컴퓨터보안
실습 02

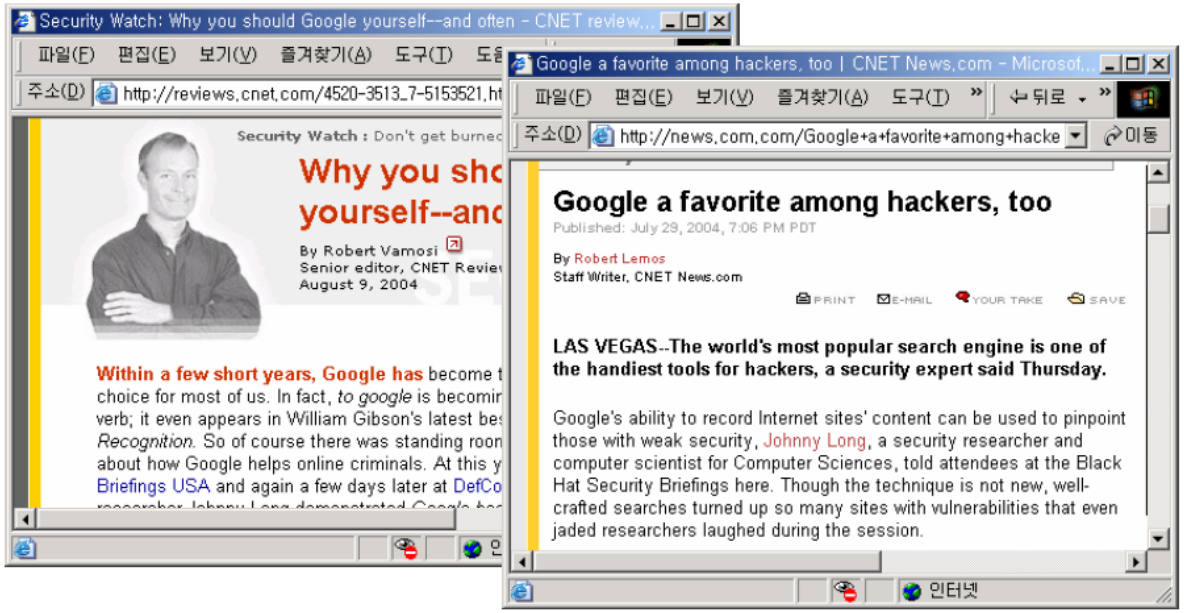
3주차

Googledork

- 구글의 위험성

전세계적으로 구글 검색이 범죄에 이용되고 있음.

가장 대중적인 해킹 도구로 인식되고 있음.



