



Directory Listing

2019.07.24 HACKDUN



INDEX

● 01. Directory Listing이란 ?

● 02. 해킹 시나리오

● 03. 실습

● 04. 방어 방법





01 Directory Listing이란 ?

WAS의 환경 설정 미흡으로 웹 디렉토리 호출 시 해당 WAS의
디렉토리 목록이 외부에 노출되는 취약점



위험도 ?

1. 브라우징하는 모든 파일을 보여줌
2. 백업파일 및 소스코드, 스크립트 파일의 유출로 인해 계정 정보가 유출 가능함



공격 방법 ?

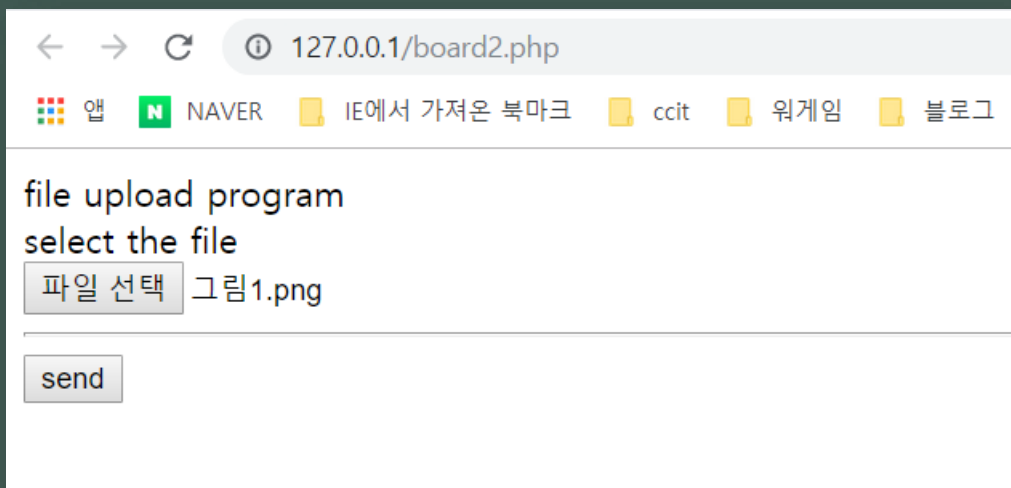
1. 이미지 파일 등 경로를 알 수 있을 때, URL 부분에 파일명을 지우고 입력하면
파일 리스트를 볼 수 있음
2. 무작위로 많이 사용되는 디렉토리명 대입
ex) `http://nxxxxx.com/upload` 등



