Authentication & Authorization

What is authentication?

출처: https://www.flaticon.com/

What is authentication?

Who are you?

출처: https://www.flaticon.com/

What is authorization?

What is authorization?

What can I do?

RESTRICTED AREA

AUTHORIZED PERSONNEL ONLY

출처: https://www.flaticon.com/

Authentication vs Authorization

- **Authentication(인증)**

  - "Authentication is the process of <mark>verifying who a user is</mark>."

  - 401 Unauthorized

- **Authorization(권한/허가)**

  - "Authorization is the process of <u>verifying what they have</u> <mark>access to</mark>."

  - 403 Forbidden

출처: https://auth0.com/docs/authorization/authentication-and-authorization

Authentication vs Authorization

- ## Authentication(인증)

  - **자신이라고 주장하는 유저 확인**

  - Credentials(비밀번호, 얼굴인식) 검증

  - *Django -> 게시판 서비스 로그인*

  - 인증 이후에 획득하는 권한 (생성, 수정, 삭제)

- ## Authorization(권한/허가)

  - **유저가 자원에 접근할 수 있는지 여부 확인**

  - 규칙/규정에 의해 접근할 수 있는지 확인

  - *Django -> 일반 유저 vs 관리자 유저*

  - 인증 이후에 부여되는 권한
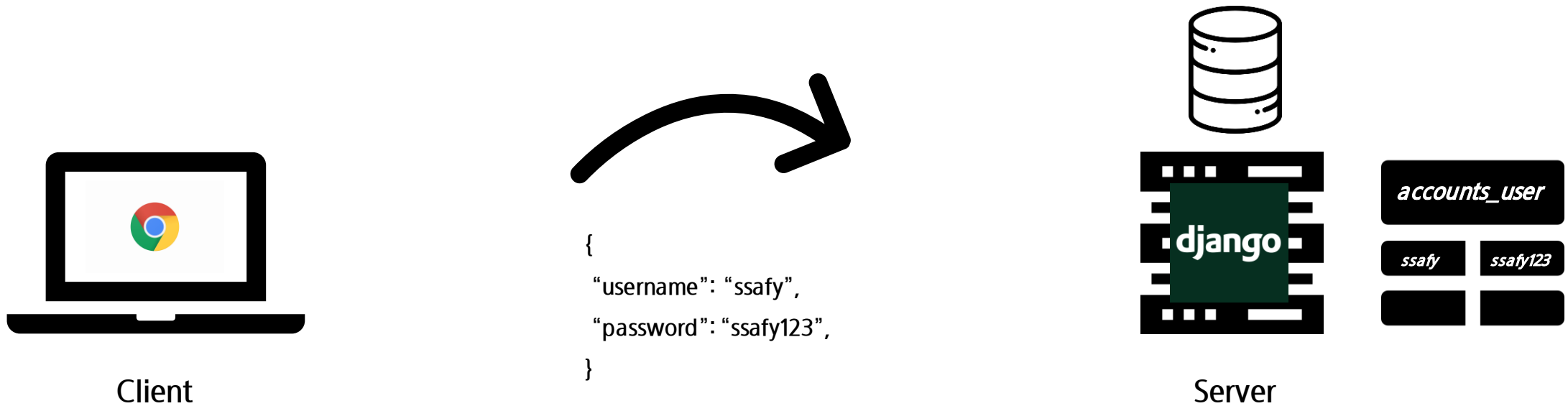
    - 예시 - 로그인 후 글 작성 여부

Session

Client

```
{
  "username": "ssafy",
  "password": "ssafy123",
}
```

Server

Session

Client
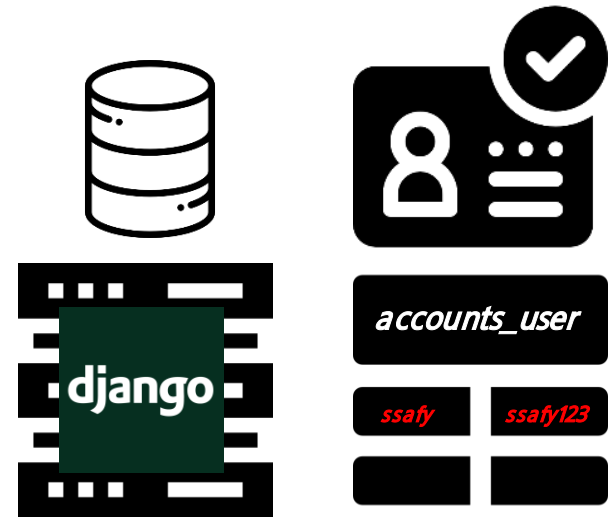
```
{
  "username": "ssafy",
  "password": "ssafy123",
}
```

