PL (상)	위치 공개
취약점 개요	
점검목적	■ 공격자가 폴더의 위치를 예측하여 파일 및 정보 획득을 방지하고자 함
보안위협	■ 폴더나 파일명의 위치가 예측 가능하여 쉽게 노출될 경우 공격자는 이를 악용하여 대상에 대한 정보를 획득하고 민감한 데이터에 접근 가능
참고	·
조치방법	웹 루트 디렉터리 이하 모든 불필요한 파일 및 샘플 페이지 삭제

보안설정 방법

* robots.txt 파일 작성을 통해 검색 차단할 디렉터리, 확장자, 페이지 등을 지정할 수 있으며 HTML의 HEAD 태그 내에 META 태그를 추가하여 검색엔진의 인덱싱을 차단
* 웹 디렉터리를 조사하여 아래의 삭제해야 할 파일 확장자에 포함된 백업 파일을 모두 삭제하고, *.txt 확장자와 같이 작업 중 생성된 일반 텍스트 파일이나 이미지 파일 등도 제거함

※ 삭제해야 할 파일 확장자 예시

*.bak	*.backup	*.org	*.old	*.new	*.txt
*.zip	*.log	*.!	*.sql	*.tmp	*.temp

* 백업 파일은 백업 계획을 수립하여 안전한 곳에 정기적으로 백업해야 하며 웹 서버에서는 운영에 필요한 최소한의 파일만을 생성하여야 함
* 웹 서버 설정 후 디폴트 페이지와 디폴트 디렉터리 및 Banner를 삭제하여 Banner Grab에 의한 시스템 정보 유출을 차단함
* Apache, IIS, Tomcat 등 각 웹 서버 설정 시 함께 제공되는 샘플 디렉터리 및 매뉴얼 디렉터리, 샘플 애플리케이션을 삭제하여 보안 위험을 최소화함