Googledork

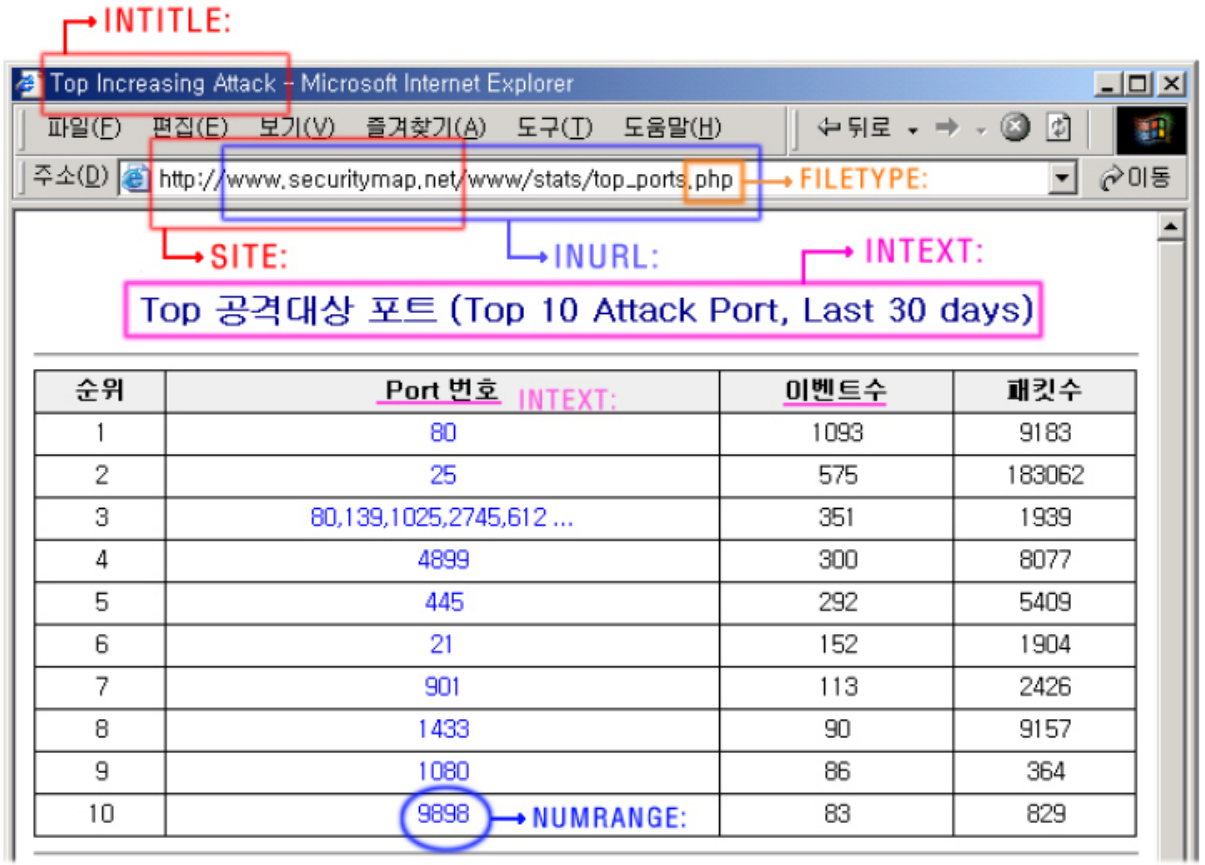
- 실습 후 제출
  - 실습 화면 캡쳐
  - 분석 : 공격을 통해 파악할 수 있는 정보 **(캡쳐x)**
    - **Ex) ooo** 명령을 통해 패스워드, 고객주소, 핸드폰 번호등을 알수있었음
    - **Ex2) ooooo** 소스코드를 통해 **ooo**에 취약함
    - **Ex3) ooo** 명령을 방어할 수 있는 방안
  - 압축해서 제출바랍니다.
- 제출 메일주소 : **kor_moon@naver.com**

Googledork

- 옵션

다양한 검색 옵션으로 사용자가 원하는 결과를 보다 정확하게 검색

기타 검색옵션
allintitle:
allinurl:
link:
daterange:
define:
phonebook:
related:
"Strings"



Googledork

- 옵션

❖ (+) 성격이 비슷한 문자를 포함하여 검색

filetype:eml eml +intext: “Subject” +intext: “From” +intext: “To”

❖ (-) 검색 결과에서 제외

filetype:conf inurl:firewall -intitle:cvs

❖ (“ ”) 완전한 문구 포함

“#mysql dump” filetype:sql

❖ (.) 적어도 한 단어를 포함한 모든 단어 검색

intitle:index.of. sites.ini

❖ (*) 모든 단어 검색

filetype:cfg mrtg “target[*]” -sample -cvs –example

❖ (|) 또는(OR)

filetype:bak inurl: “htaccess|passwd|shadow|htusers”

Googledork

- 해킹 기초

  단어나 문장을 활용한 검색 기능 이외에 상세 옵션을 줄 수 있음.

  다중 옵션을 제공하여 검색 결과를 세부적으로 필터링 가능.

  검색 옵션은 소문자이며 검색문자열 사이에 빈 공간이 없어야 함.

