디렉터리 노출

대부분의 취약점은 프로그램의 오류로 인해 발생되는 문제점이나 디렉토리 노출만은 웹서버 설정 오류로 인해 발생되는 취약점이다.

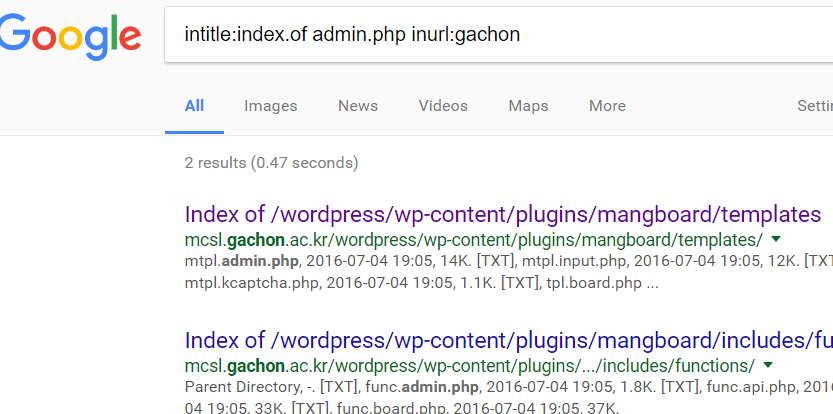
웹 서버 별 설정오류와 그에 따른 디렉토리 노출

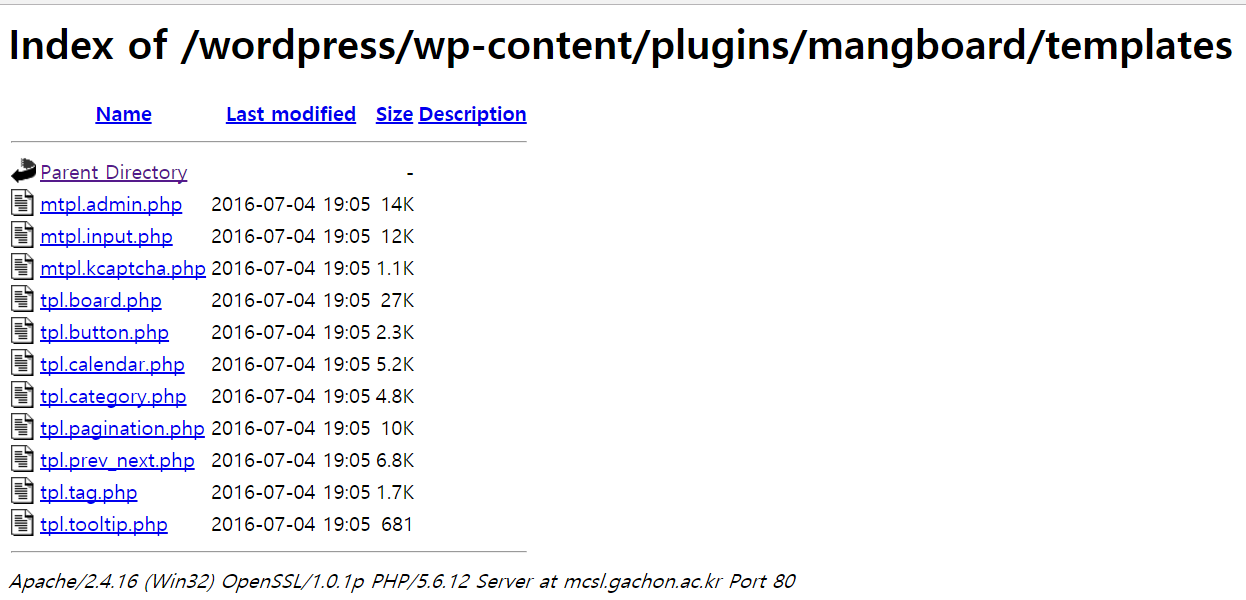
1. IIS(마이크로 소프트 인터넷 서비스)

