웹 애플리케이션의 접근 제어 취약점에 대한 자동 탐지 기법

송호길

2011 ROSAEC

June 26, 2011

PLASSE RESEARCH

목차

1. 목차
2. 접근 제어
3. 취약점 탐지 방법
4. 취약점 탐지 자동화

PLASSE RESEARCH

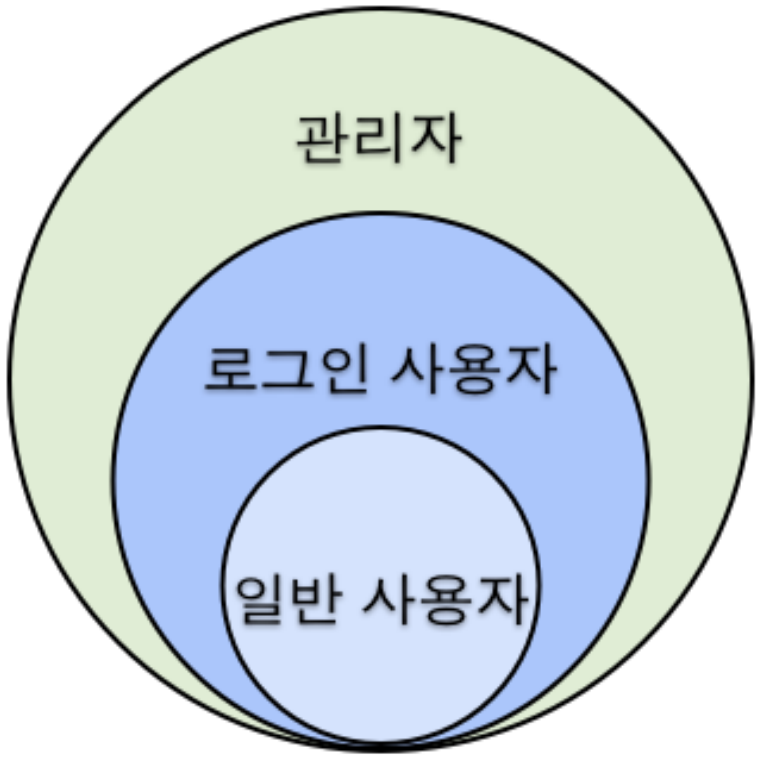
접근 제어?

- 애플리케이션은 사용자가 해서는 안될 행동에 대해 정의
- 민감한 자원에 대한 사용자의 요청이 합법적인지 검증
- 애플리케이션의 중요한 자원을 보호하기 위해 필요