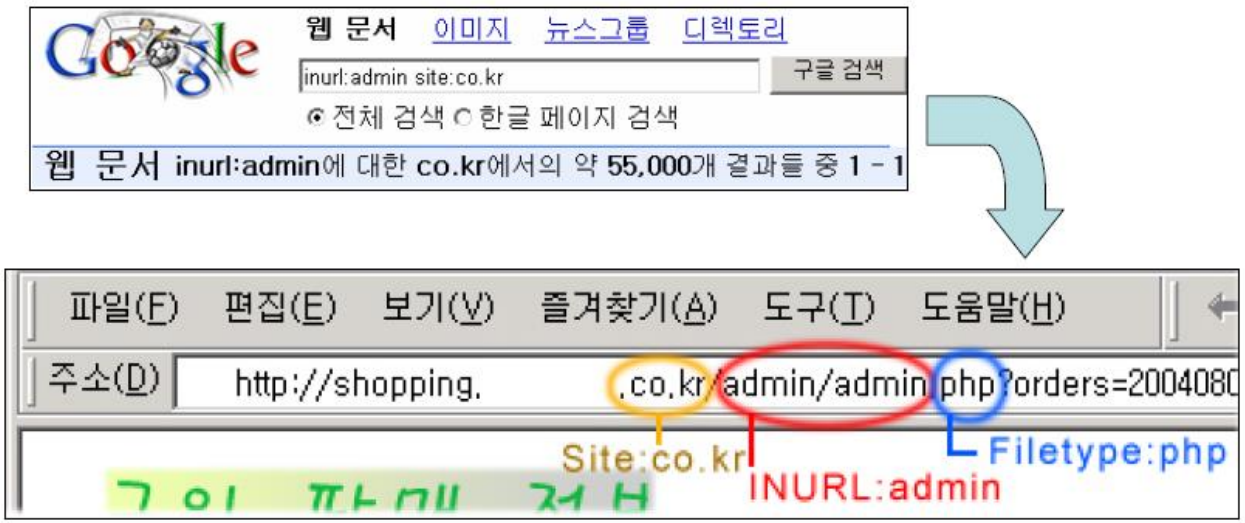
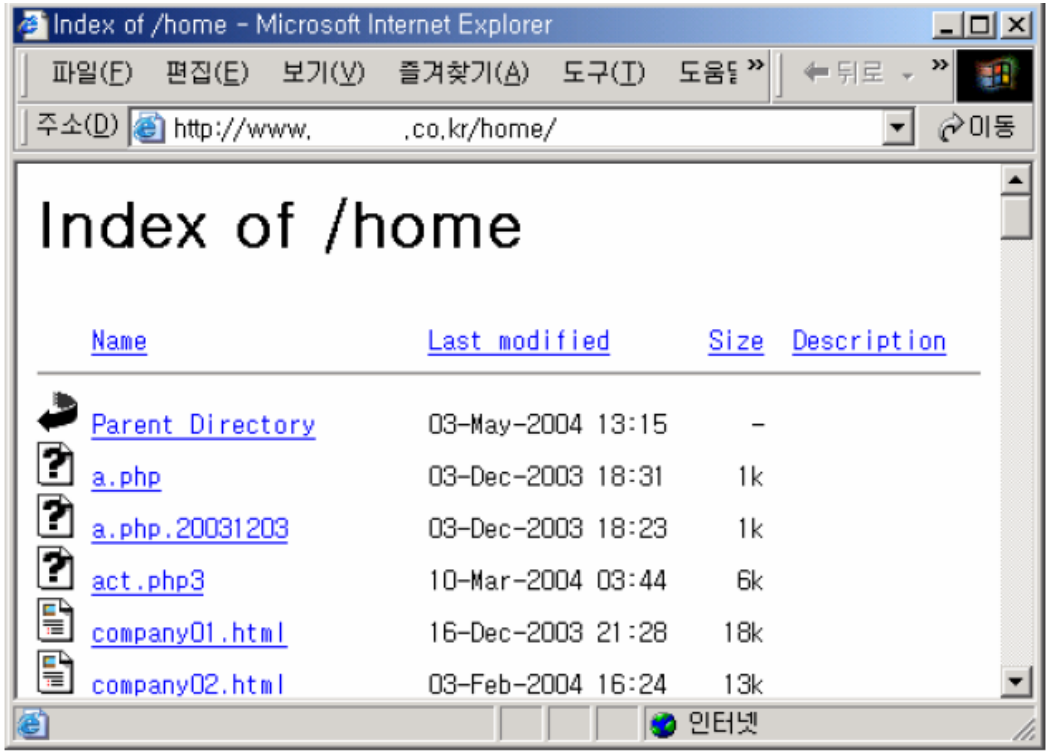


