

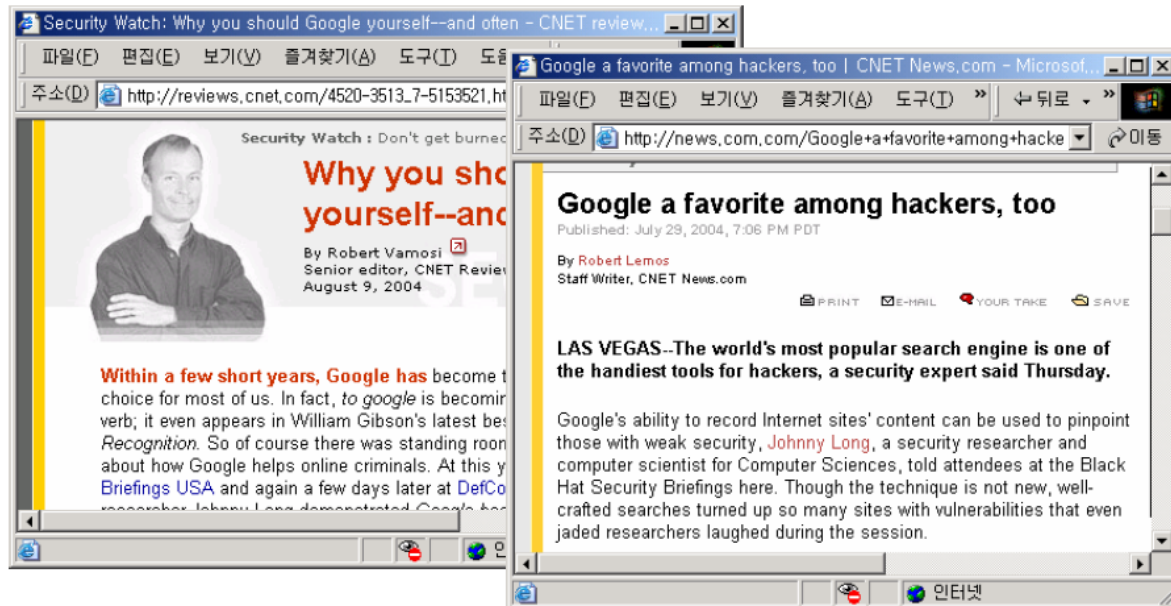
컴퓨터보안 실습 02

3주차

Googledork

- 구글의 위험성

전세계적으로 구글 검색이 범죄에 이용되고 있음.
가장 대중적인 해킹 도구로 인식되고 있음.



Googledork

- 실습 후 제출
 - 실습 화면 캡처
 - 분석 : 공격을 통해 파악할 수 있는 정보 (캡처x)
 - Ex) ooo 명령을 통해 패스워드, 고객주소, 핸드폰 번호등을 알수있었음
 - Ex2) ooooo 소스코드를 통해 ooo에 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”

The screenshot shows a Microsoft Internet Explorer browser window with the title 'Top Increasing Attack'. The address bar contains the URL 'http://www.securitymap.net/www/stats/top_ports.php'. The search bar contains the text 'Top 공격대상 포트 (Top 10 Attack Port, Last 30 days)'. The search options are highlighted with colored boxes and arrows: 'INTITLE:' (red), 'SITE:' (red), 'INURL:' (blue), 'INTEXT:' (pink), and 'NUMRANGE:' (blue). The search results page displays a table with the following data:

순위	Port 번호 <small>INTEXT:</small>	이벤트수	패킷수
1	80	1093	9183
2	25	575	183062
3	80,139,1025,2745,612 ...	351	1939
4	4899	300	8077
5	445	292	5409
6	21	152	1904
7	901	113	2426
8	1433	90	9157
9	1080	86	364
10	9898 <small>NUMRANGE:</small>	83	829

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.