PLASSE RESEARCH

수직적 접근 제어

- 애플리케이션 기능에 따라 사용자의 접근을 허용할지 결정
- 사용자 계층 별로 권한을 분리하는 방식

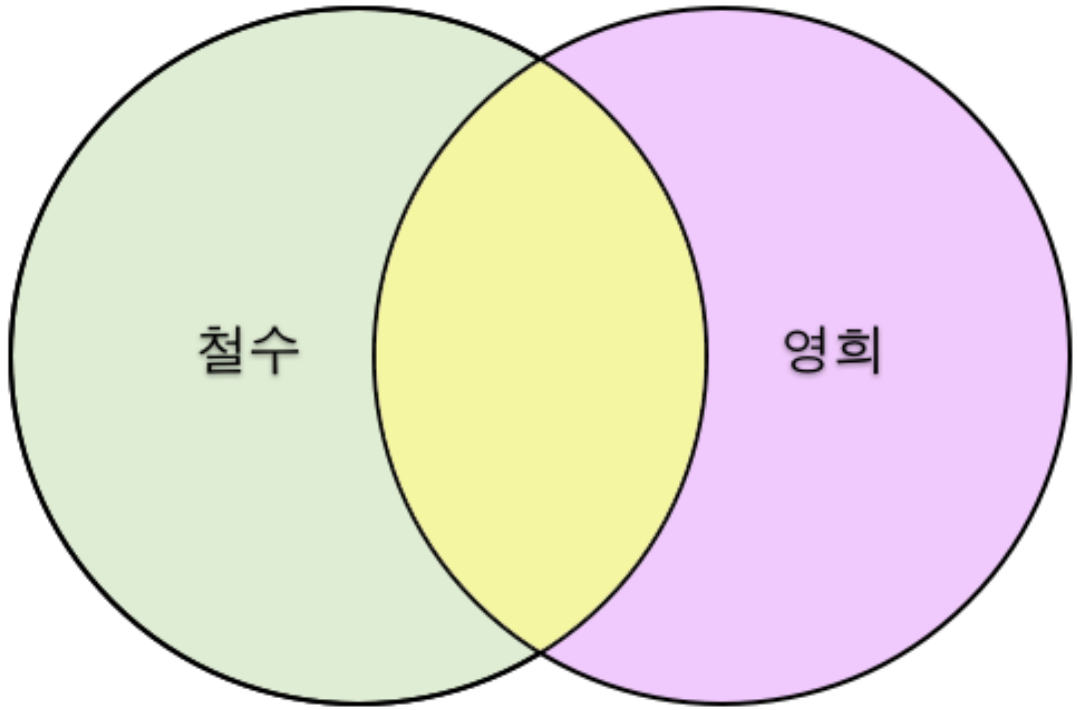


수직적 권한 구조

PLASSE RESEARCH

수평적 접근 제어

- 동일한 형태의 자원에 접근할 수 있는 규칙을 사용자 별로 제공



수평적 권한 구조

PLASSE RESEARCH

취약 탐지 방법

관리자 URL

https://sample-url.com/admin/
https://sample-url.com/secure/44t/DoAdminPage3.jsp

클라이언트 측 자바스크립트

```
if(isAdmin) {
   adminMenu.addItem("/secure/44t/addNewMember.jsp","create a new user")
}
```

PLASSE RESEARCH

취약점 탐지 방법

식별자

https://sample-url.com/ModifyDoc.php?id=19850808

정적인 자원

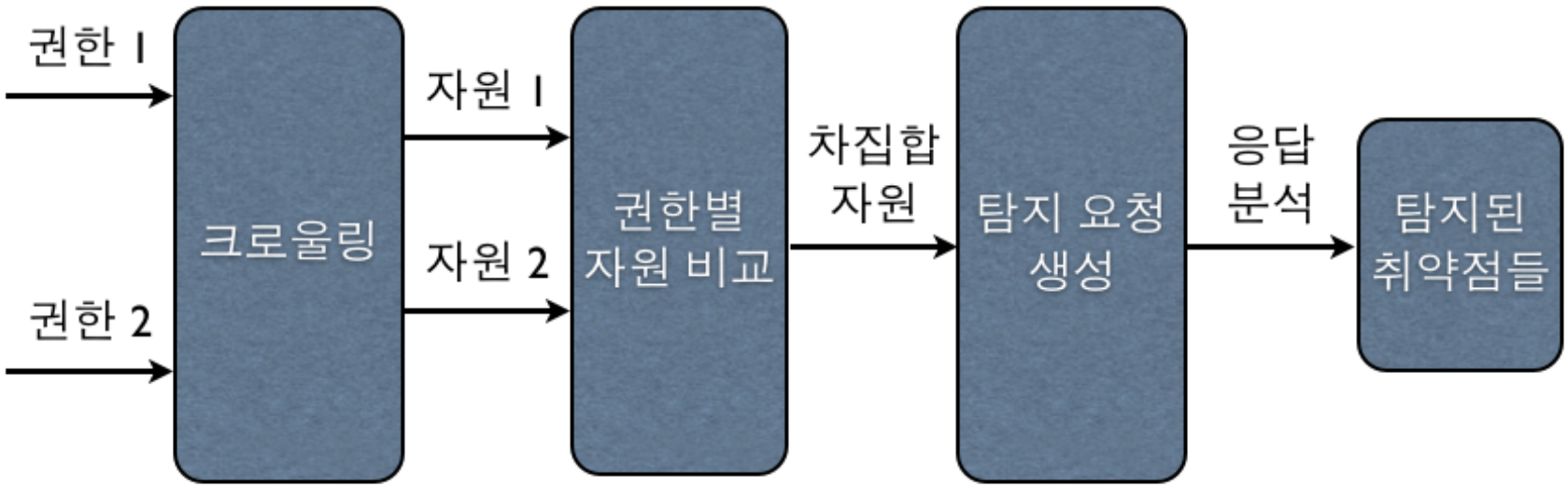
https://sample-url.com/download/19850808.pdf

요청하는 변수

https://sample-url.com/login/memberlist.jsp?admin=true

PLASSE RESEARCH

취약점 탐지 자동화



PLASSE RESEARCH

취약점 탐지 자동화

- 서로 다른 권한의 두 사용자로 웹 애플리케이션의 자원 수집
  - 관리자 URL, 식별자, 요청 변수 수집 용이
- 숨겨진 자원 분석을 통한 숨겨진 자원도 수집
  - 폼 분석, 숨겨진 필드 분석
- 구조화된 자원들을 분석하여 서로에 대한 차집합을 도출
- 차집합에 해당되는 조작된 요청을 보내 응답을 통해 취약점 탐지

PLASSE RESEARCH