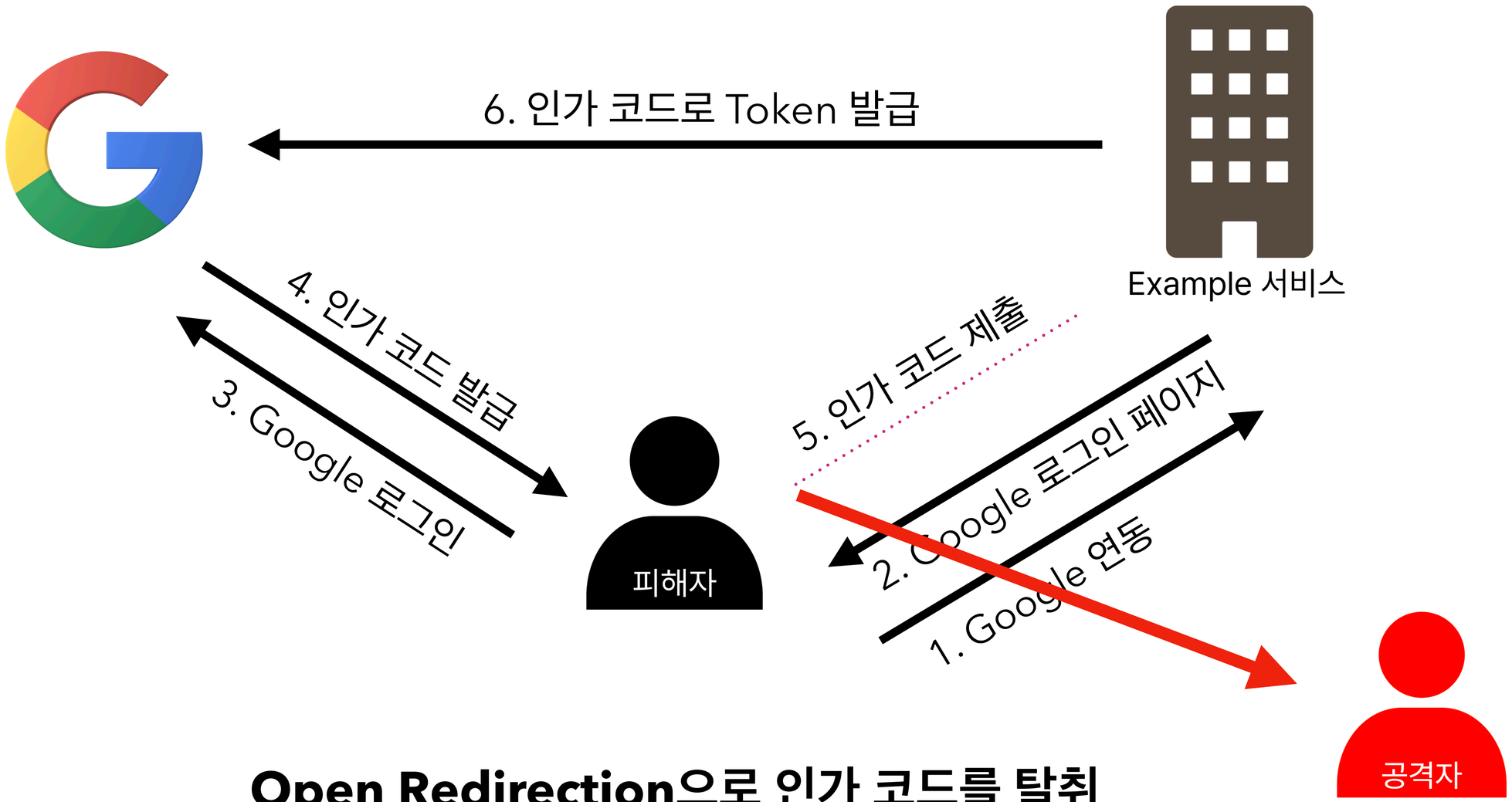
일회용 인가 코드로 Token을 발급받는 방식

What if …?



피해자의 계정에서 공격자의 인가 코드로 소셜 연동/로그인

What if …?