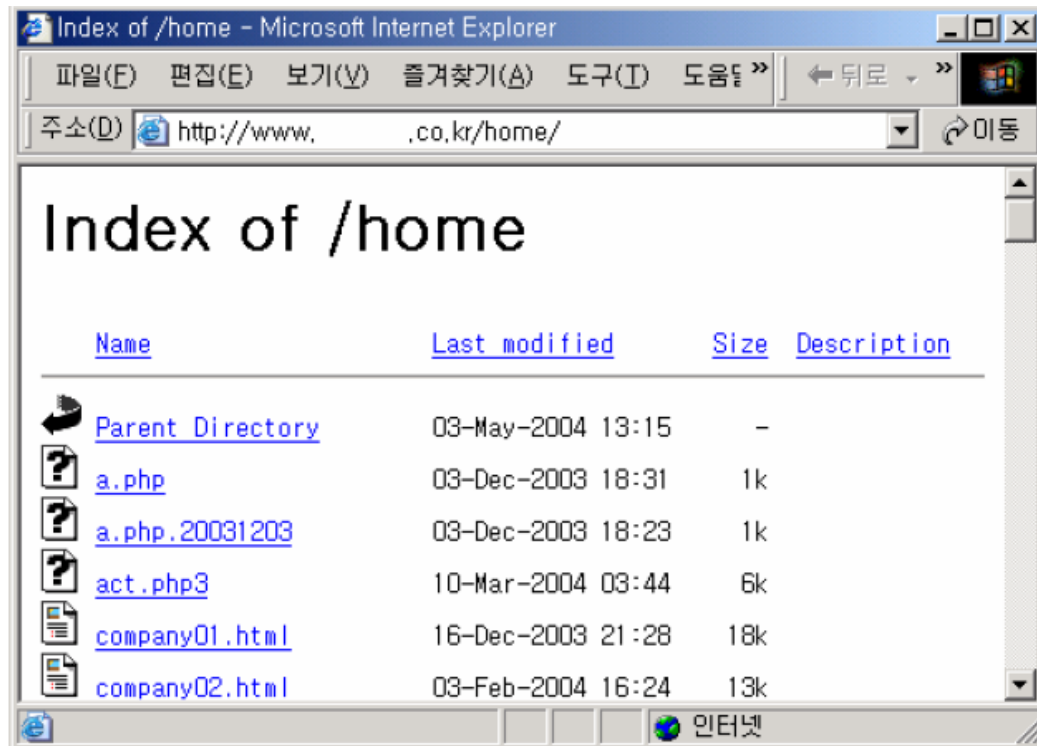


그림. 관리자 페이지의 주문 판매 정보 검색

Googledork

- 실습 1)

- 디렉터리 목록화 `intitle:index.of/home inurl:co.kr`

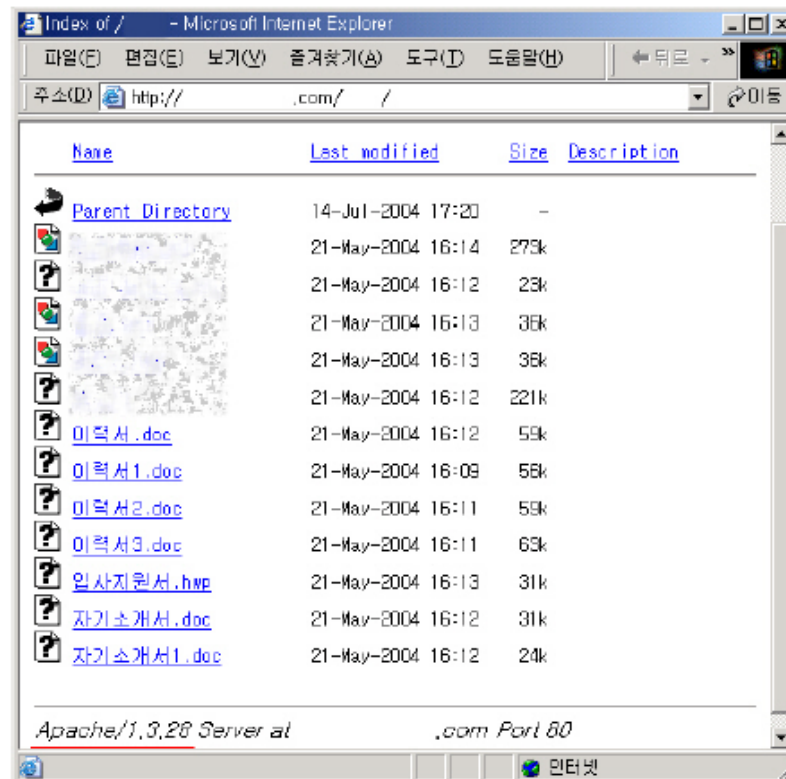


Googledork

- 실습 2)

- 데이터 다운로드

intitle:"index of" intext:이력서



Googledork

- 실습 3)

