분석 설계 SW 보안강화

3. 에러 처리

에러처리

예외처리

요구사항 분류	에러처리	요구사항번호	SR3-1
DBMS이름	예외처리		
설명	오류메시지에 중요정보(개인정보, 시스템 정보, 민감 정보 등)가 포함되어 출력되거나 에러 및 오류가 부적절하게 처리되어 의도치 않은 상황이 발생하는 것을 막기 위한 안전한 방안을 설계한다.		
요구사항내용	1. 명시적인 예외의 경우 예외처리 블록을 이용하여 예외발생시 수행해야 하는 기능이 구현되도록 해야 한다. 2. 런타임 예외의 경우 입력값의 범위를 체크하여 애플리케이션이 정상적으로 동작할 수 있는 값만 사용되도록 보장해야 한다.		

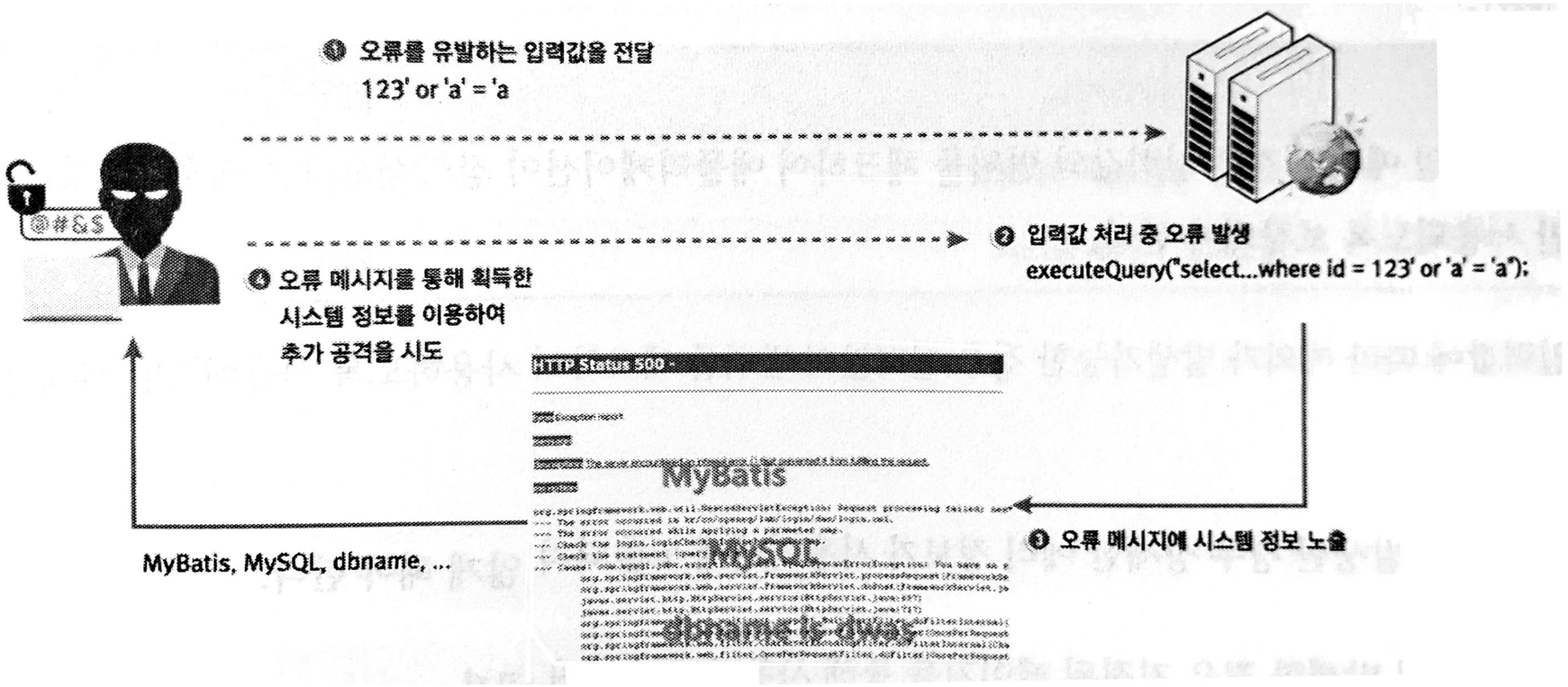
에러처리

예외처리

소프트웨어 보안

취약점 개요

- 사례 1 : 오류메시지를 통한 정보노출
  - ❖ 웹 서버에 별도의 에러 페이지를 설정하지 않은 경우, 에러 메시지를 통해 서버 데이터 정보 등 공격에 필요한 정보가 노출되는 취약점이다.