그림. 관리자 페이지의 주문 판매 정보 검색

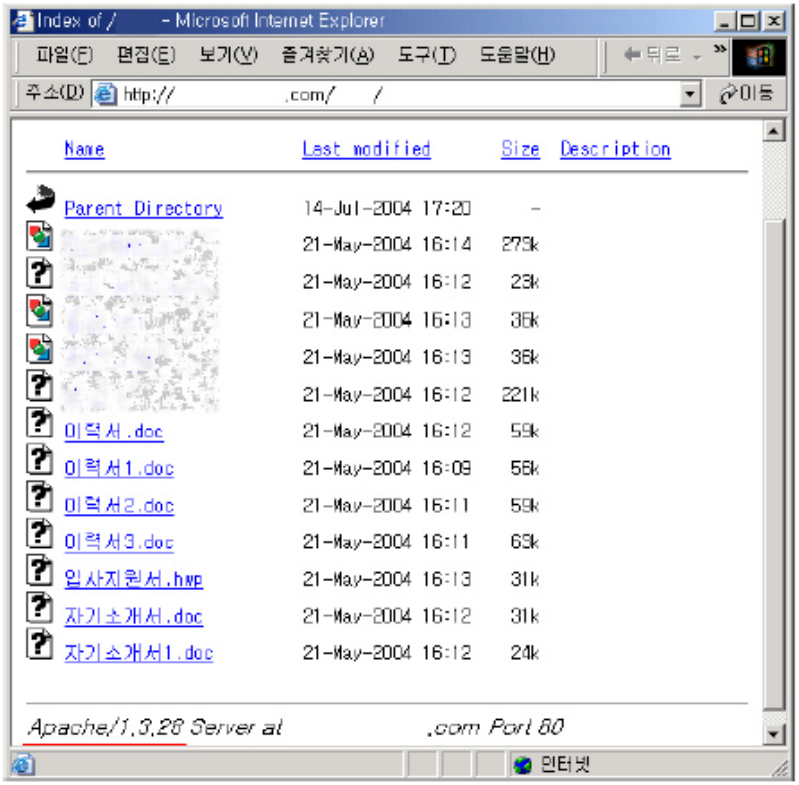
Googledork

- 실습 1)
  - 디렉터리 목록화 intitle:index.of/home inurl:co.kr



Googledork

- 실습 2)
  - 데이터 다운로드 intitle:"index of" intext:이력서