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

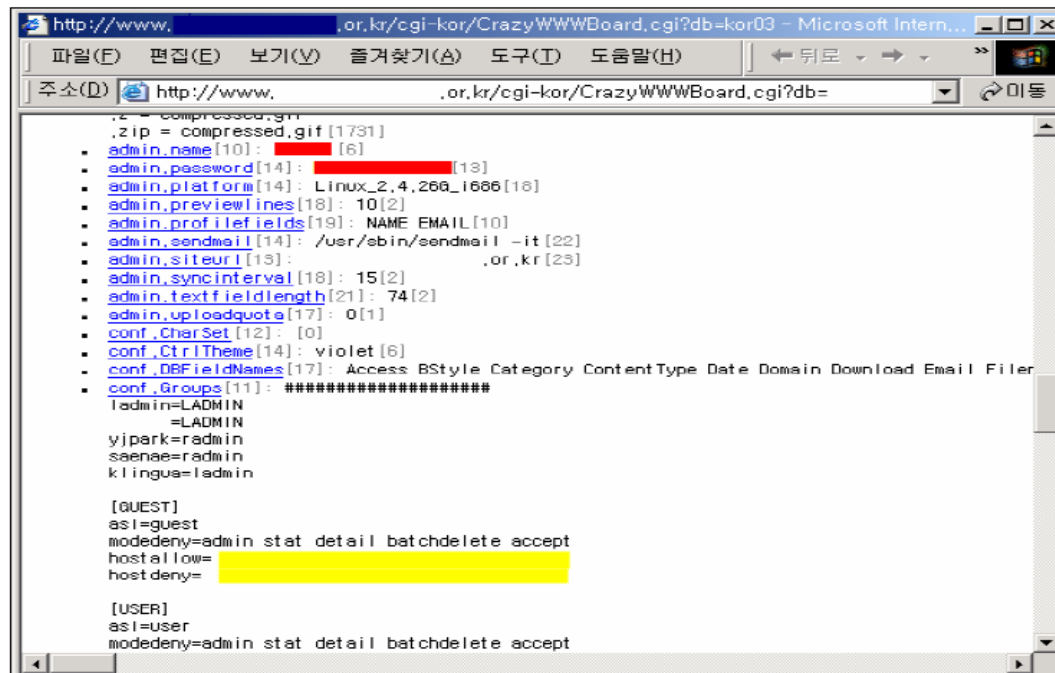


Oracle DB 예외 처리 오류 검색

Googledork

- 실습 4)

- 에러메시지 "HTTP_USER_AGENT=googlebot" site:or.kr



```
http://www. .or.kr/cgi-kor/CrazyWWWBoard.cgi?db=kor03 - Microsoft Intern...
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
주소(D) http://www. .or.kr/cgi-kor/CrazyWWWBoard.cgi?db=
admin_name[10]: [REDACTED] [6]
admin_password[14]: [REDACTED] [13]
admin_platform[14]: Linux_2.4.266_1686[18]
admin_previewlines[18]: 10[2]
admin_profilefields[19]: NAME EMAIL[10]
admin_sendmail[14]: /usr/sbin/sendmail -it[22]
admin_siteurl[18]: .or.kr[23]
admin_syncinterval[18]: 15[2]
admin_textfieldlength[21]: 74[2]
admin_uploadquote[17]: 0[1]
conf_CharSet[12]: [0]
conf_CtrlTheme[14]: violet[6]
conf_DBFieldNames[17]: Access BStyle Category ContentType Date Domain Download Email File
conf_Groups[11]: #####
  ladmin=LADMIN
    =LADMIN
  yjpark=admin
  saenae=admin
  kilingua=ladmin

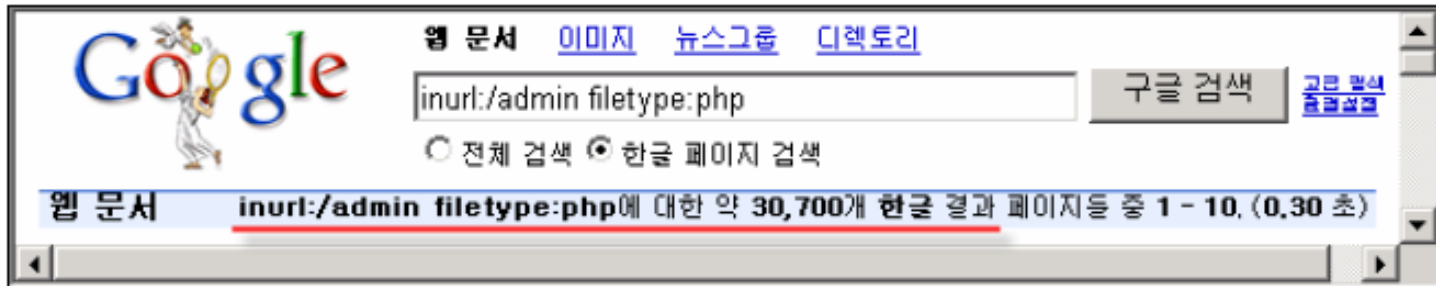
[GUEST]
asl=guest
modedeny=admin stat detail batchdelete accept
hostallow=
hostdeny=

[USER]
asl=user
modedeny=admin stat detail batchdelete accept
```

