웹서버 보안 방법

Date @August 5, 2021

유저 권한은 필요한 만큼

- 유관 부서 계정의 권한은 매우 제한적 → Read/Write 권한만 존재하기 때문에 시스템이나 DB에 영향을 미칠 수 없는 구조
- 기본적으로 root 유저로 프로세스를 실행해서는 안되고 사용하는 목적에 맞게 유저 권한을 분리해야 함

  → 목적에 맞게 유저 권한을 분리해야 한다.

  ⇒ 웹서버를 root 유저로 실행하면 해당 프로세스가 실행하는 명령을 모두 root권한으로 실행한다.

Privilege Escalation

- 낮은 권한을 가진 사용자에서 시작해서 높은 권한을 가진 사용자까지 권한을 높이는 공격 방법
- 주로 운영 체제의 보안 취약점을 이용한다. 흔히 '쉘 따기'라고 부른다.
- 오래된 운영 체제를 사용하고 있다면 너무나 쉽게 공격받을 수 있다.

  → 개발자 입장에서는 운영 체제를 최신화 하는 일이 매우 많지만 그냥 두게 되면 **잠재적 폭탄**

ACL(Access Control List)

- 접근 제어 목록
- 허용하는 IP에 대해서만 접근을 허용한다.
- inbound 뿐만 아니라 outbound도 중요하다.

  : inbound가 열려있고, 공격자가 심은 파일이 서버에서 동작한다고 하더라고 outbound만 제대로 막아두었다면 정보가 외부로 유출되지 않는다.

따라서 중요한 고객 데이터 은 사내에서도 허가 받은 IP로만 접근이 가능하도록 제한해야 한다.

실제로 회사에서도 특정 데이터에 접근하기 위해서는 사전에 신청하고 결재 후 접속 가능하다.

Ubuntu-ufw

```
sudo ufw status
```

- Uncomplicated FireWall (Complicated FireWall)
- BUT, SSAFY에서 서버 접속이 불가능해지는 원인 1위

  → 개발하는 개발자도 차단당할 수 있기 때문에 사용에 주의를 기울여야한다.

  ⇒ 보안이 중요한 서버라면 정해진 ip외에는 접속을 차단해야 함

인증(Authentication) 인가(Authorization)

1. 인증 : 유저가 누구인지 확인하는 절차

   → 클라이언트가 자신이 주장하는 사용자와 같은 사용자인가?
2. 인가 : 유저에 대한 권한을 허락하는 것

   → 클라이언트가 하고자 하는 작업이 해당 클라이언트에게 허가된 작업인가.

자주 실수하는 사례

- 유저 권한으로 로그인 한 후, 게시글 수정의 url을 수정해서 수정이 된다면...?!

  → 인증 완료 : 유저의 권한

  → 인가 실패 : 해당 유저가 작성한 글인지는 확인하지 않음