Open Redirection으로 인가 코드를 탈취

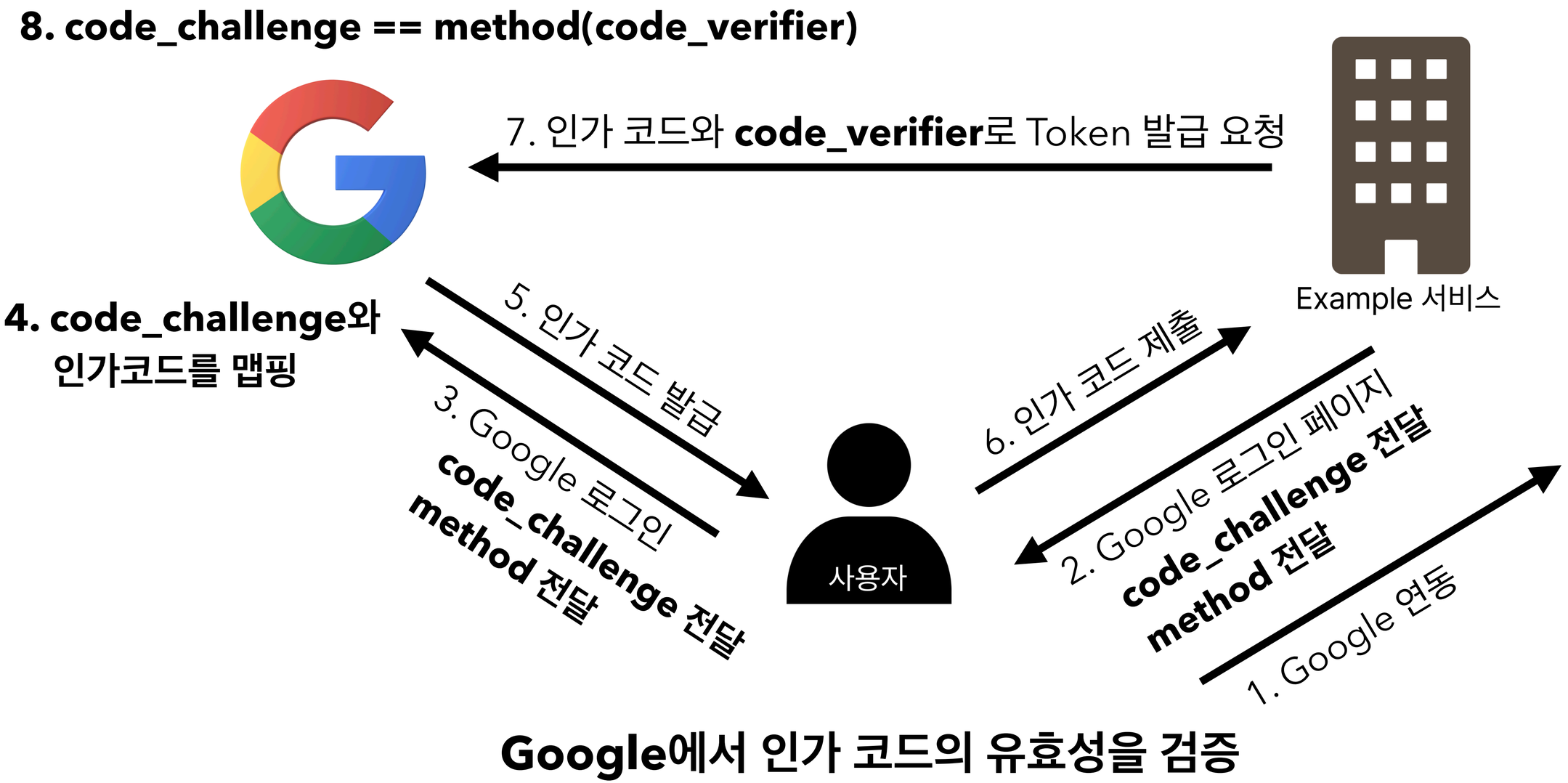
Authorization Code Grant Type 보안 위협

일회용 인가 코드를 발급한다는 점에서

Implicit Grant Type에 비해 안전한 것은 사실

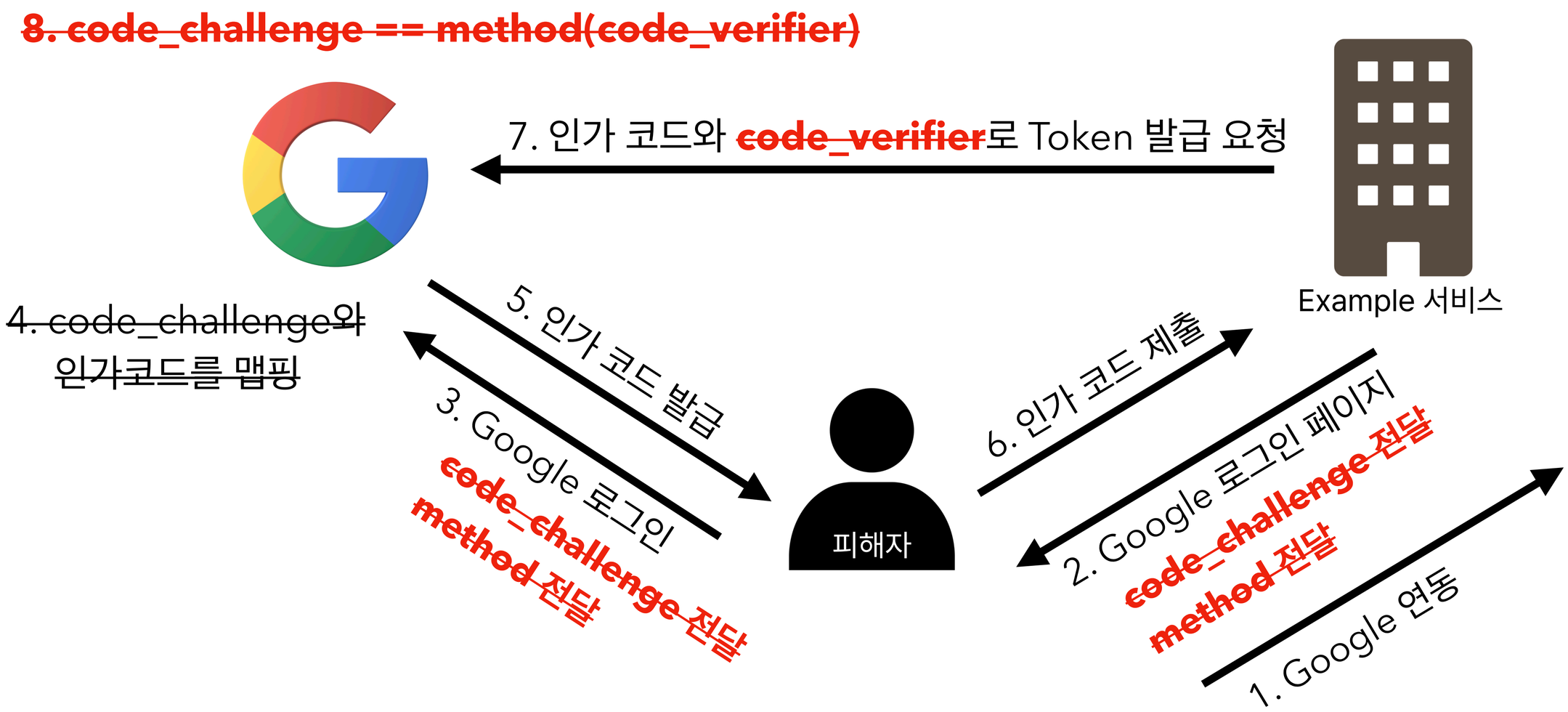
하지만 인가 코드가 탈취되거나 남용될 시나리오가 여전히 존재

Authorization Code Grant Type + PKCE



Google에서 인가 코드의 유효성을 검증

What if …?



PKCE 정보를 누락한 요청을 허용한다면..?

Authorization Code Grant Type + PKCE 보안 위협

권한 부여 방식 중 가장 안전

하지만 PKCE를 강제하지 않으면

PKCE를 사용하지 않는 Authorization Code Grant Type으로

Downgrade될 가능성 존재

복잡한 OAuth를 깊이 파고

이를 간결하게 바라볼 수 있었습니다

리얼 월드의 수많은 서비스들은

OAuth를 안전하게 구현하였을까?

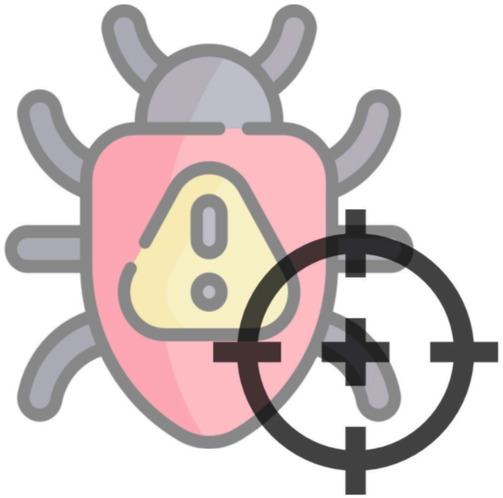
hackerone

bugcrowd

프로젝트 방향성

취약성 탐지
자동화 도구 제작

버그 헌팅



자동화 도구 제작

기존 자동화 도구 벤치마킹

기존 자동화 도구의 한계

수동으로 로그인 과정 진행

제한적인 취약성 탐지 (2개)