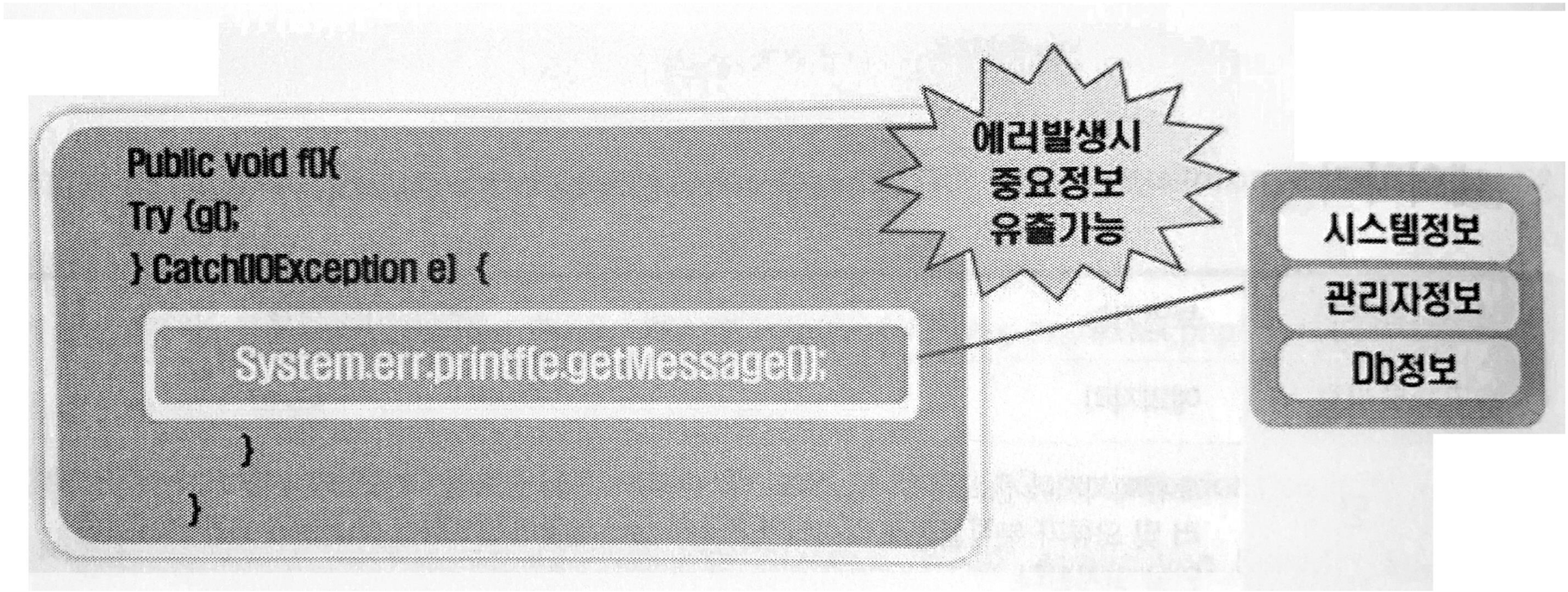
오류메시지를 통한 정보노출

에러처리

예외처리

취약점 개요

- 사례 2 : 시스템 정보노출
  - ❖ 시스템, 관리자, DB정보 등 시스템의 내부데이터가 공개되면, 공격자에게 또 다른 공격의 빌미를 제공하게 된다.



시스템 데이터 정보노출

에러처리

예외처리

설계시 고려사항

1. 명시적인 예외의 경우 예외처리 블록을 이용하여 예외발생시 수행해야 하는 기능이 구현되도록 해야 한다.
   - ❖ 각 프로그래밍 언어별 문법에 대한 안전한 사용방법을 기술하고 모든 개발자가 구현 단계에서 안전하게 예외처리를 할 수 있도록 시큐어코딩 규칙을 정의한다.

(예시) 자바 플랫폼 사용시

- 프로그램에서 발생된 에러 정보를 로깅하는 Logger API를 활용할 수 있도록 시큐어코딩 규칙을 정의한다.