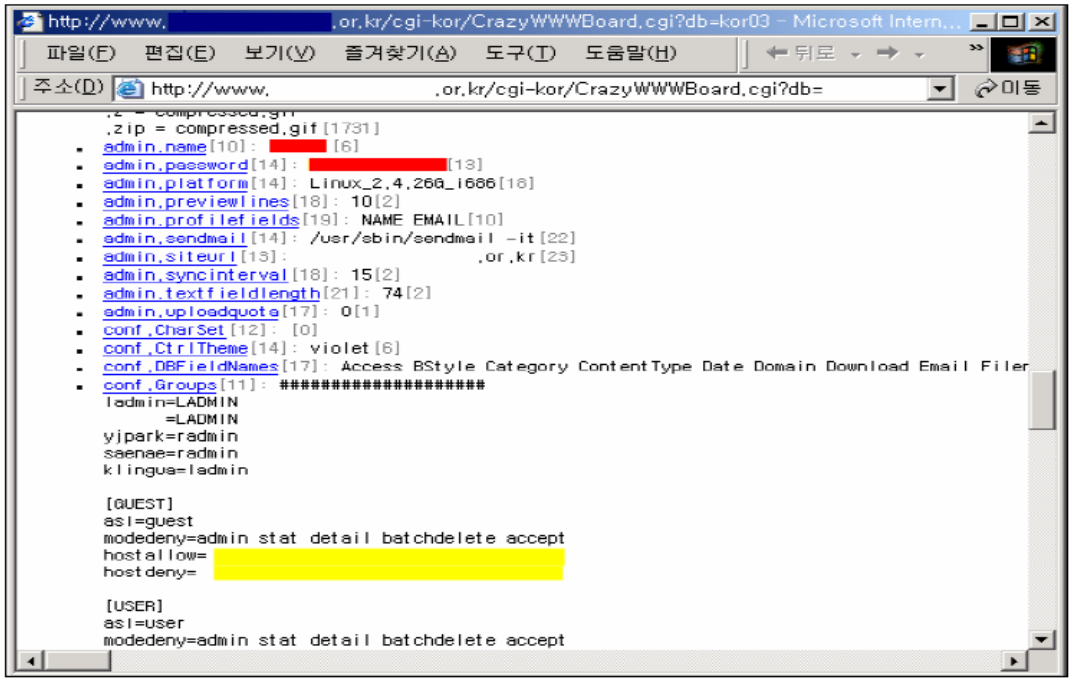
Googledork

- 실습 3)
  - 에러메시지 ORA-00921: unexpected end of SQL command site:co.kr

Oracle DB 예외 처리 오류 검색