*Caido Workflow Eval SSO 플러그인 기준

기능 확장이 어려움

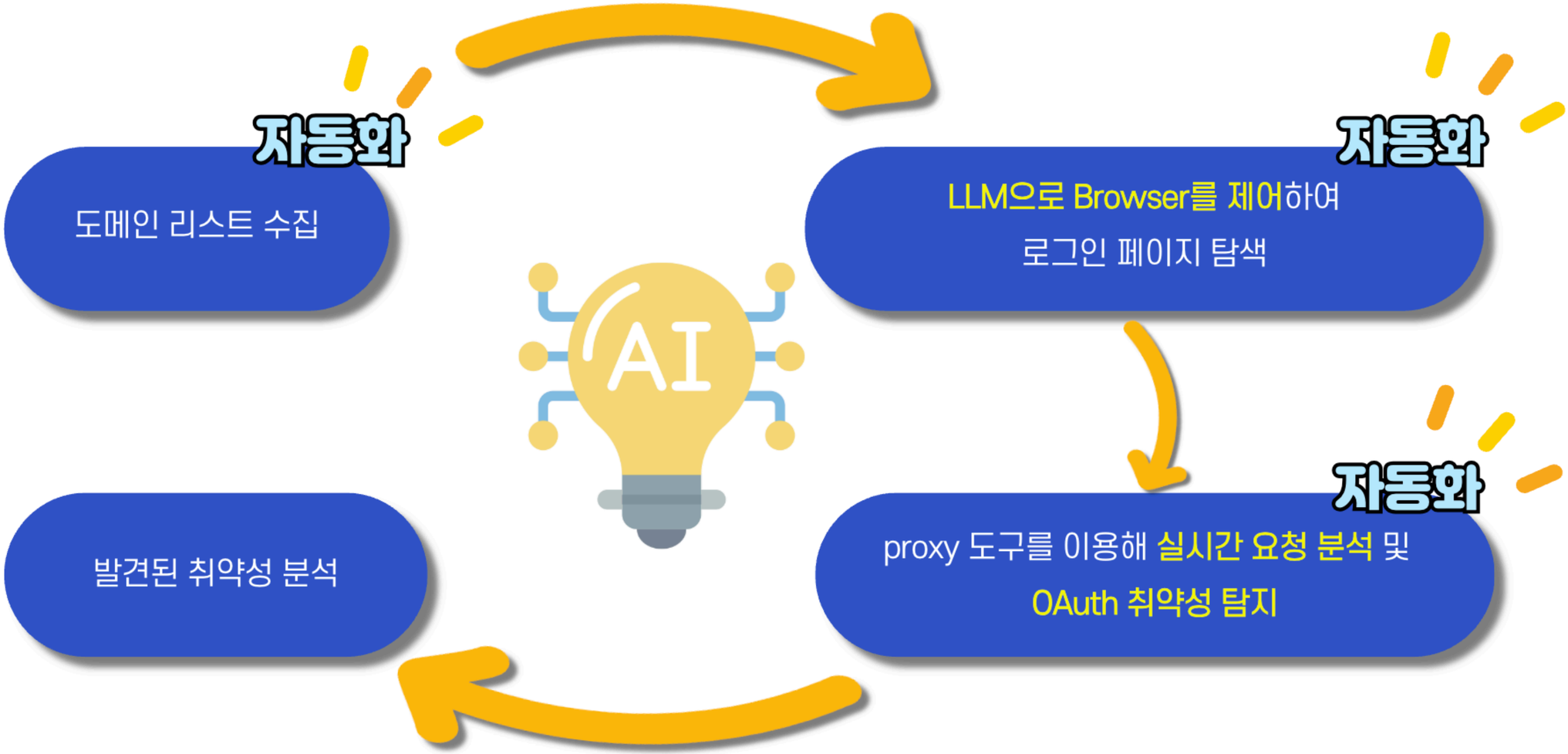
개선 사항

AI를 활용한 로그인 자동화

폭넓은 취약성 탐지

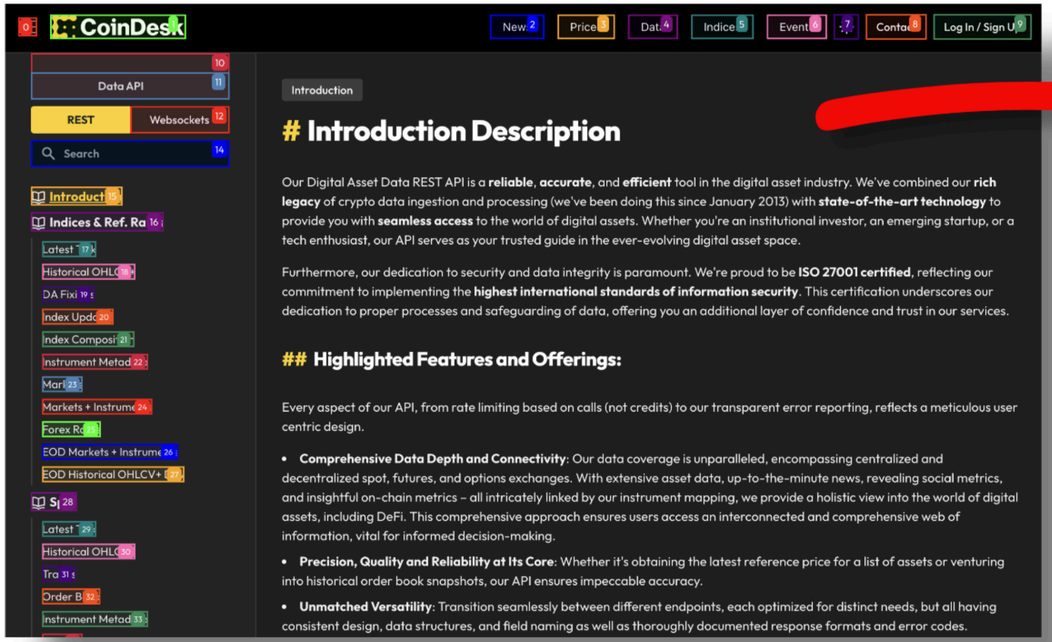
확장성을 고려하여 설계

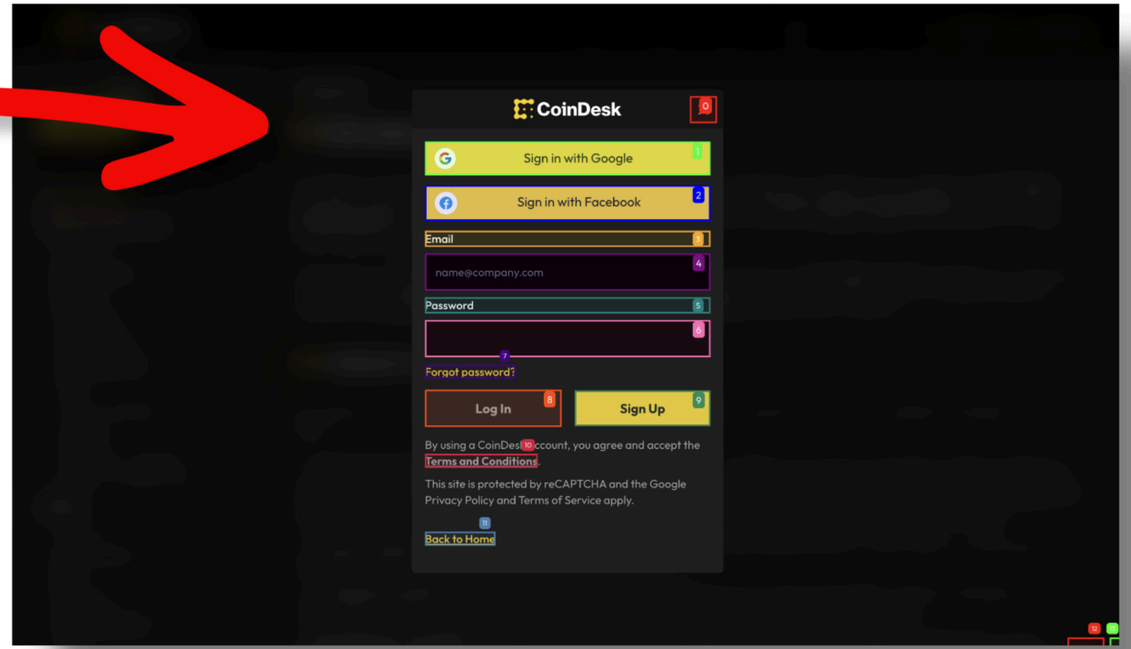
워크 플로우


자동화
도메인 리스트 수집
자동화
LLM으로 Browser를 제어하여
로그인 페이지 탐색
AI
자동화
proxy 도구를 이용해 실시간 요청 분석 및
OAuth 취약성 탐지
발견된 취약성 분석