에러처리

예외처리

설계시 고려사항

2. 런타임 예외의 경우 입력값의 범위를 체크하여 애플리케이션이 정상적으로 동작할 수 있는 값만 사용되도록 보장해야 한다.
   - ❖ 입력값에 따라 예외가 발생가능한 경우 입력값의 범위를 체크하여 사용하도록 시큐어코딩 규칙을 정의한다.

3. 에러가 발생한 경우 상세한 에러 정보가 사용자에게 노출되지 않게 해야 한다.
   - A. 에러가 발생한 경우 지정된 페이지를 통해 사용자게 에러 공지
     - ▪ 에러가 발생한 경우 프로그램 내에서 지정된 에러페이지로 리다이렉트 되도록 시큐어코딩 규칙을 정의하거나, 웹 애플리케이션 서버 설정을 통해 특정에러나 예외사항에 대해 지정된 페이지가 사용자에게 보여질 수 있도록 설계한다.
   - B. 사용자에게 보내지는 오류메시지에 중요정보가 포함되지 않도록 함.
     - ▪ 오류메시지에 중요정보(개인정보, 시스템정보, 민감정보 등)가 포함되지 않도록 시큐어코딩 규칙을 정의한다.

에러처리

예외처리

소프트웨어 보안

사고사례

‘오류 보고 메시지’, 해커의 정보 획득 수단?

[보안뉴스 김경애] 운영체제가 시스템 오류 발생, 하드웨어 변경 등의 상황을 마이크로소프트 서버로 전송하기 위해 생성하는 윈도우 보고 메시지가 악의적 목적을 가진 공격자의 정보 획득 수단이 될 수 있다는 가능성이 제기돼 주목되고 있다.

인터넷침해대응센터는 10일 윈도우 오류 발생 시 생성되는 오류 보고 메시지에는 사용자의 하드웨어 및 운영체제 정보 등의 사용자 정보가 포함되어 있다고 밝혔다.

윈도우 오류 보고는 시스템 충돌 발생 시 자동으로 생성되며, 사용자 동의하에 인터넷을 통해 해당 보고서를 마이크로소프트 서버로 전송할 수 있도록 구성된다. 보고서 내용에는 PC 모델명, PC ID, OS 버전, 문제를 유발시킨 프로그램명 등이 있다.

에러처리

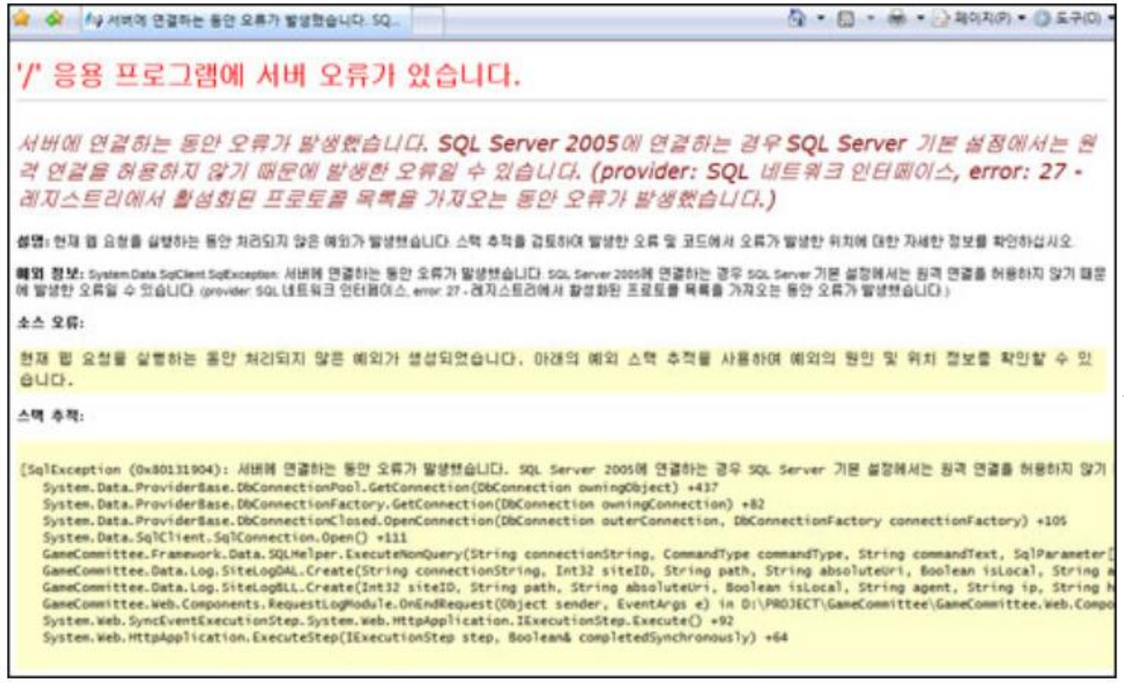
예외처리

소프트웨어 보안

사고사례

게임위 홈페이지 해킹시도 당해 하루 종일 '먹통'

정부산하 기관인 게임물등급위원회(이하 게임위)의 공식홈페이지가 해킹시도를 당해 서비스가 불가능한 상태인 것으로 확인 되었다.