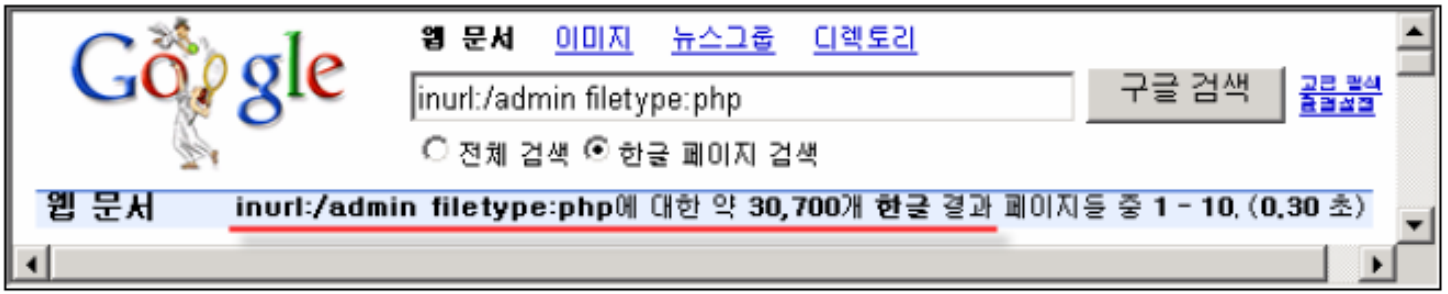
Googledork

- 실습 4)
  - 에러메시지 "HTTP_USER_AGENT=googlebot" site:or.kr

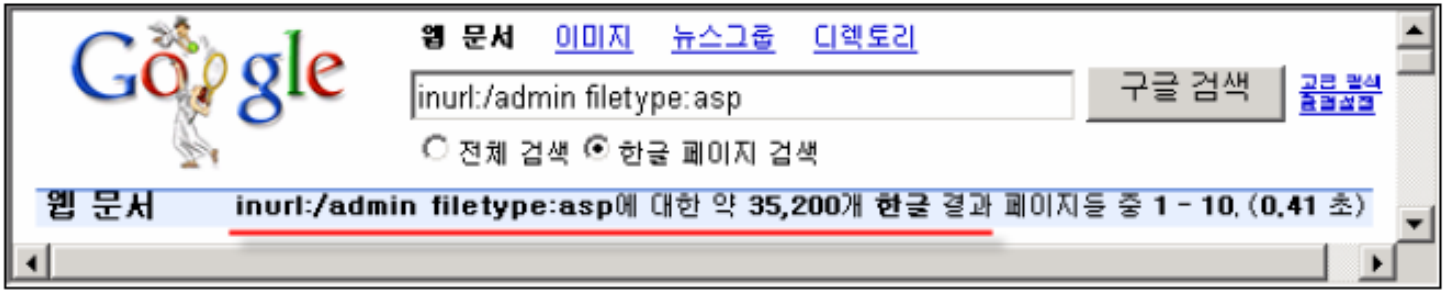


Googledork

- 실습 5)
  - 로그인