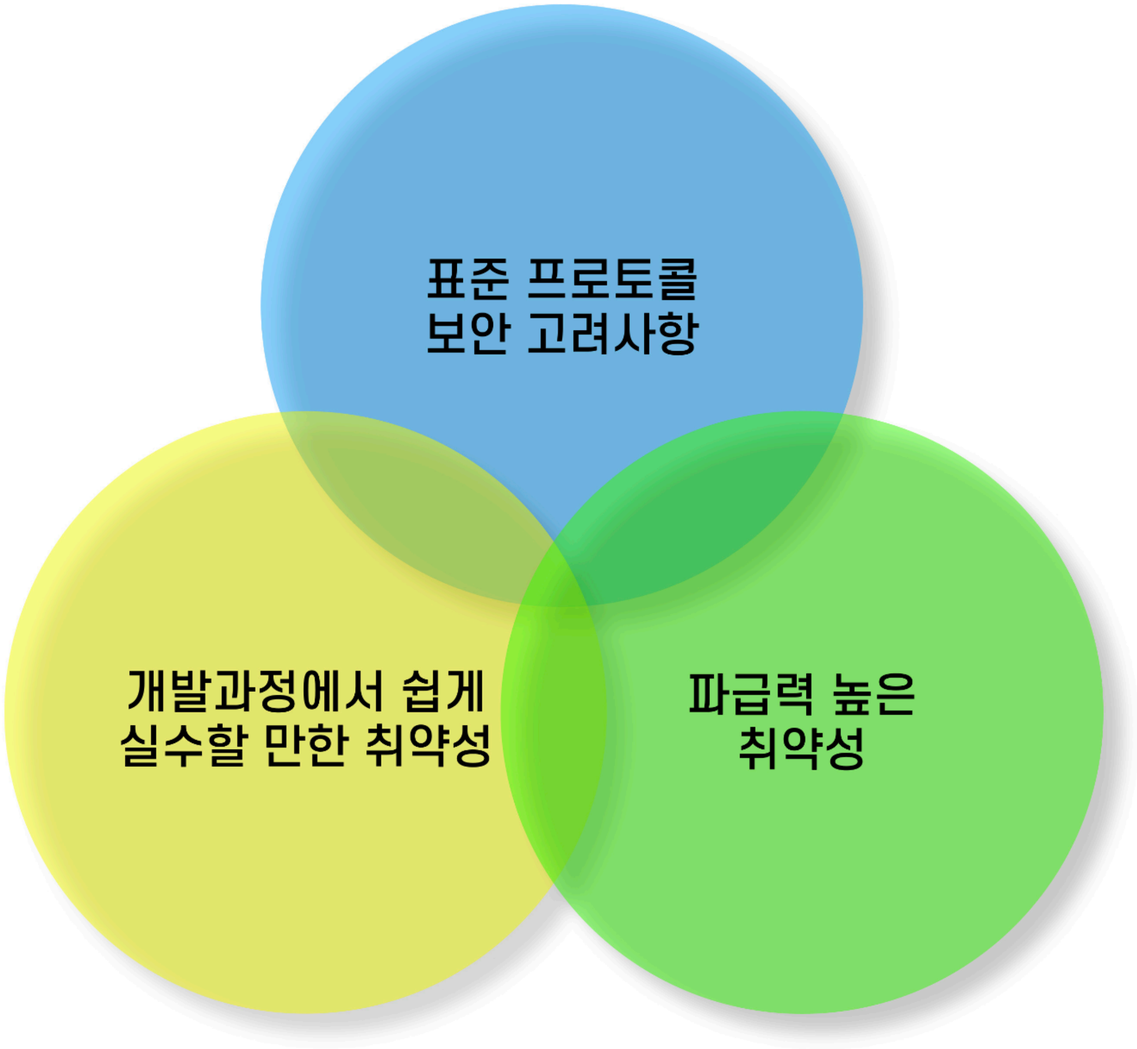
LLM을 활용한 로그인 자동화

Browser Use





자동화할 취약성 선정 기준



폭넓은 취약성 탐지

검증 가능한 취약성

1. PKCE Downgrade
2. CSRF
3. Access Token Leak
4. Redirect URI
5. Scope 범위 설정
6. Client_Secret 노출

기존 도구*

1. grant type 검사
2. state 파라미터 유무 검사

*Caido Workflow Eval SSO 플러그인

기술적 시행착오

알고리즘 기반

→ 디버깅 용이

→ 결과 예측 가능

→ 명확한 로직을 정할 수 있음

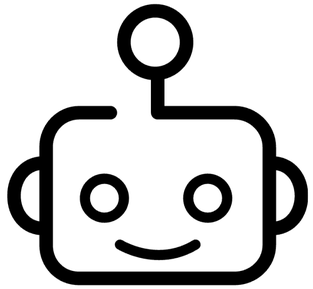
AI 프롬프트 기반

→ 디버깅 어려움

→ 같은 프롬프트여도 다른 결과가 산출될 수 있음

→ 명확한 로직을 프롬프트로 지정하여도
로직대로 실행되지 않음

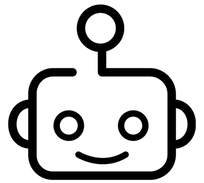
기술적 시행착오



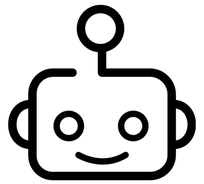
OAuth 리스트 탐색 Agent


```
{
    "msg": "Login page found",
    "url": "https://example.com/login",
    "sso_list": ["Google", "GitHub"]
}
```