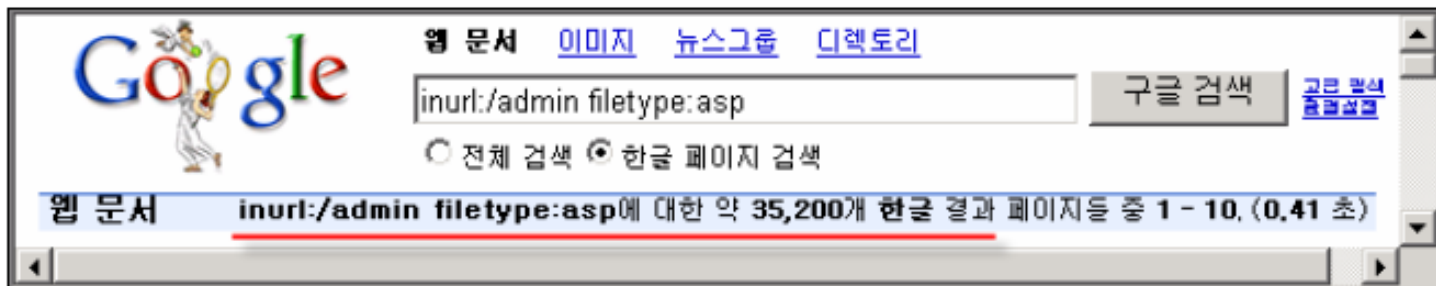
HTTP_USER_AGENT=googlebot" site:or.kr

Googledork

- 실습 5)
 - 로그인



inurl:/admin filetype:php



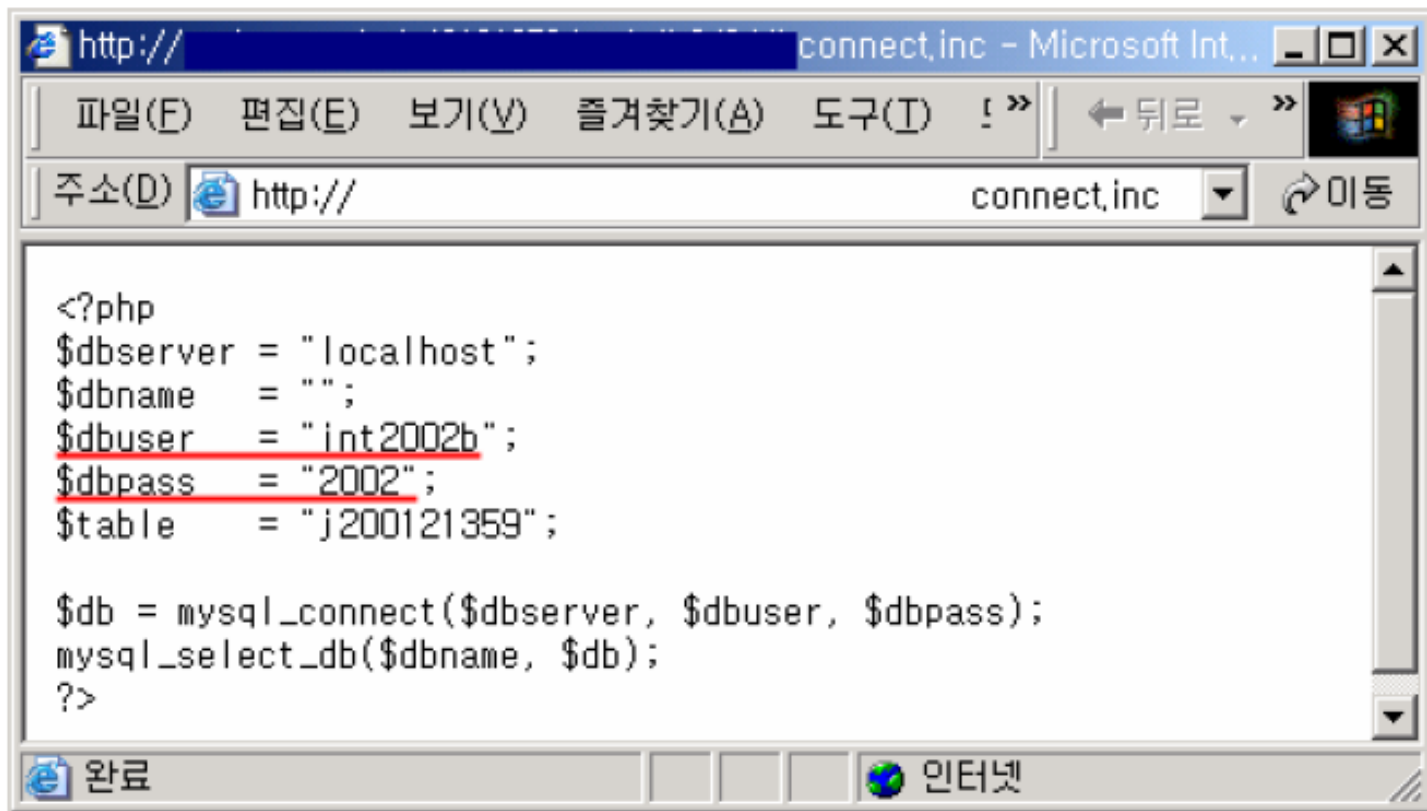
inurl:/admin filetype:asp

Googledork

- 실습 6)

- 패스워드(DB)

intext:mysql_connect+pass