Server

Session

Client

```
{
  "username": "ssafy",
  "password": "ssafy123",
}
```
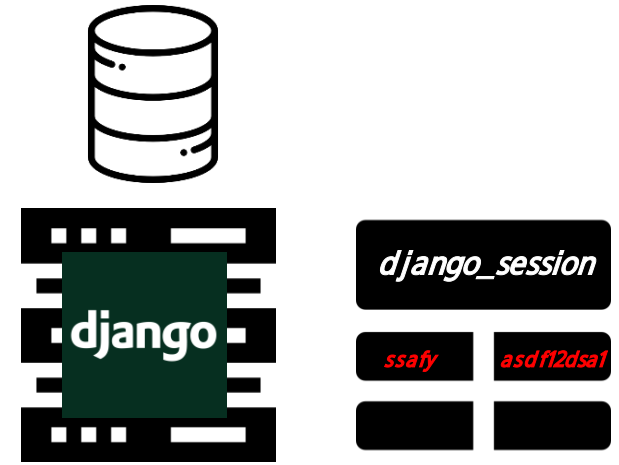
accounts_user

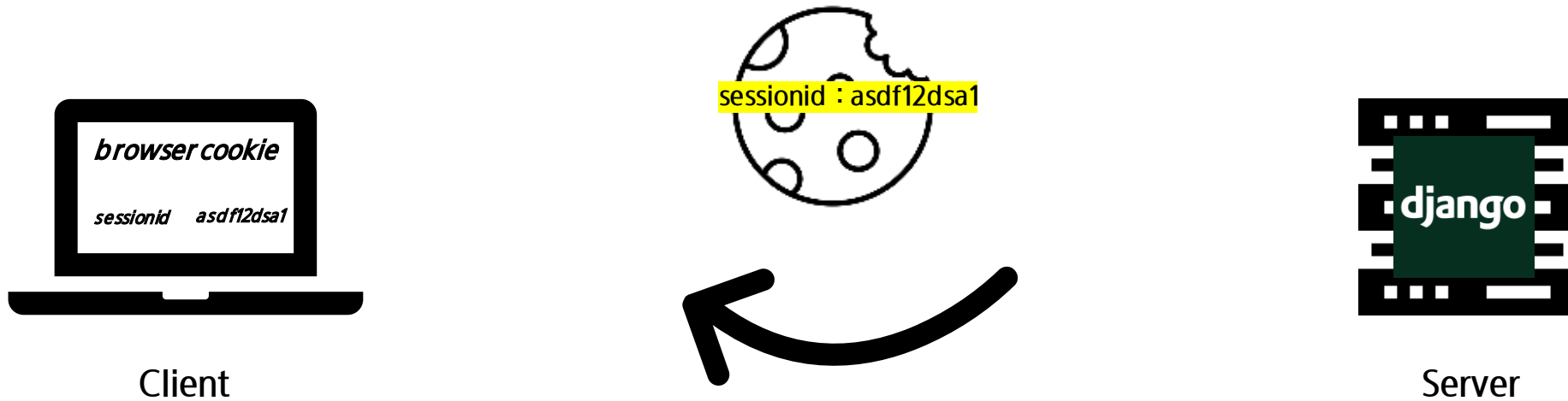ssafy   ssafy123

Server

Session

Client

Server

Session

Client

sessionid : asdf12dsa1

django_session

ssafy | asdf12dsa1

Server

Session

browser cookie

sessionid   asdf12dsa1

sessionid : asdf12dsa1

django

Client

Server

Session

browser cookie

sessionid   asdf12dsa1

Client

▼ Request Headers   view source

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9

Accept-Encoding: gzip, deflate, br

Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7

Cache-Control: max-age=0

Connection: keep-alive

Cookie: name=justin; csrftoken=IZtQSZzml4wrn9VqQTJ2Amek1eivWVriLLXE9NddirYJmNPONnXwjQjKcq3j5Bwv; sessionid=goyr8j3btfhfys6x7lyywhfrla1d4dfd

django

Server

Session

Client

Server

Session

Client

Server