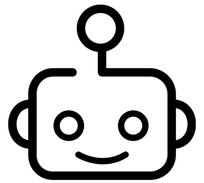

OAuth 리스트 반환



Google 연동 Agent



Github 연동 Agent



네이버 연동 Agent

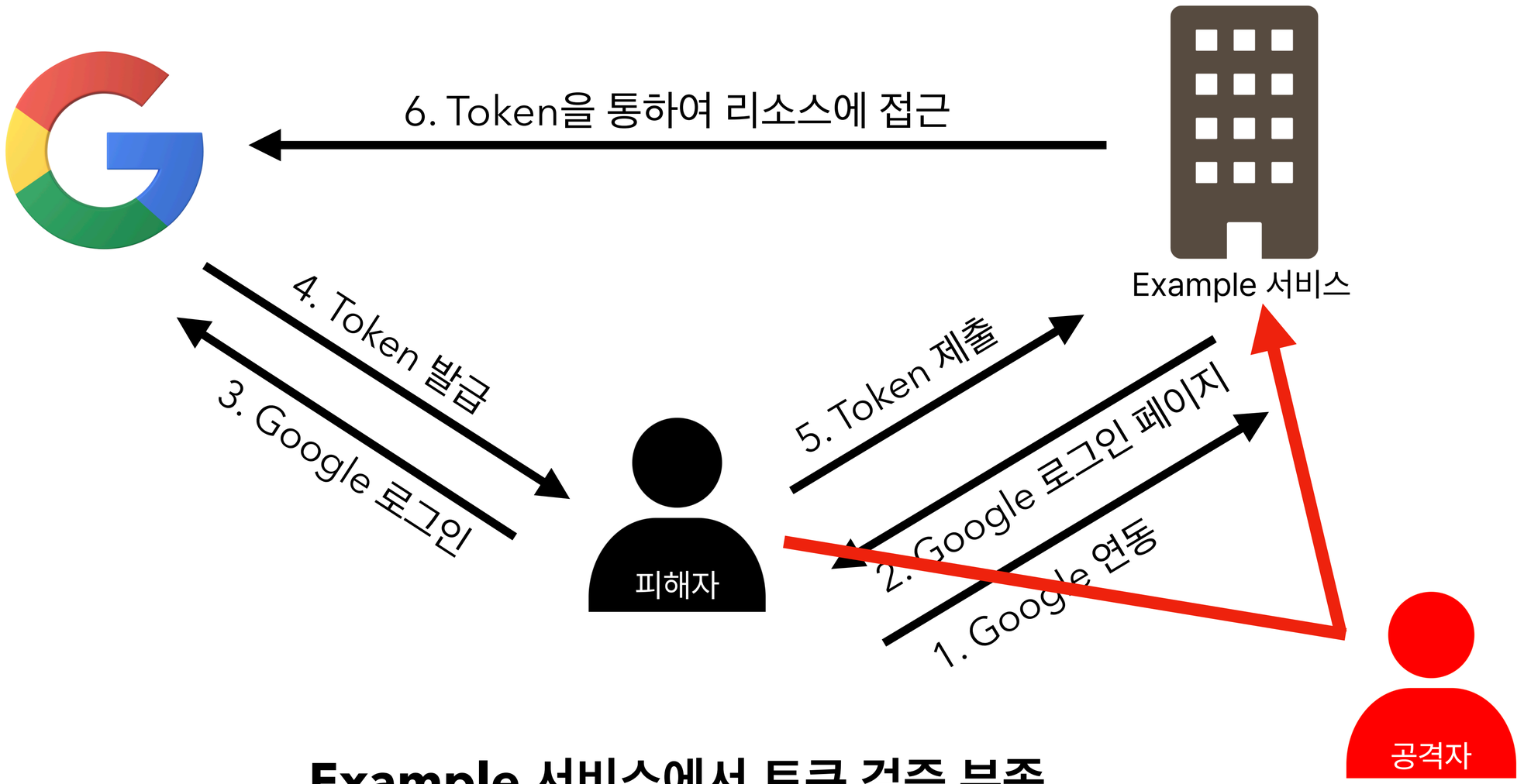
자동화 도구 사용 결과

- 6-8_1-600
- 6-8_1-600.csv
- 600-700
- 600-700.csv
- 2000~2200
- 2000~2200.csv
- 4000-5000
- 4000-5000.csv
- 5000-5200.csv
- 5200-5500.csv
- 8000-8100.csv
- 10000-10500
- 10000-10500.csv
- 14000-15500
- 14000-15500.csv

http://velog.io	MEDIUM	CSRF Risk	Nonce reused without cookies
http://velog.io	MEDIUM	CSRF Risk	Nonce reused without cookies
http://data-api.coindesk.com	MEDIUM	CSRF Risk	Missing state/nonce in request
http://data-api.coindesk.com	MEDIUM	CSRF Risk	Missing state/nonce in request
http://data-api.coindesk.com	MEDIUM	CSRF Risk	Missing state/nonce in request
http://intranet.cbre.com	MEDIUM	CSRF Risk	Nonce reused without cookies
http://intranet.cbreim.com	MEDIUM	CSRF Risk	Nonce reused without cookies
http://intranet.cbreim.com	MEDIUM	CSRF Risk	Nonce reused without cookies
http://regatta.aiven.io	MEDIUM	CSRF Risk	Identical redirects on nonce swap → potential CSRF
http://asp-stg-develop.eks-stg-use1.getaws.arubanetworks.co	MEDIUM	CSRF Risk	Identical redirects on nonce swap → potential CSRF
http://lms-stg-develop.eks-stg-use1.getaws.arubanetworks.co	MEDIUM	CSRF Risk	Identical redirects on nonce swap → potential CSRF
http://lms-stg-develop.eks-stg-use1.getaws.arubanetworks.co	MEDIUM	Potential PKCE Downgrade	Potential PKCE downgrade vulnerability! Server accepts requests without PKCE.
http://www.arubanetworks.com	MEDIUM	CSRF Risk	Identical redirects on nonce swap → potential CSRF
http://mspshowcase.arubanetworks.com	MEDIUM	CSRF Risk	Identical redirects on nonce swap → potential CSRF
http://mspshowcase.arubanetworks.com	MEDIUM	Potential PKCE Downgrade	Potential PKCE downgrade vulnerability! Server accepts requests without PKCE.
http://aed.arubanetworks.com	MEDIUM	CSRF Risk	Nonce reused without cookies
http://id.atlassian.com	MEDIUM	CSRF Risk	Identical redirects on nonce swap → potential CSRF
http://id.atlassian.com	MEDIUM	Potential PKCE Downgrade	Potential PKCE downgrade vulnerability! Server accepts requests without PKCE.
http://id.atlassian.com	MEDIUM	PKCE Not Enforced	Server accepts OAuth request without PKCE parameters.
http://id.atlassian.com	MEDIUM	CSRF Risk	Identical redirects on nonce swap → potential CSRF
http://id.atlassian.com	MEDIUM	PKCE Not Enforced	Server accepts OAuth request without PKCE parameters.
http://id.atlassian.com	MEDIUM	PKCE Not Enforced	Server accepts OAuth request without PKCE parameters.
http://id.atlassian.com	MEDIUM	CSRF Risk	Identical redirects on nonce swap → potential CSRF
http://id.atlassian.com	MEDIUM	CSRF Risk	Identical redirects on nonce swap → potential CSRF
http://start.atlassian.com	MEDIUM	CSRF Risk	Identical redirects on nonce swap → potential CSRF
http://start.atlassian.com	MEDIUM	Potential PKCE Downgrade	Potential PKCE downgrade vulnerability! Server accepts requests without PKCE.
http://start.atlassian.com	MEDIUM	PKCE Not Enforced	Server accepts OAuth request without PKCE parameters.
http://start.atlassian.com	MEDIUM	CSRF Risk	Identical redirects on nonce swap → potential CSRF
http://start.atlassian.com	MEDIUM	PKCE Not Enforced	Server accepts OAuth request without PKCE parameters.
http://start.atlassian.com	MEDIUM	PKCE Not Enforced	Server accepts OAuth request without PKCE parameters.
http://start.atlassian.com	MEDIUM	CSRF Risk	Identical redirects on nonce swap → potential CSRF

16,000개의 서비스 검증

실제 취약점 사례1



Example 서비스에서 토큰 검증 부족

Access Token의 aud 클레임


```
{
  "issued_to":"16435018183-9a880bertda0en85387ge8f8mgsves71.apps.googleusercontent.com",
  "audience":"16435018183-9a880bertda0en85387ge8f8mgsves71.apps.googleusercontent.com",
  "user_id":"105753821512785749705",
  "scope":"https://www.googleapis.com/auth/userinfo.email https://www.googleapis.com/auth/userinfo.profil
  "expires_in":3560,
  "email":"whs.imnya.ng@gmail.com",
  "verified_email":true,
  "access_type":"online"
}
```