★ 해킹 시나리오

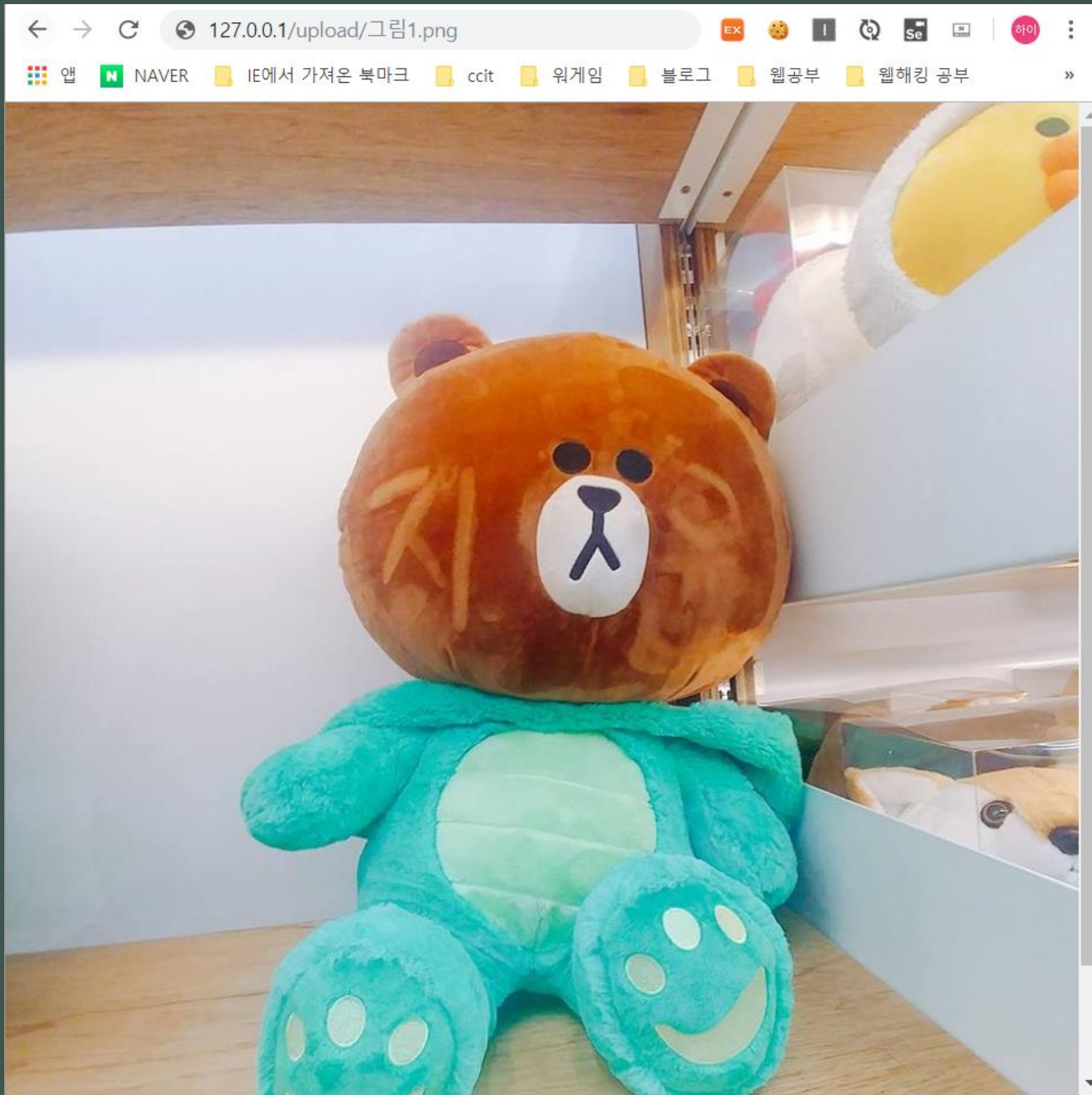
1. 웹페이지에서 파일을 업로드 해본 뒤 경로를 확인
2. 경로에서 파일명을 지우고 다시 엔터
3. 끝!!!!!!!





웹 페이지에서 파일 업로드를 한다!