게임위 홈페이지의 해킹시도로 인해 20일 개최 하기로 되어 있던 제 51차 등급심의회의가 열리지 못하고 22일로 연기 되었다. 게임위에서는 심의를 온라인으로도 받고 있기 때문에 금일 게임등급 신청을 하려고 예정했던 게임업체들의 등급심의가 늦어질 가능성이 있다.

사례의 오류페이지에서는 스택추적 정보가 포함되어 있다. 서버에 오류 또는 예외가 발생한 경우 위와 같이 예외이름이나 스택추적정보를 출력하도록 되어있다면 공격자가 프로그램 내부구조를 파악할 수 있기 때문에 공격자의 악성행위를 도울 수 있다는 위협이 발생한다.

분석 설계 SW 보안강화

4. 세션 통제

세션 통제

세션 통제

- 세션은 클라이언트와 서버의 논리적인 연결이다.
- 이미 연결이 종료된 클라이언트의 정보가 삭제되지 않고 사용가능한 상태로 방치되는 경우 해당 연결을 탈취한 허가되지 않은 사용자에 의해 시스템의 기능이 사용되거나 다른 개인의 중요정보에 접근하는 침해사고를 발생시킬 수 있으므로 안전한 세션 통제 정책이 적용되어야 한다.
- 또한 사용자를 구분하기 위한 세션 ID를 안전하게 관리하지 않으면 세션하이재킹과 같은 공격으로 허가되지 않은 사용자가 시스템을 사용할 수 있게 되므로 반드시 안전하게 관리해야 한다.

세션 통제

세션 통제

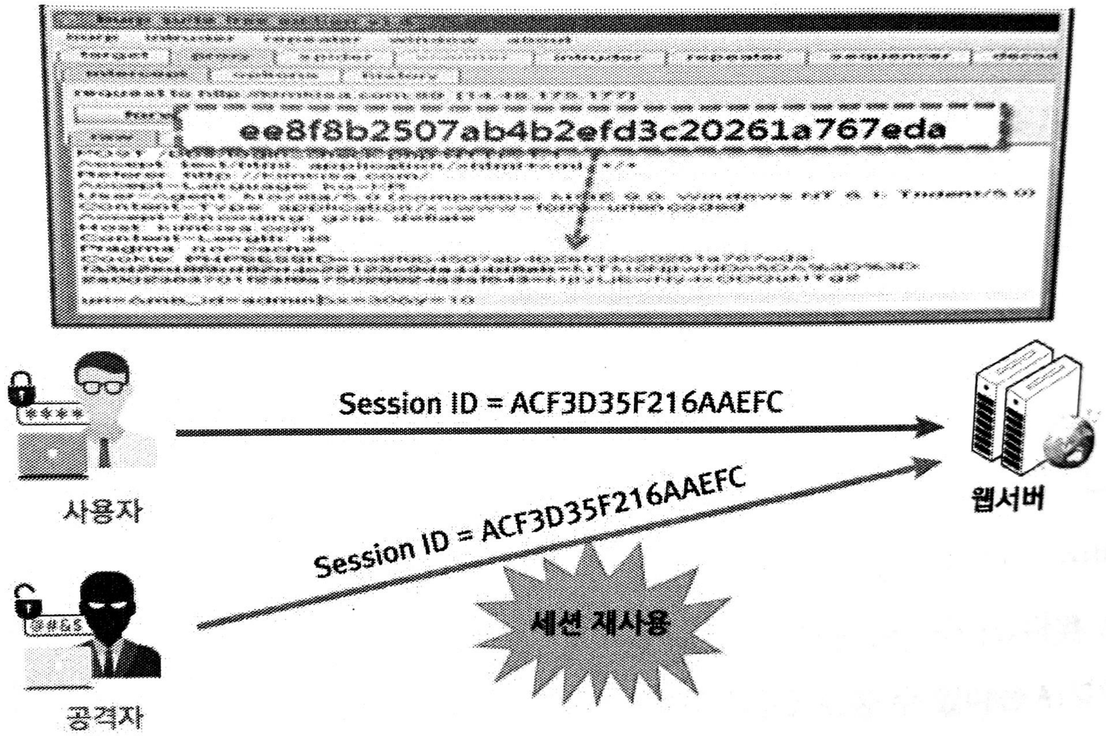
요구사항 분류	세션 통제	요구사항번호	SR4-1
DBMS이름	세션 통제		
설명	다른 세션간 데이터 공유금지, 세션 ID 노출금지, (재)로그인시 세션 ID 변경, 세션종료(비활성화, 유효기간 등) 처리 등 세션을 안전하게 관리할 수 있는 방안을 설계해야 한다.		
요구사항내용	1. 세션간 데이터가 공유되지 않도록 설계해야 한다. 2. 세션이 안전하게 관리되도록 해야 한다. 3. 세션 ID가 안전하게 관리되도록 해야 한다.		