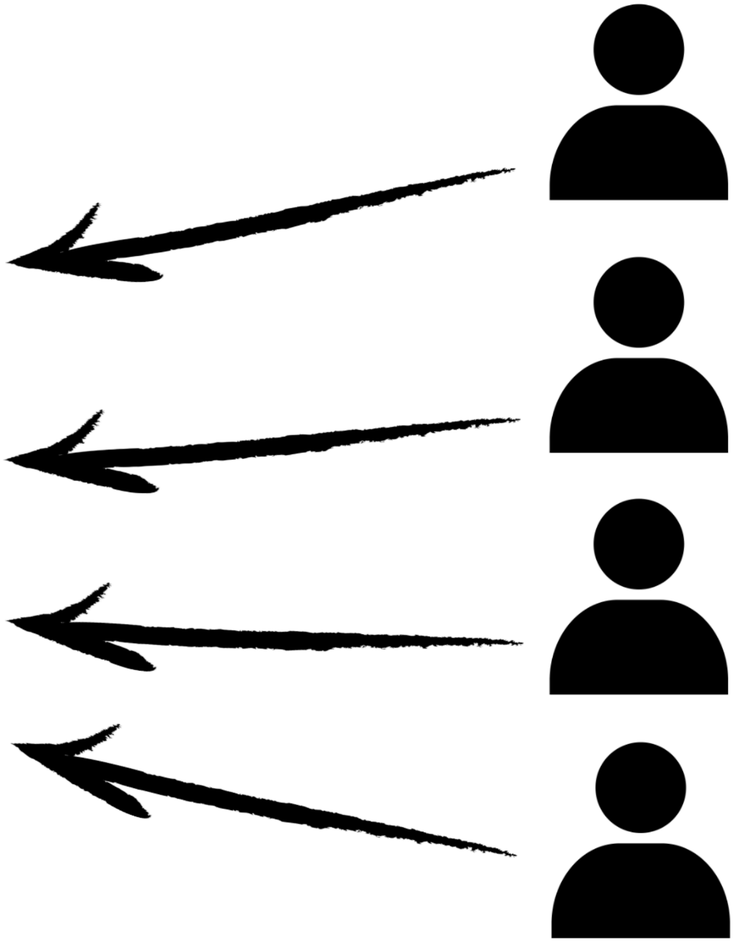

audience 클레임

→ 이 토큰의 수신 대상자

→ 용도인증 또는 자원 접근 시 토큰이 정당한 대상자에게 발급된 것인지 검증

공격자의 Access Token 수집

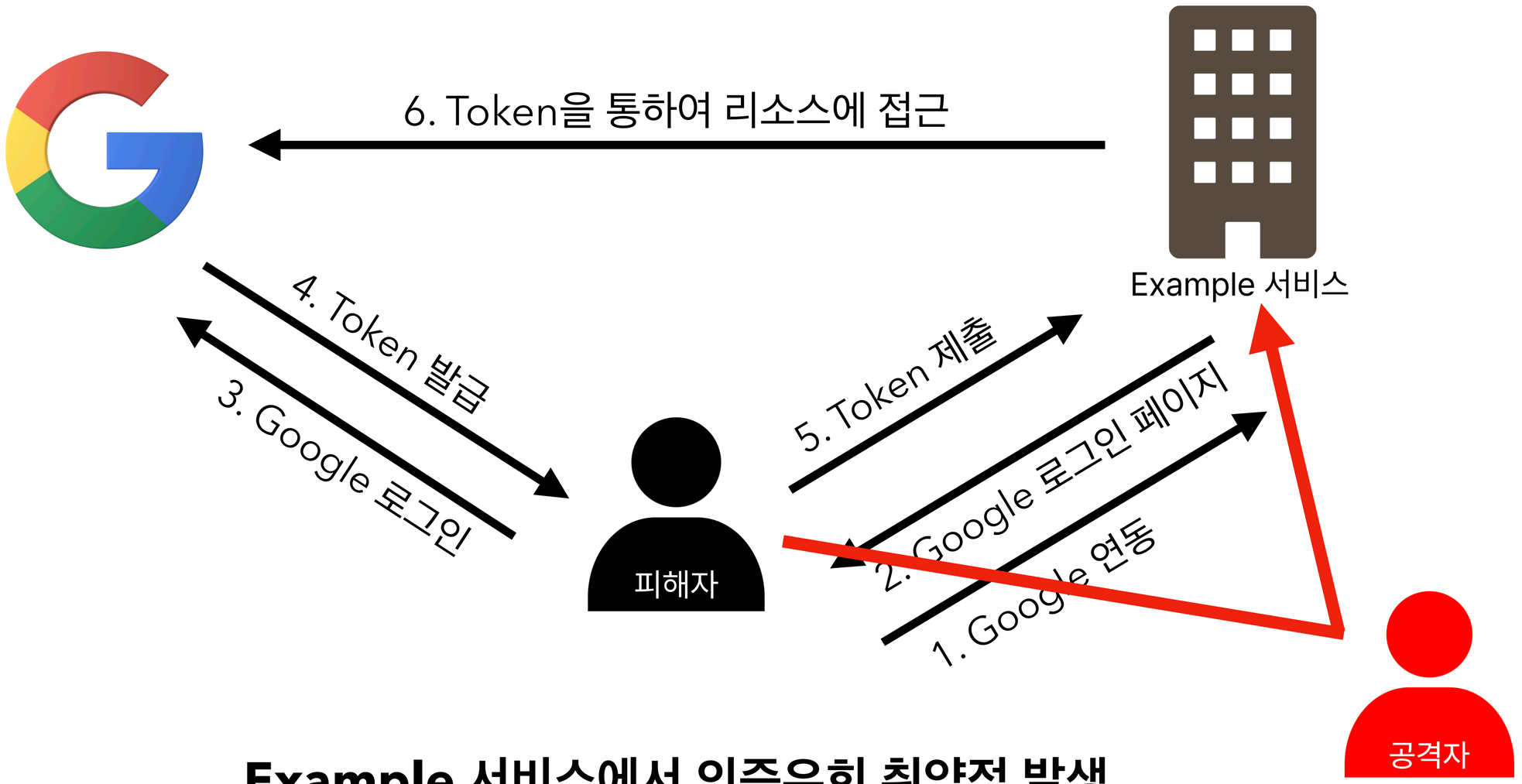
1. 공격자가 악성 사이트 제작