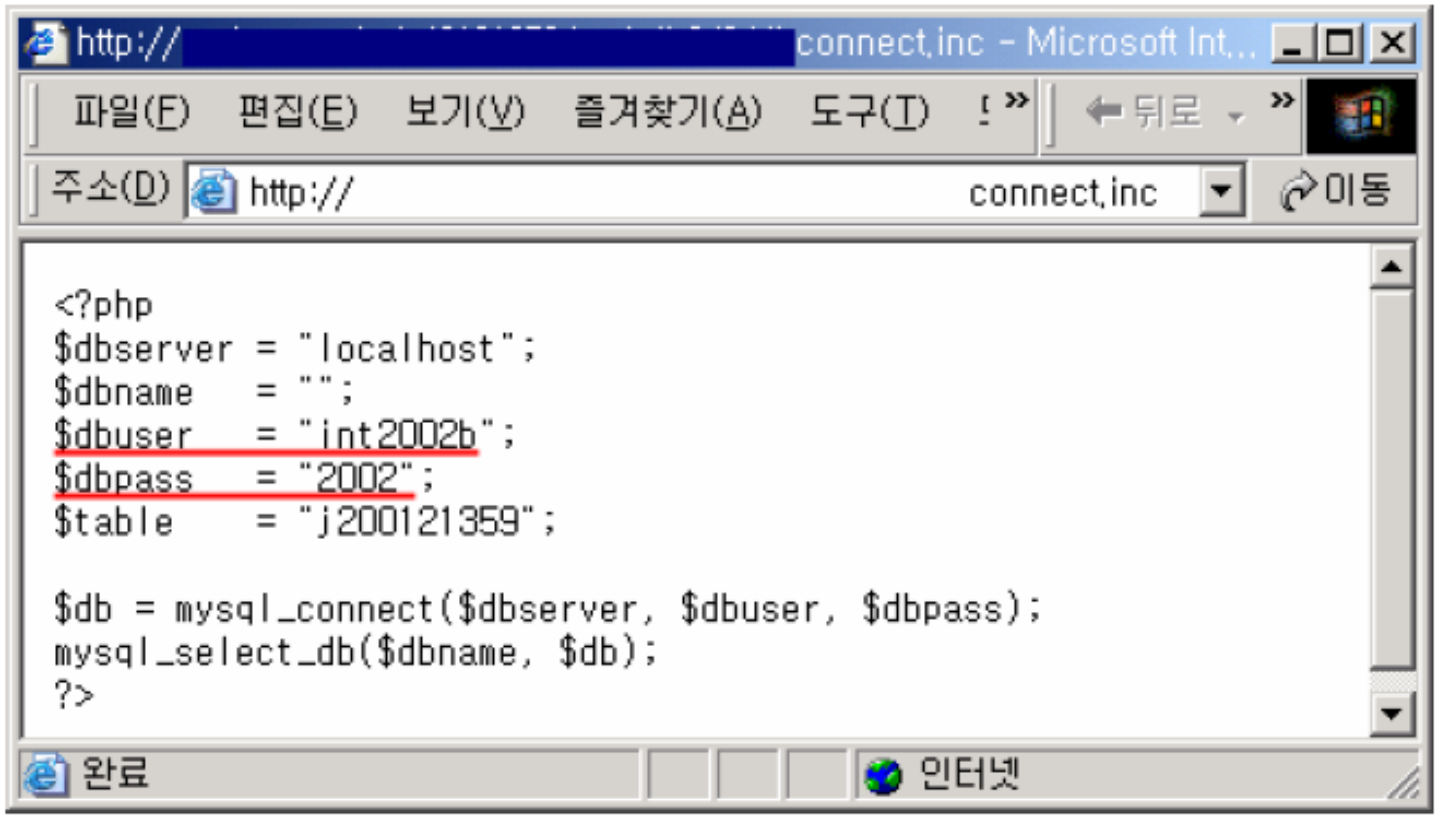
inurl:/admin filetype:php



inurl:/admin filetype:asp

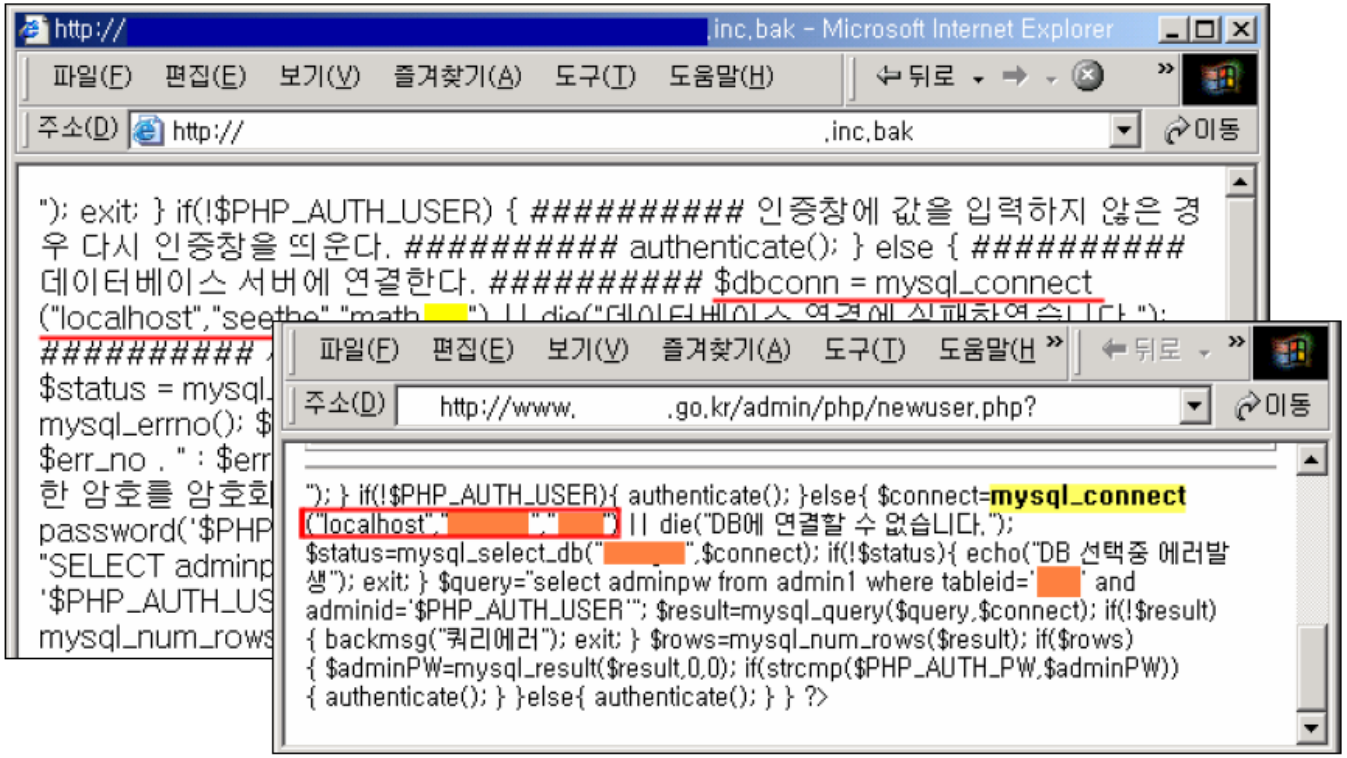
Googledork

- 실습 6)
  - 패스워드(DB) intext:mysql_connect+pass