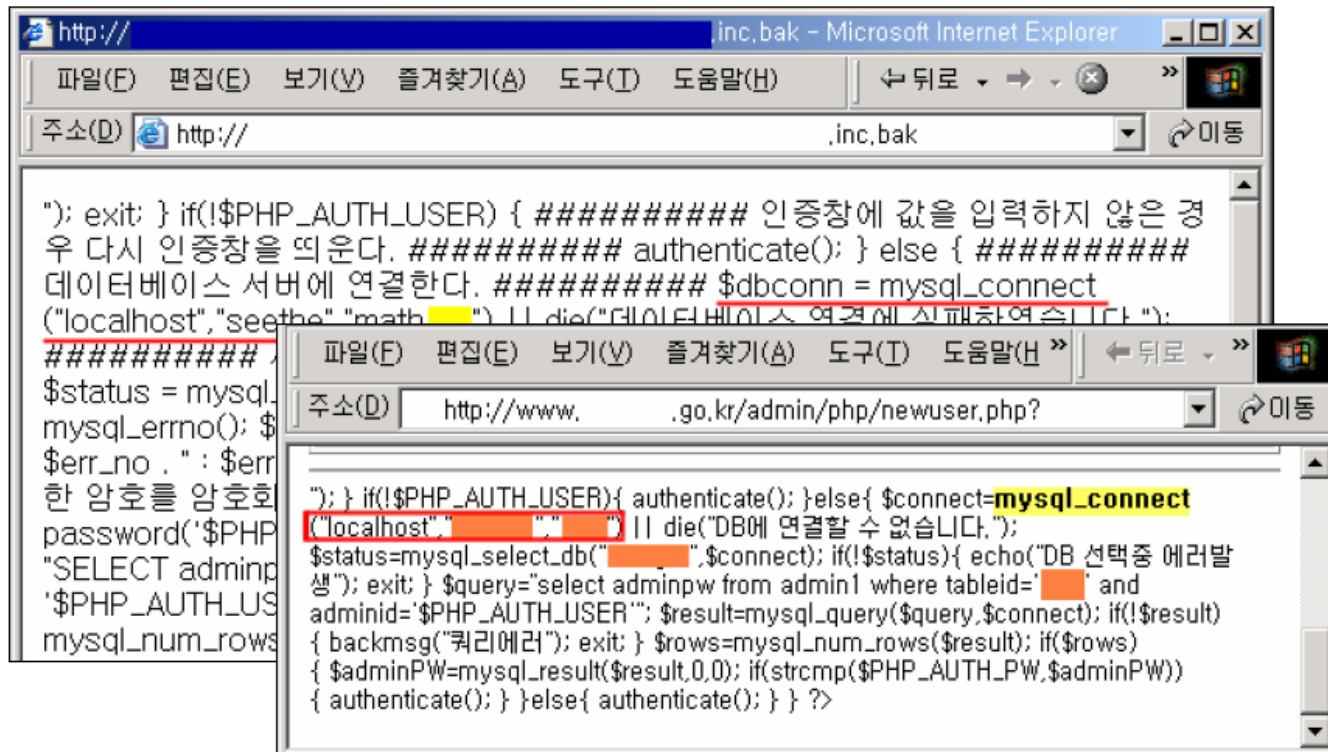
```
<?php
$dbserver = "localhost";
$dbname   = "";
$dbuser   = "int2002b";
$dbpass   = "2002";
$table    = "j200121359";

$db = mysql_connect($dbserver, $dbuser, $dbpass);
mysql_select_db($dbname, $db);
?>
```