2. 피해자가 공격자의 사이트에 소셜 로그인

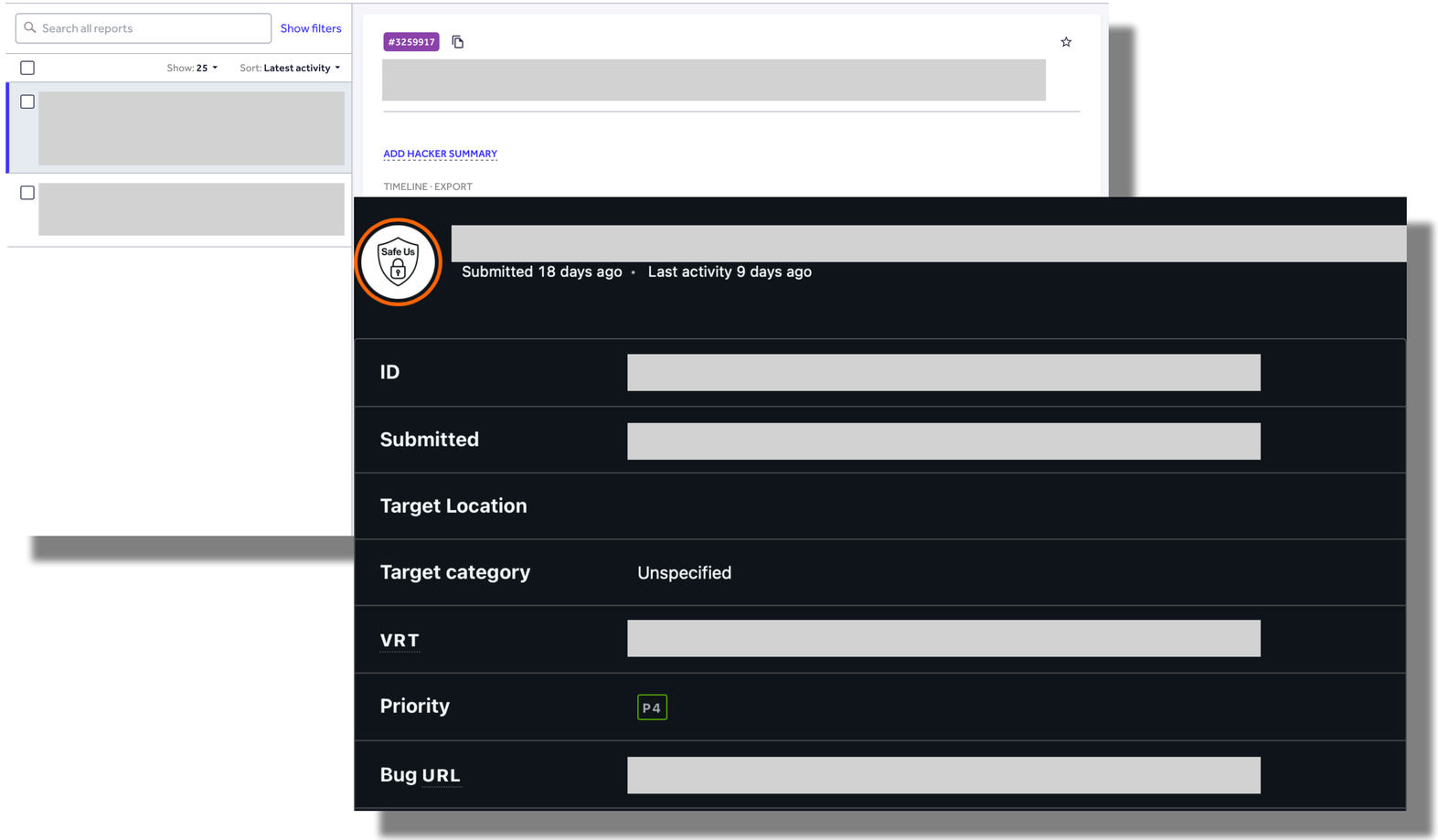
3. 피해자의 Access Token 수집

위협 시나리오



Example 서비스에서 인증우회 취약점 발생

계정 탈취 취약점 제보

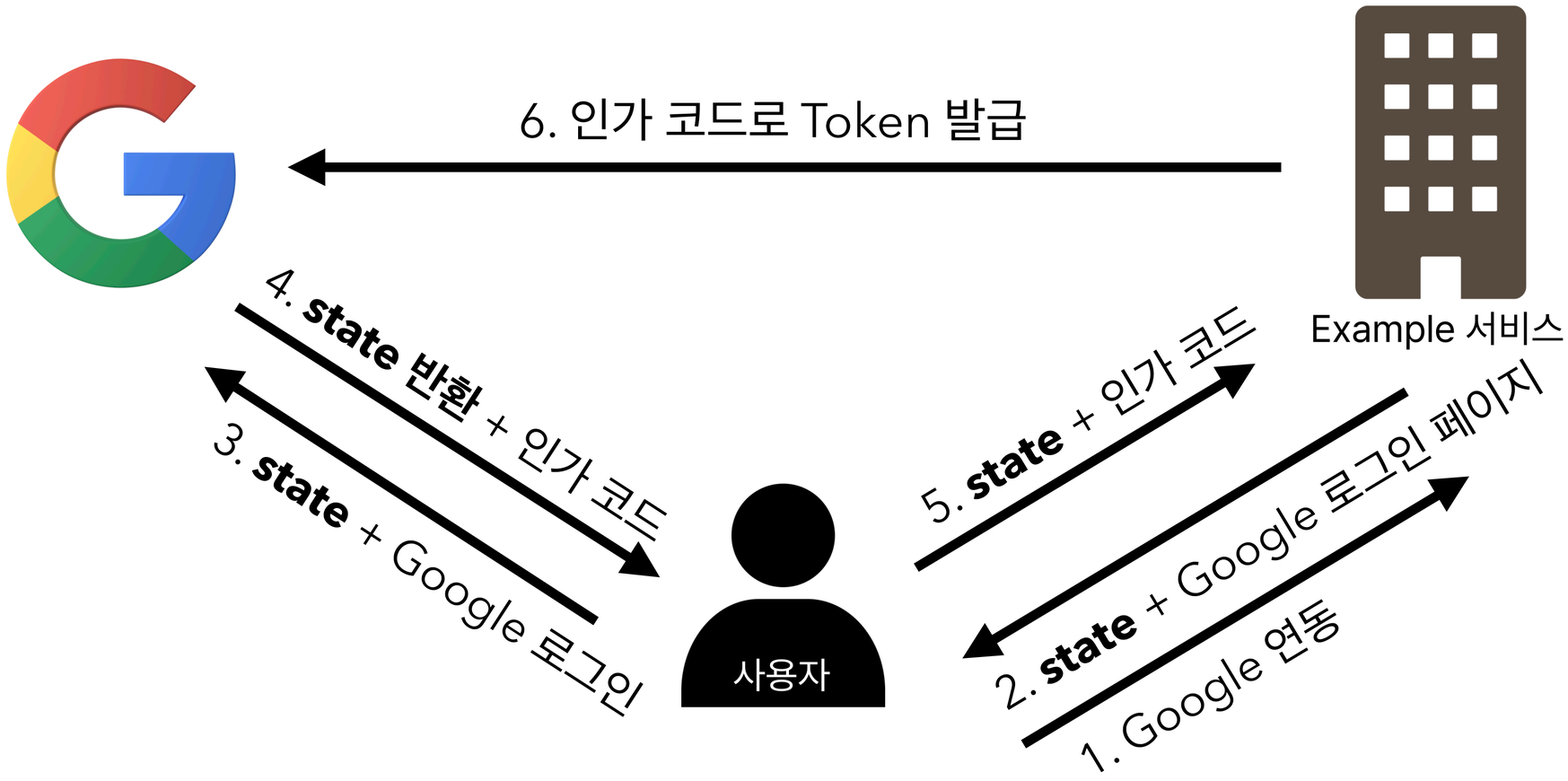


해당 취약점을 악용하여

계정 탈취 가능!

