12 기본 인증

CodeDiary18(codediary18@gmail.com)

2022.03.08

목차

12 기본 인증

모든 정보나 업무는 공용이 아니다

↓

허가된 사람만이 **데이터에 접근하고 업무를 처리**할 수 있도록 해야 함

서버가 **사용자가 누구인지 식별**할 수 있어야 함

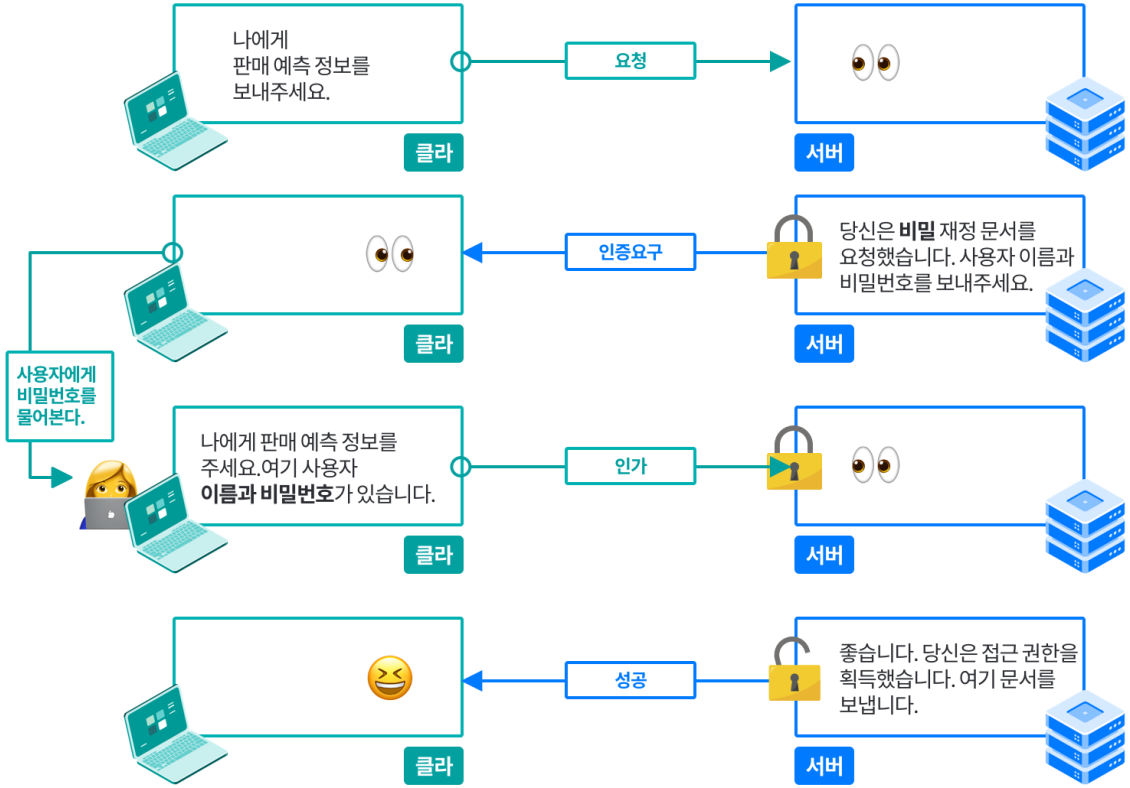
12.01 인증

- 인증이란?
  당신이 **누구인지 증명**하는 것

- 완벽한 인증이 존재할까?
  - 완벽한 인증이란 **없음**
  - 하지만, 당신에 대한 여러 데이터는 당신이 누구인지 판단하는데 도움

12.01 인증

- HTTP의 인증요구/응답 프레임워크



12.01 인증

- 인증 프로토콜과 헤더
  - HTTP는 필요에 따라 고쳐 쓸 수 있는 제어 헤더를 통해, 다른 인증 프로토콜에 맞추어 확장할 수 있는 프레임워크를 제공
  - HTTP에는 **기본 인증, 다이제스트 인증, OAuth 인증**이 존재

단계	헤더	설명	메서드/상태
요청		첫번째요청에는 인증 정보가 없음	GET
인증 요구	WWW-Authenticate	서버는 사용자에게 사용자 이름과 비밀번호를 제공하라는 의미로 401	401 Unauthorized
인증	Authorization	클라이언트는 요청을 다시보내는데 인증 정보헤더를 보냄	GET
성공	Authentication-Info	인증 정보가 정확하면 서버는 문서와 함께 응답	200 OK