Googledork

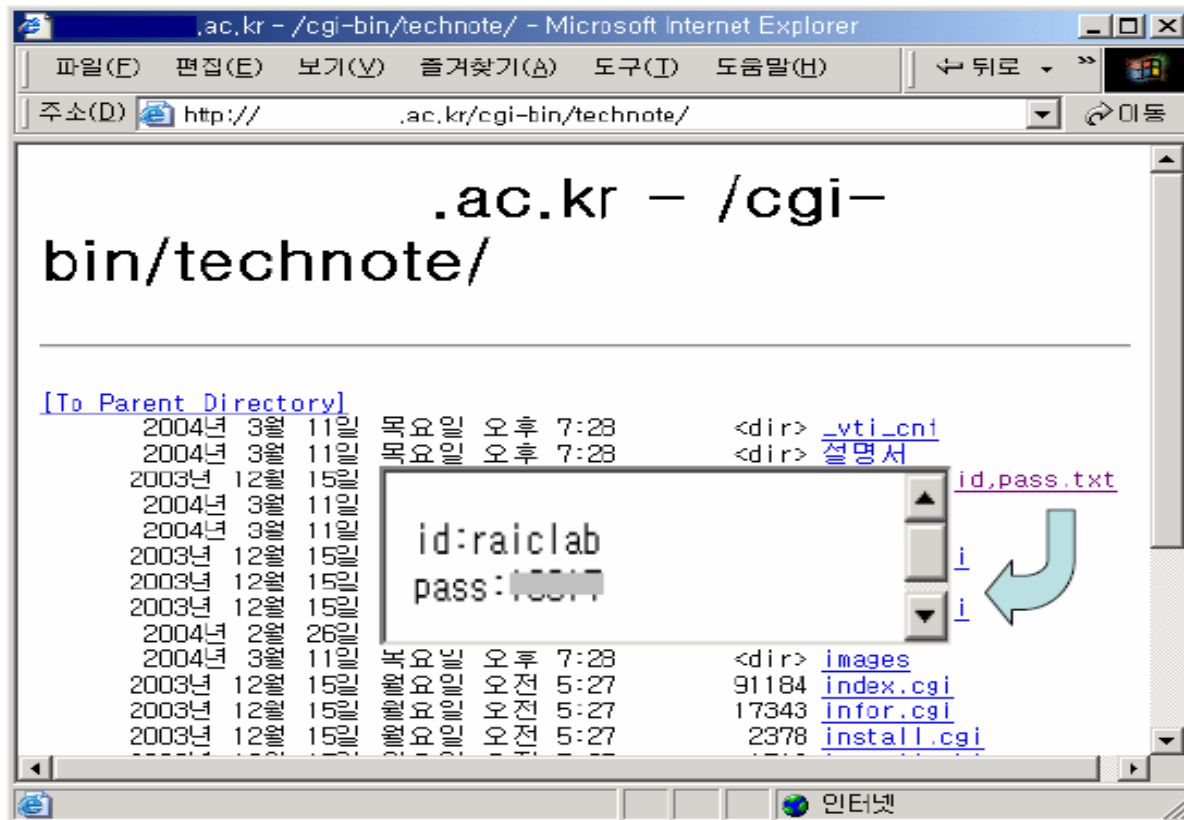
- 실습 7)

- 패스워드(DB) `intext:mysql_connect filetype:bak`



Googledork

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



Q & A