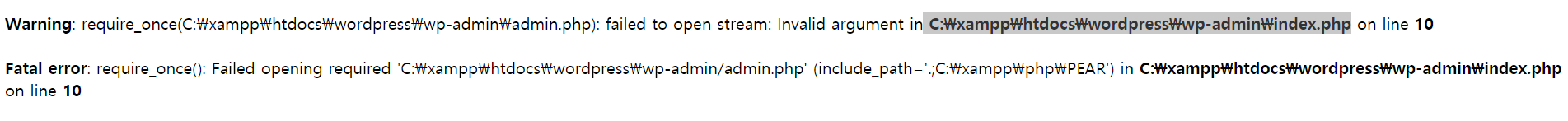
IIS는 마이크로소프트 윈도우를 사용하는 서버들을 위한 인터넷 기반 서비스들의 모임들로 HTTP,HTTPS,FTP,SMTP 서비스를 지원하고 있다.

디렉터리 노출은 디렉터리 검색(B) 부분이 체크 되어있는 경우 발생됨.

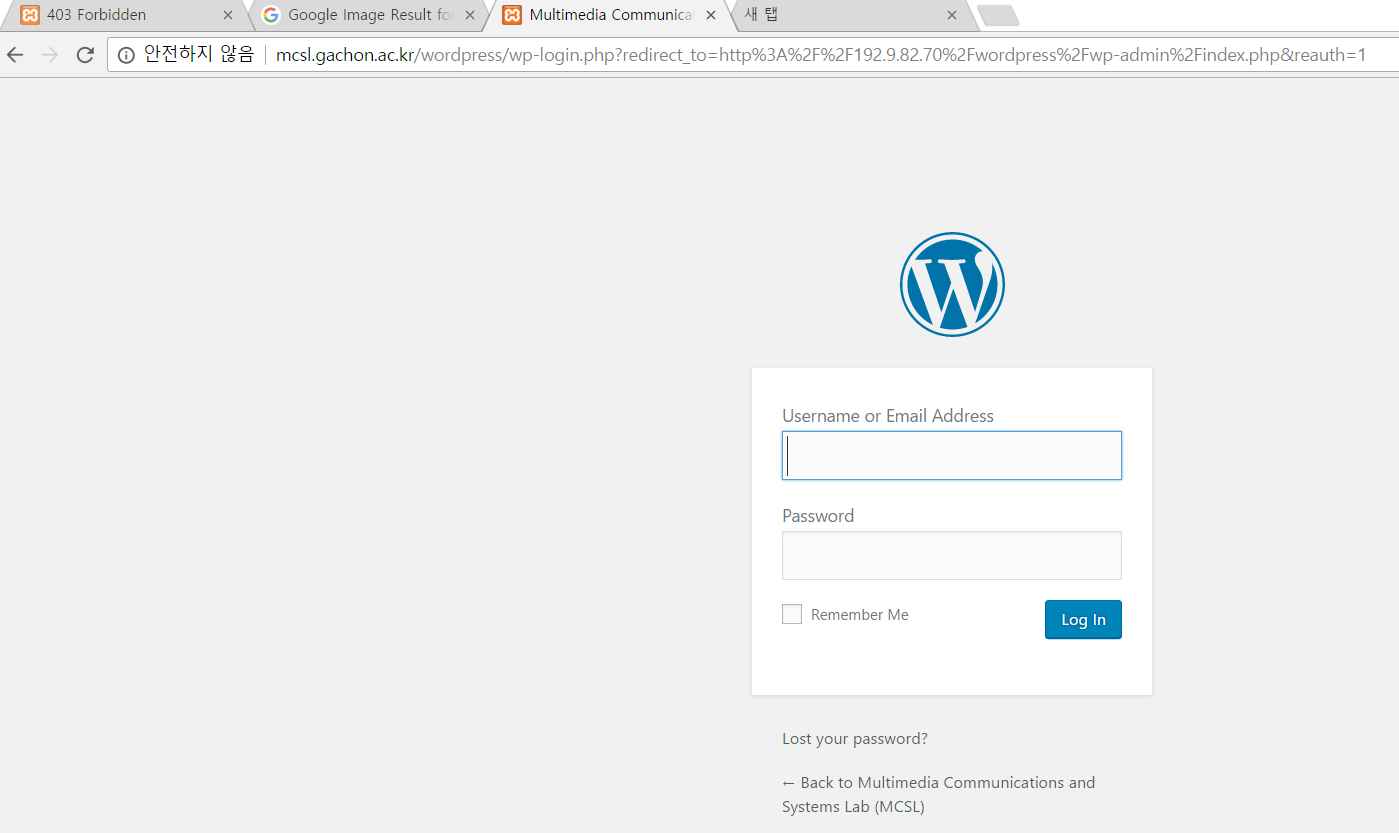
[제어판]- 관리도구-인터넷 정보 서비스(IIS 관리) 메뉴에서 인터넷 정보 서비스 – 웹사이트 – 설정할 사이트 에서 오른쪽버튼을 클릭하여 속성부분을 보면 설정 사항을 볼 수 있고 취약점 발생시 To parent Directory 라는 키워드를 볼 수 있다.