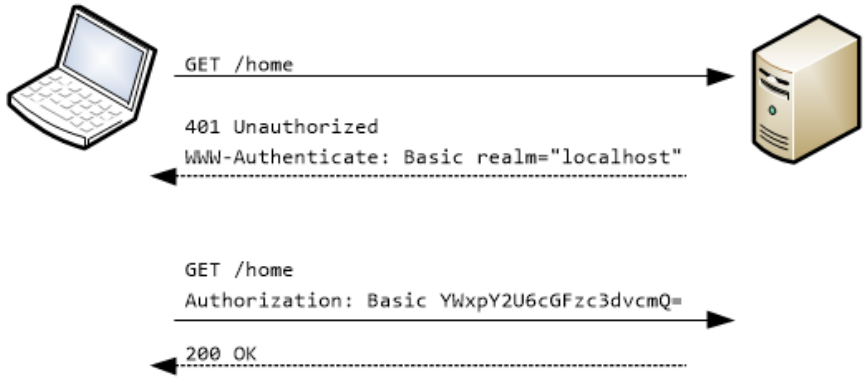
12.01 인증

- 기본 인증의 예

1. 서버가 사용자에게 인증요구를 보낼 때,
   서버는 401 Unauthorized 응답과 함께
   WWW-Authenticate헤더를 기술해서
   어디서 어떻게 인증할지 설명

2. 클라이언트가 서버로 인증
   인코딩된 비밀번호와 그 외 인증
   파라미터들을 Authorization 헤더에
   담아서 요청

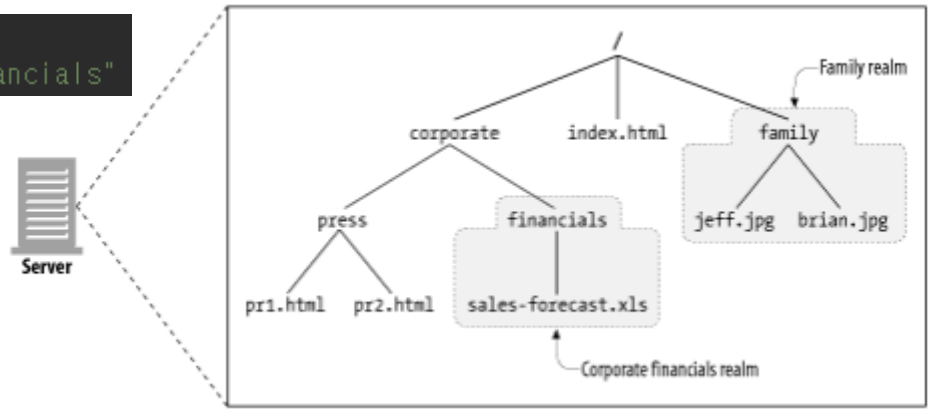
3. 정상적인 상태 코드를 반환
   추가적인 인증 알고리즘에 대한 정보를
   Authentication-Info 헤더에 기술



12.01 인증

- 보안 영역
  - 서버가 클라이언트로 인증 요구를 할 때, realm 지시자가 기술 되어 있는 WWW-Authenticate헤더를 전송
  - 웹 서버는 기밀 문서를 **보안 영역(realm) 그룹**으로 나눔
  - 보안 영역은 저마다 다른 사용자 권한을 요구

```
HTTP/1.0 401 Unauthorized
WWW-Authenticate: Basic realm="Corporate Financials"
```



12.02 기본 인증

- 기본 인증
  - 가장 잘 알려진 HTTP 인증 규약
  - 거의 모든 주요 클라이언트와 서버에 기본 인증이 구현됨
  - 웹 서버는 클라이언트의 요청을 거부하고 유효한 사용자 이름과 비밀번호를 요구할 수 있음
  - 서버는 200 대신 401 상태코드와 클라이언트가 접근하려고 했던 보안 영역을 WWW-Authenticate에 기술해서 응답하여, 인증요구를 시작