업로드 된 파일의 경로 확인

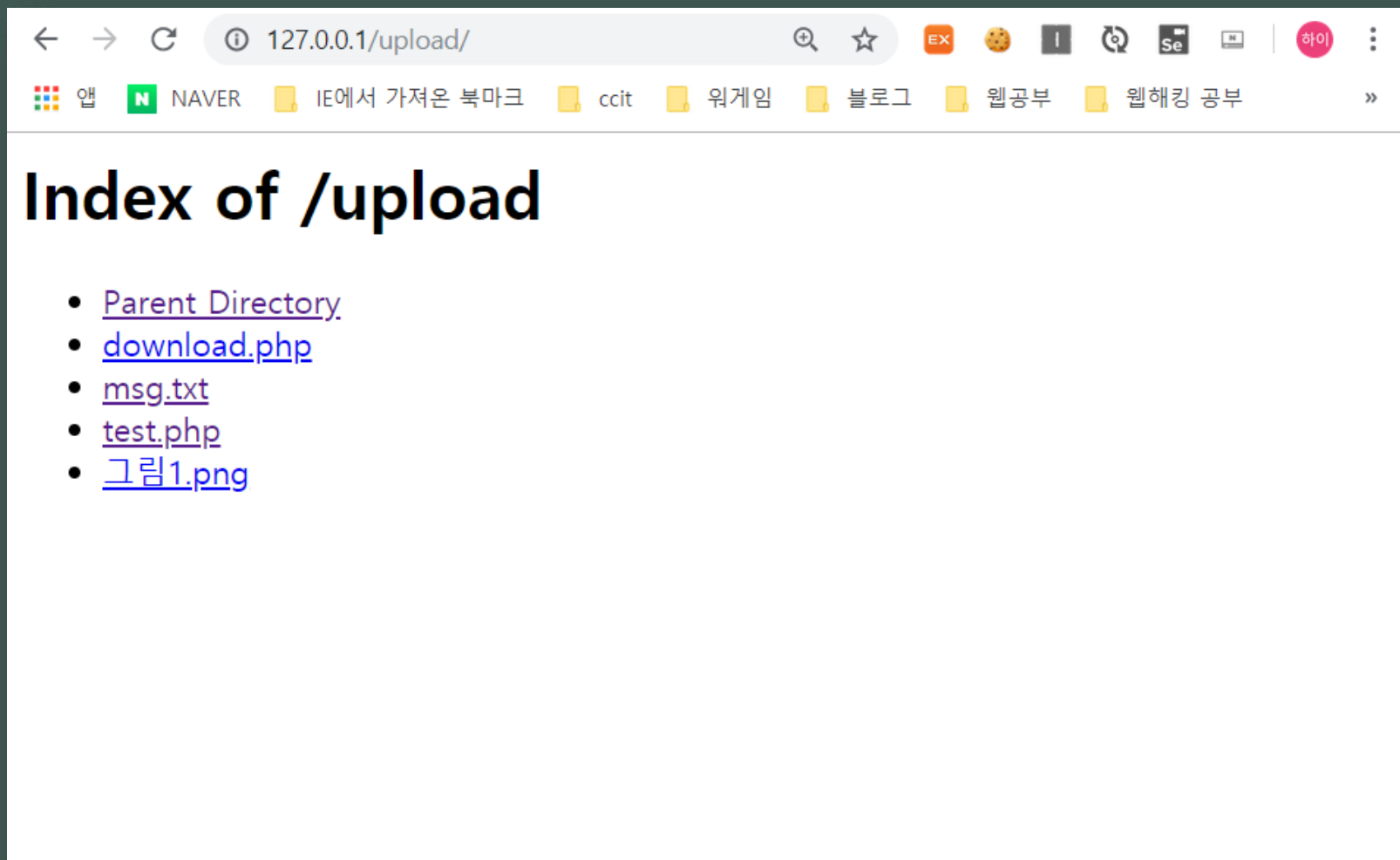
127.0.0.1/upload/그림1.png

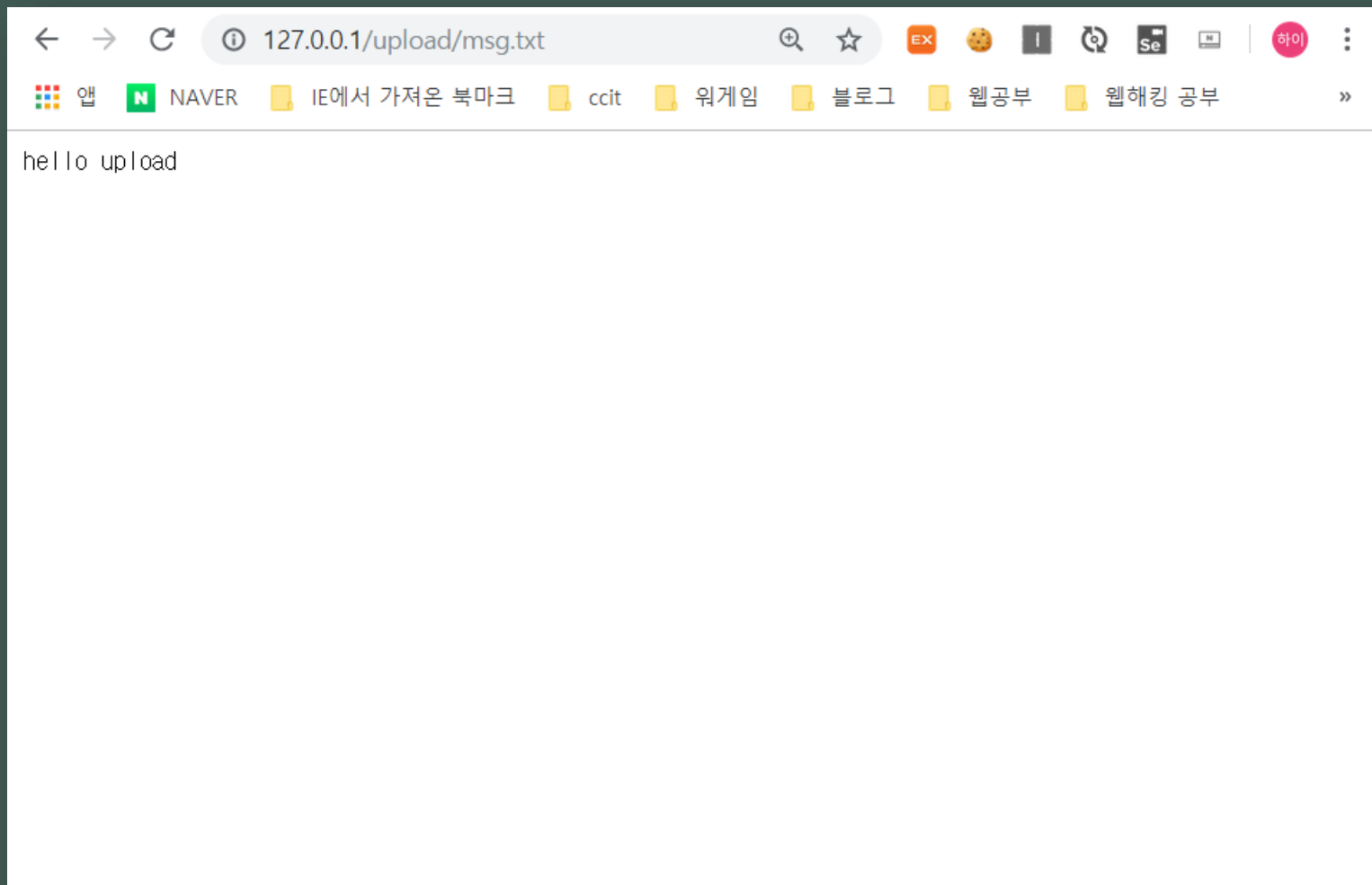


확인된 경로에서 파일명을 지우고 다시 엔터를 누르면 ?



Directory Listing 발생!





내용을 확인할 수도 있음



이렇게 디렉토리 노출 취약점은 브라우징하는 모든 파일명이 노출되므로 매우 위험한 취약점임

그래서 최근에는 대부분 해당 기능을 사용하지 않음 ㅎㅎ...



★꿀팁★

구글링으로도 Directory Listing 취약점을 찾을 수 있음

1. `site:[취약점 진단 도메인] intext:"parent directory"`
2. `site:[취약점 진단 도메인] intext:"index of"`



★ 방어 방법

★ 서버의 설정을 변경해서 기본 페이지가 없을 경우 디렉토리 목록이 노출되지 않게 함 ★

아파치 웹 서버라면 ?

Httpd.conf 내용 중 Options 항목 뒤에 Indexes 단어를 삭제

Options Indexes FollowSymLinks MultiViews



Options -Indexes FollowSymLinks MultiViews

Thank You ★ ●

감사합니다.