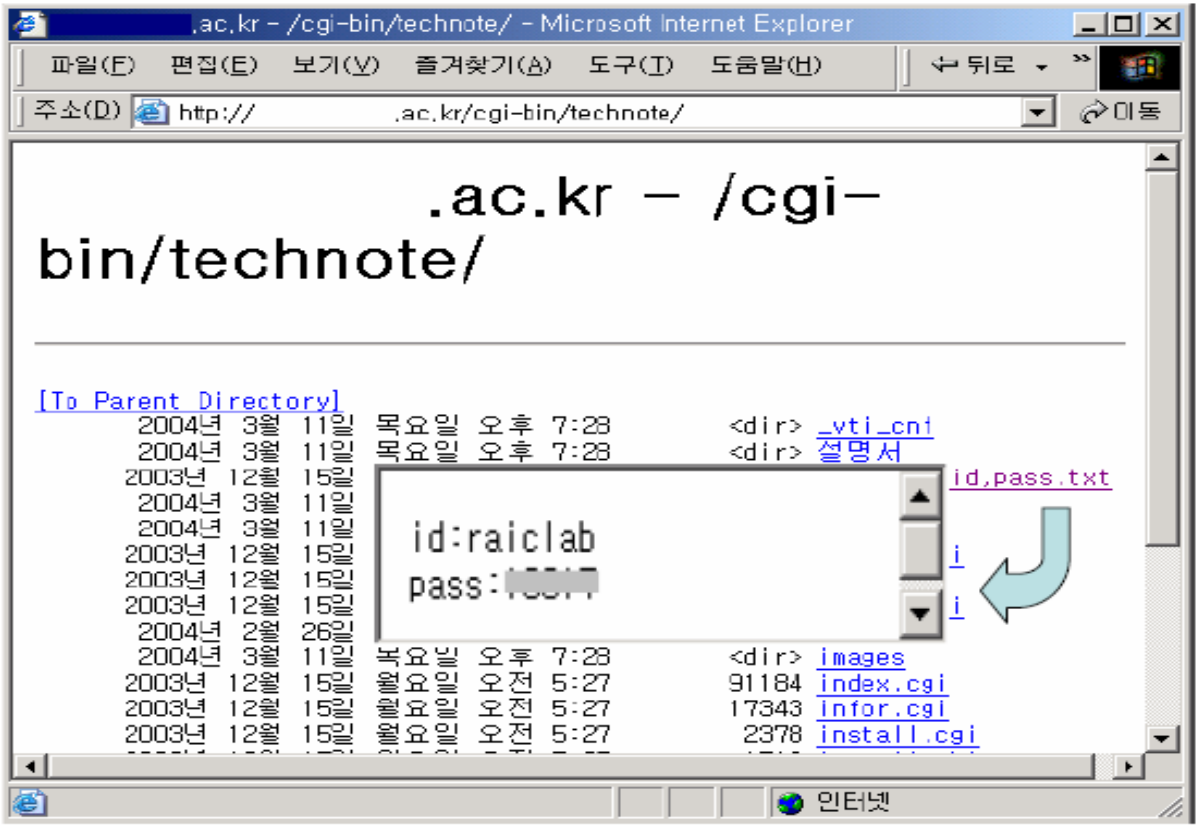
Googledork

- 실습 7)
  - 패스워드(DB) intext:mysql_connect filetype:bak



Googledork

- 실습 8)
  - 패스워드(게시판) intitle:technote inurl:cgi-bin



Q & A