CSRF

크로스 사이트 요청 위조(CSRF)는 사용자가 의도하지 않은 요청을 악용하여 공격자가 특정 동작을 수행하도록 유도하는 공격이다. 사용자가 이미 인증된 상태로 웹 애플리케이션을 사용하고 있을 때 발생한다.

CSRF 공격의 작동 원리

1. **희생자의 인증**: 공격자는 희생자의 인증 정보(쿠키, 세션 등)를 얻지 않더라도 이미 로그인한 상태인 희생자를 대상으로 한다.
2. **공격자의 페이지**: 공격자는 악의적인 웹 페이지를 생성한다. 이 페이지에는 공격을 수행하는 스크립트가 포함되어 있다.
3. **피해자의 방문**: 희생자는 공격자의 페이지를 방문한다. 이 페이지에는 피해자가 의도하지 않은 요청을 트리거하는 스크립트가 삽입되어 있다.
4. **의도하지 않은 요청 실행**: 피해자가 악성 페이지를 방문하면, 브라우저는 피해자의 인증 정보를 함께 서버로 요청을 보낸다. 이 요청은 피해자가 아무런 조치를 취하지 않아도 자동으로 수행된다.
5. **공격 수행**: 서버는 피해자의 인증 정보를 가지고 있는 것으로 인식하여 요청을 처리한다. 이로써 공격자가 의도한 악성 동작(계정 변경, 금전 이체 등)이 수행될 수 있다.

CSRF 공격 보안 대책

1. **CSRF 토큰 사용**: 웹 애플리케이션에서는 사용자의 세션과 관련된 CSRF 토큰을 생성하여 사용해야 한다. 이 토큰은 요청을 보낼 때 함께 전송되어야 하며, 서버에서는 이 토큰을 검증하여 요청의 유효성을 확인한다.

2. **SameSite 쿠키 속성 설정**: SameSite 쿠키 속성을 설정하여 같은 도메인 내에서만 쿠키가 전송되도록 제한할 수 있다.
3. **Referrer 검증**: 요청을 보낸 페이지의 Referrer 값을 검증하여 외부 도메인에서 오는 요청을 차단할 수 있다.
4. **HTTP 요청 메서드 검증**: 중요한 동작(예: 로그아웃, 계정 삭제)은 GET 메서드로 요청을 처리하지 않도록 하고, POST나 PUT과 같은 안전한 메서드로만 처리하도록 해야 한다.
5. **사용자 인증 세션 관리**: 세션 관리 시 보안적인 취약점이 없도록 강화하고, 사용자 인증 정보를 안전하게 저장해야 한다.