


PT (상)	경로 추적
취약점 개요	
점검목적	<ul style="list-style-type: none"> <li>■ 웹 서버 또는 웹 애플리케이션의 중요한 파일과 데이터의 접근 및 실행을 방지하고자 함</li> </ul>
보안위협	<ul style="list-style-type: none"> <li>■ 웹 서버와 웹 애플리케이션의 파일 또는 디렉터리 접근이 통제되지 않아 웹 서버 또는 웹 애플리케이션의 중요한 파일과 데이터에 접근을 허용하는 취약점으로 웹 루트 디렉터리에서 외부의 파일까지 접근하여 이를 실행할 수 있음</li> </ul>
참고	※ 소스코드 및 취약점 점검 필요
조치방법	사용자가 임의로 접근할 수 있는 최상위 디렉터리를 웹 루트 디렉터리로 설정하여 웹 서버의 시스템 루트 디렉터리로 접근하지 못하게 제한
보안설정 방법	
<p>* 웹 사이트에서 접근하려는 파일이 있는 디렉터리에 chroot 환경 적용 시 경로 추적 공격을 최소화할 수 있음</p> <p>※ chroot 디렉터리는 해당 디렉터리가 루트처럼 다뤄짐. chroot 파일 시스템은 대부분의 유닉스를 기반으로 한 플랫폼에서 지원 가능하며, 윈도우 플랫폼에서는 적절한 시작 디렉터리를 새로운 논리 드라이브로 만들어 웹 사이트에서 해당 드라이브를 통하여 접근하게 함 (예: 웹 사이트의 최상위 디렉터리를 웹 루트 디렉터리로 제한)</p> <p>■ IIS</p> <p>인터넷 정보서비스(IIS) 관리&gt; [해당 웹 사이트]&gt; [속성]&gt; [홈 디렉터리]탭&gt; [구성] 버튼 선택&gt; [옵션] 탭에서 [부모 경로 사용] 체크 해제</p>  <p>* 애플리케이션 소스 파일을 수정하여 파일 내용을 웹 브라우저에 표시할 수 있는 디렉터를 특정 디렉터리로 한정하고 이 외의 다른 디렉터리에서는 파일 내용을 표시할 수 없도록 설정해야 함</p> <p>* PHP를 사용하는 경우 php.ini 에서 magic_quotes_gpc를 On으로 설정하여 .₩./ 와 같은 역 슬러시 문자 입력 시 치환되도록 설정</p> <p>* 웹 사이트에서 사용되는 파라미터 값 대상으로 특수 문자를 필터링하도록 웹 방화벽 룰셋 적용</p>	