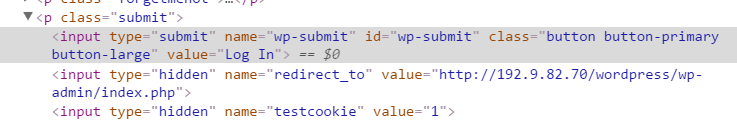








<http://192.9.82.70/wordpress/wp-admin/>



1. 탐켓

아파치 톰켓은 아파치 소프트웨어 재단에서 개발된 서블릿 컨테이너 혹은 웹 컨테이너만 있는 웹 어플리케이션 서버이다.

서블릿: jsp같은 파일들이 서블릿으로 변환되서 서블릿 컨테이너안에서 동작하며 서비스를함.

톰켓은 웹 서버와 연동하여 실행할 수 있는 자바 환경을 제공하여 자바 서버 페이지 와 자바 서블릿이 실행할 수 있는 환경을 제공하고 있다.

톰켓의 설정 파일은 conf/web.xml 이며

<init-param>

<param-name>listings</param-name>

<param-name>true</param-name>

</init-param>

이렇게 true로 설정되어있는경우 디렉터리 노출 취약점이 발생된다. 취약점발생시

“Directory Listing For”이라는 내용을 볼 수 있다.

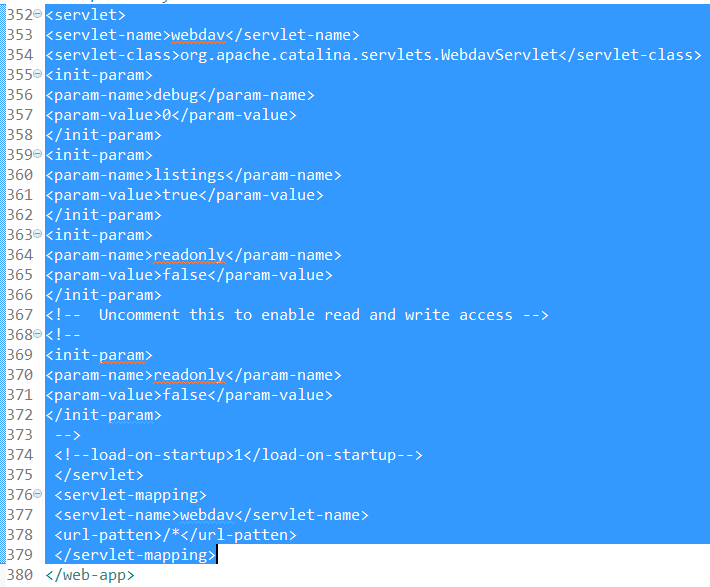
1. 아파치

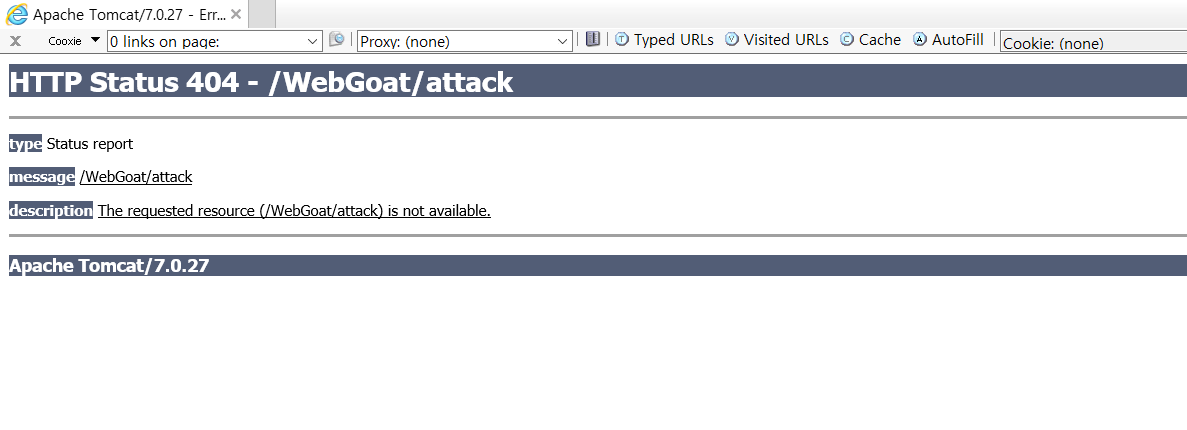
아파치 소프트웨어 재단에서 관리하는 HTTP 웹 서버를 말하며 유닉스 윈도우를 비롯해 거의 모든 운영체제와 시스템에서 운용이 가능하다.

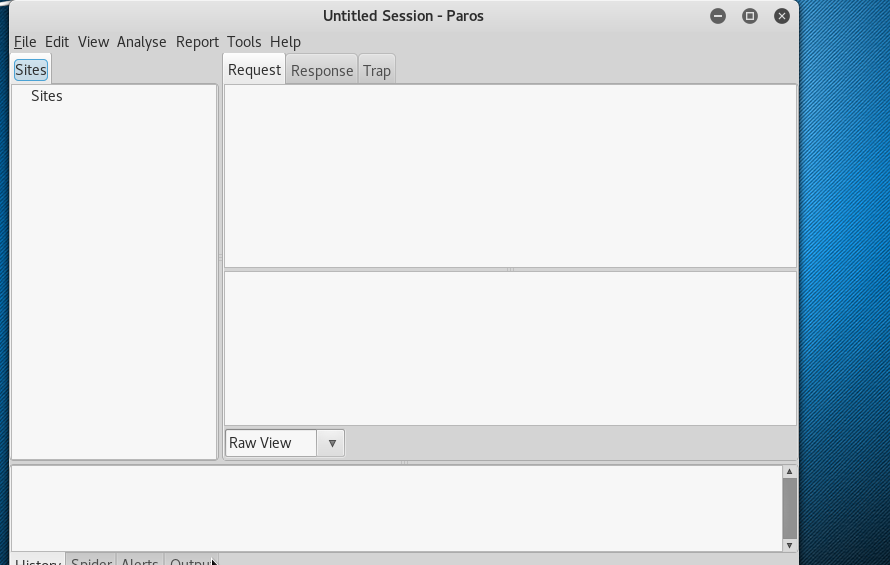
환경설정 파일은 httpd.conf 이며 특정 디렉터리에 대해 Indexes로 설정 시에 디렉터리 취약점이 발생된다.

파일삽입 취약점

HTTP PUT 메서드 악용







실패..ㅎ…392pg