에러처리

예외처리

취약점 개요

- 사례 1 : 불충분한 세션 관리
  - ❖ 인증시 일정한 규칙이 존재하는 세션 ID가 발급되거나 세션 타임아웃을 너무 길게 설정한 경우 공격자에 의해 사용자 권한이 도용될 수 있는 취약점이다.



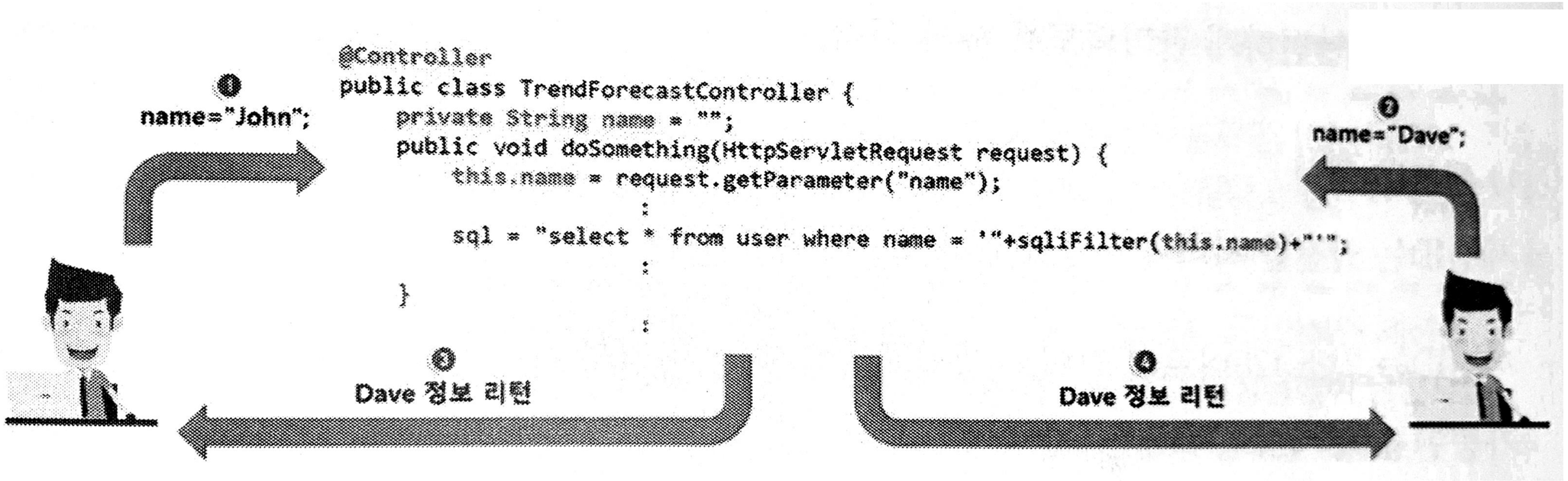
불충분한 세션관리

에러처리

예외처리

취약점 개요

- 사례 2 : 잘못된 세션에 의한 정보노출
  - ❖ 다중 스레드 환경에서는 싱글톤(Singleton)객체 필드에 경쟁조건 발생할 수 있다. 따라서 다중 스레드 환경인 java의 서블릿 등에서는 정보를 저장하는 멤버변수가 포함되지 않도록 하여, 서로 다른 세션 간에 데이터를 공유하지 않도록 해야한다.