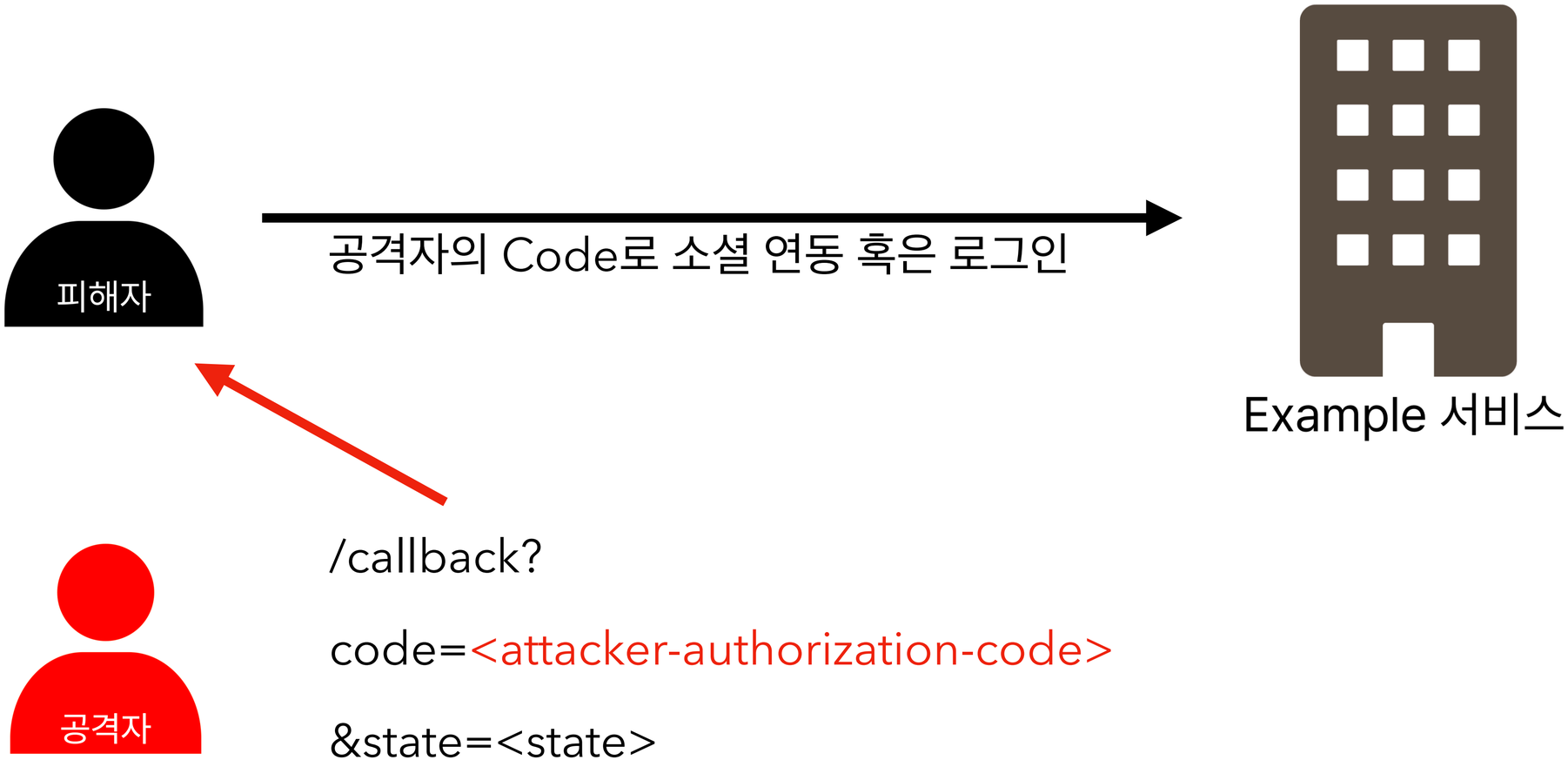
3건의 계정 탈취 취약점 발견

실제 취약점 사례2



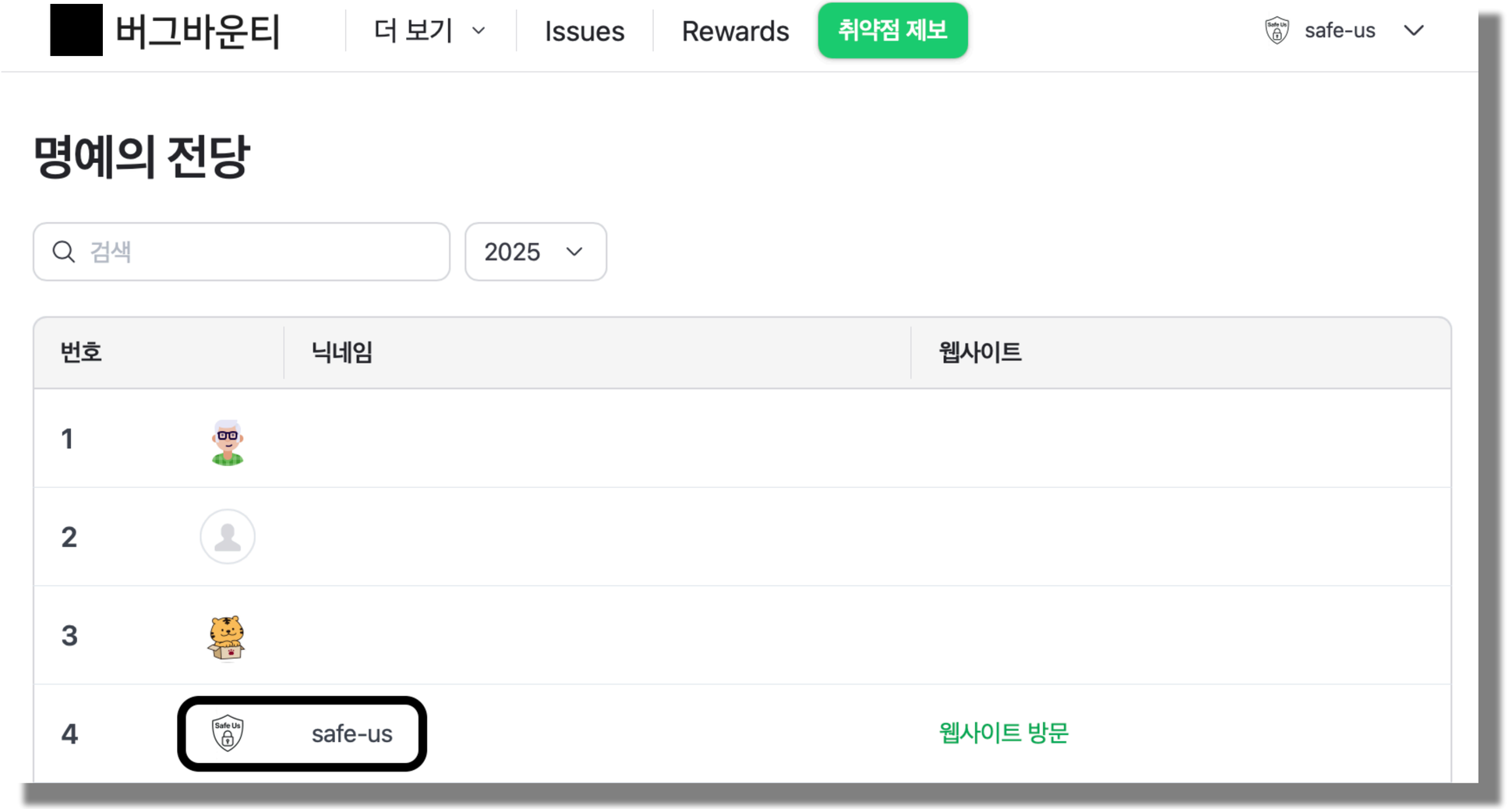
Example 서비스에서 state가 유효한지 검증하지 않음

위협 시나리오



계정 탈취 혹은 민감한 정보 유출 가능

성과


버그바운티
더 보기
Issues
Rewards
취약점 제보
safe-us
명예의 전당
검색
2025
번호
닉네임
웹사이트
1
2
3
4
safe-us
웹사이트 방문

Q & A