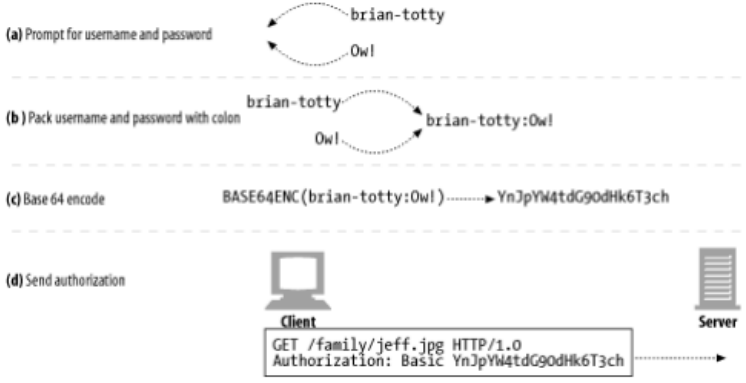
12.02 기본 인증

- 기본 인증의 예

인증요구/응답	헤더 문법과 설명
인증요구 (서버 → 클라이언트로)	각 사이트는 보안 영역마다 다른 비밀번호가 있음 realm은 요청 받은 문서 집합의 이름을 따옴표로 감싼 것으로, 사용자는 이 정보를 보고 어떤 비밀번호를 사용해야 하는지 알 수 있음 **WWW-Authenticate: Basic realm=따옴표로 감싼 문서 집합 정보**
응답 (클라이언트 → 서버로)	사용자 이름과 비밀번호는 콜론으로 잇고, base-64로 인코딩해서 사용자 이름과 비밀번호에 쉽게 국제문자를 포함할 수 있게 하고, 네트워크 트래픽에 사용자 이름과 비밀번호가 노출되지 않게 함 **Authorization: Basic base-64로 인코딩한 사용자 이름과 비밀번호**

12.02 기본 인증

- Base-64 사용자 이름/비밀번호 인코딩
  - HTTP 기본 인증은 사용자 이름과 비밀번호를 클론으로 이어서 합치고, base-64 인코딩 메서드를 사용해 인코딩
    - base-64 인코딩은 8비트 바이트로 이루어져 있는 시퀀스를 6비트 덩어리의 시퀀스로 변환
    - 각 6비트 조각은 대부분 문자와 숫자로 이루어진 특별한 64개의 문자 중에서 선택됨



12.02 기본 인증

- 프락시 인증
  - 중개 프락시 서버를 통해 인증 할 수 있음
  - 프락시 서버에서 접근 정책을 중앙 관리 할 수 있기 때문에, 회사 리소스 전체에 대해 통합적인 접근 제어를 하기 위해서 프락시 서버를 사용하면 좋음

웹서버	프락시 서버
비인증 상태 코드:401	비인증 상태 코드:407
WWW-Authenticate	Proxy-Authenticate
Authorization	Proxy-Authorization
Authentication-Info	Proxy-Authentication-Info

12.03 기본 인증의 보안 결함

- 기본 인증은 단순하고 편리하지만 안심할 수 없음
- 보안 결함
  - 기본 인증은 사용자 이름과 비밀번호를 **쉽게 디코딩**할 수 있는 형식으로 네트워크에 전송
  - 보안 비밀번호가 디코딩하기 복잡하더라도 이를 **캡쳐해서 인증**에 성공하고 서버에 접근이 가능
  - 기본 인증이 중요하지 않는 곳에 사용되더라도, 다른 사이트에서 해당 비밀번호를 사용하는 경우가 있기에 매우 위험
  - 메시지의 인증 헤더를 건드리지는 않지만 그 외 다른 부분을 수정해서 **트랜잭션의 본래 의도를 바꿔버리는 프락시나 중개자가 개입**하는 경우, 정상적인 동작을 보장하지 않음
  - 기본 인증은 **가짜 서버의 위장**에 취약

참고 및 사진 출처

- HTTP 완벽 가이드
- https://moon-seung-chan.tistory.com/13
- https://bebiangel.github.io/2019/11/24/http-guide-chap12/
- https://feel5ny.github.io/2019/11/23/HTTP_012_01/
- https://hamait.tistory.com/416
- https://docs.microsoft.com/en-us/aspnet/web-api/overview/security/basic-authentication
- https://ideveloper2.dev/blog/2019-11-23--%EA%B8%B0%EB%B3%B8-%EC%9D%B8%EC%A6%9D-%EB%8B%A4%EC%9D%B4%EC%A0%9C%EC%8A%A4%ED%8A%B8-%EC%9D%B8%EC%A6%9D/

QnA