잘못된 세션에 의한 데이터 정보노출

설계시 고려사항

1. 세션 간 데이터가 공유되지 않도록 설계해야 한다.
   - ❖ 스레드로 동작하는웹 애플리케이션의 컨트롤러 컴포넌트나, 싱글톤 객체로 생성되는 서비스 컴포넌트를 설계하는 경우 클래스 멤버 변수나 클래스변수는 세션 간에 공유되는 데이터가 되므로 클래스 설계시 읽고 쓰기가 가능한 변수를 사용하지 않도록 설계해야 한다.

에러처리

예외처리

설계시 고려사항

2. 세션이 안전하게 관리 되도록 설계해야 한다.
   - 시스템 내의 모든 페이지에서 로그아웃이 가능하도록 UI를 설계하고, 로그아웃을 요청하면 사용자에게 할당된 세션을 완전히 제거하는 API를 사용하도록 시큐어코딩 규칙을 정의한다. 예를 들어, Java의 경우 session.invalidate() 메서드를 사용하여 세션에 저장된 정보를 완전히 제거할 수 있다.
   - 세션 타임아웃 시간은 중요기능의 경우 2~5분, 위험도가 낮은 애플리케이션의 경우에는 15~30분으로 설정하고, 이전 세션이 종료되지 않은 상태에서 새로운 세션이 생성되지 않도록 해야 한다.
   - 웹 브라우저 종료로 인한 세션종료는 서버 측에서 인지할 수 없기 때문에 일정시간 동안 사용되지 않는 세션 정보는 강제적으로 삭제되도록 설정한다.
   - 중복로그인을 허용하지 않는 경우, 새로운 로그인 세션 생성시 이전에 생성된 로그인세션을 종료하거나, 새로 연결되는 세션을 종료하도록 하는 정책이 설계 단계에 고려되어야 한다.
   - 세션 ID가 포함된 쿠키에 대해 HttpOnly 속성을 설정하여 자바스크립트로 조회할 수 없도록 만들어 XSS공격에 대응하도록 설계한다.
   - 사용자가 패스워드를 변경하는 경우 현재 활성화된 세션을 삭제하고 다시 할당한다.

설계시 고려사항

3. 세션 ID가 안전하게 관리도록 해야 한다.

   A. 세션 ID 생성

   - 세션 ID는 안전한 서버에서 생성해서 사용되어야 한다.
   - 세션 ID는 최소 128비트의 길이로 생성되어야 하며, 안전한 난수 알고리즘을 적용하여 예측이 불가능한 값이 사용되어야 한다.

   B. 세션 ID 사용

   - URL Rewrite 기능을 사용하는 경우 세션 ID가 URL에 노출될 수 있으므로, 사용하지 않도록 설계한다.

   C. 세션 ID 폐기

   - 로그인 성공시 로그인 전에 할당받은 세션 ID는 파기하고 새로운 값으로 재할당하여 세션 ID 고정공격에 대응하도록 시큐어 코딩 규칙을 정의한다.
   - 장기간 접속되어 있는 경우 세션 ID의 노출위험이 커지므로, 일정시간 주기적으로 세션 ID를 재할당 하도록 설계한다.

에러처리

예외처리

소프트웨어 보안

사고사례

온라인 뱅킹시 하이재킹 시도 맬웨어 발견 주의!

[보안뉴스 권 준] 개인이 온라인 뱅킹 거래를 위해 사용자 계정에 로그인 했을 때 망 환경에서 사용자 간 또는 컴퓨터 간의 대화를 위한 연결과정인 세션을 하이재킹 하는 사례가 발견돼 주의가 요구된다고 영국 IT 전문 뉴스 사이트인 The Register 지가 보도했다.

'Shylock'라고 명명된 이 맬웨어는 온라인 뱅킹 고객을 대상으로 고객이 계정을 로그인하면 세션을 하이재킹 할 수 있다. 이 맬웨어를 통해 공격자는 실시간 채팅 창을 열고 은행 고객상담센터 담당자인 것처럼 속여 고객에게 세션이 보류됐다고 알린 후, 실시간 채팅을 통해 고객들의 정보를 빼내는 수법을 사용한 것으로 알려졌다.

세션이 다시 진행되기 위해서는 고객 정보를 알아야 한다고 속인 다음, 고객의 계좌정보 등을 탈취하고 이를 통해 고객의 계좌로부터 자금을 빼돌렸던 것,

국내에서도 온라인 뱅킹 거래 비중이 매우 크기 때문에 이러한 맬웨어를 통한 계좌정보 탈취 가능성에도 대비할 필요가 있다는 게 보안전문가들의 지적이다.