

Googledork

구글 검색을 이용한 해킹 방어

심정재(jjshim@hanaro.com)

2004.08.27

구글해킹(googledork)?

“새로운 것은 아니다!!!” 이미 2001년 부터 인터넷 검색엔진의 부작용을 이야기 하고 있었으며, 최근 2004년 defecon, Blackhat에서 이슈로 떠오름.

Is not new!!!

- ✓ 국내 에서는 아직까지 googledork 위험성에 대해 인식 부족
- ✓ 국가적으로 대응책 마련 필요

구글(google)이란?

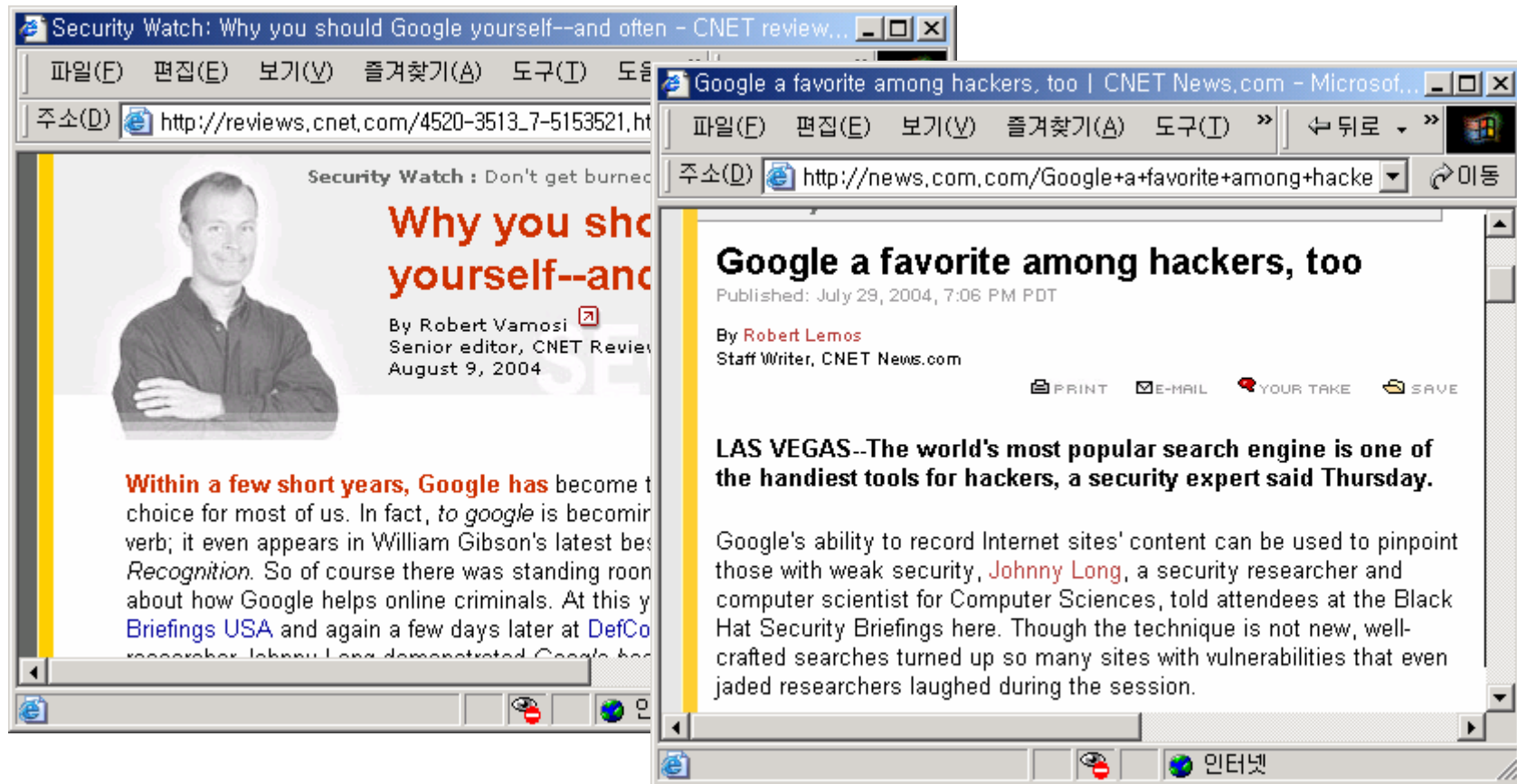
- ✓ 1999년부터 인터넷 검색 서비스를 시작한 현재 세계에서 가장 크고 빠른 검색 엔진
- ✓ 40억 페이지 이상 보유
- ✓ 1일 2억번 이상 검색 결과 제공
- ✓ 다양한 구글의 검색 기능은 사용자가 원하는 정보를 매우 신속하고 정확하게 제공
- ✓ 2003년 이후 인터넷 검색엔진이 지능화 되면서 시스템의 주요 정보, 민감한 데이터의 접근 경로까지 검색 제공.

무엇을 이야기 하려는가?

- ✓ 해커가 Google을 이용하여 취약한 시스템과 기밀 정보를 어떻게 찾아 낼 수 있는가?
- ✓ 해커가 Google을 이용하여 찾아낸 정보를 해킹에 어떻게 이용하는가?
- ✓ 구글해킹(googledork)을 통해 자신의 사이트가 안전한지 테스트하는 방법은?
- ✓ 구글해킹(googledork)에 대한 현재까지 많은 논의들은?

구글의 위험성은?

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



구글 검색 기초

■ 검색 옵션

다양한 검색 옵션으로 사용자가 원하는 결과를 보다 정확하게 검색

기타 검색 옵션

allintitle:

allinurl:

link:

daterange:

define:

phonebook:

related:

“Strings”

INTITLE:

FILETYPE:

SITE:

INURL:

INTEXT:

NUMRANGE:

순위	Port 번호	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	83	829

구글 검색 기초

■ 단어 검색 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"

구글 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.

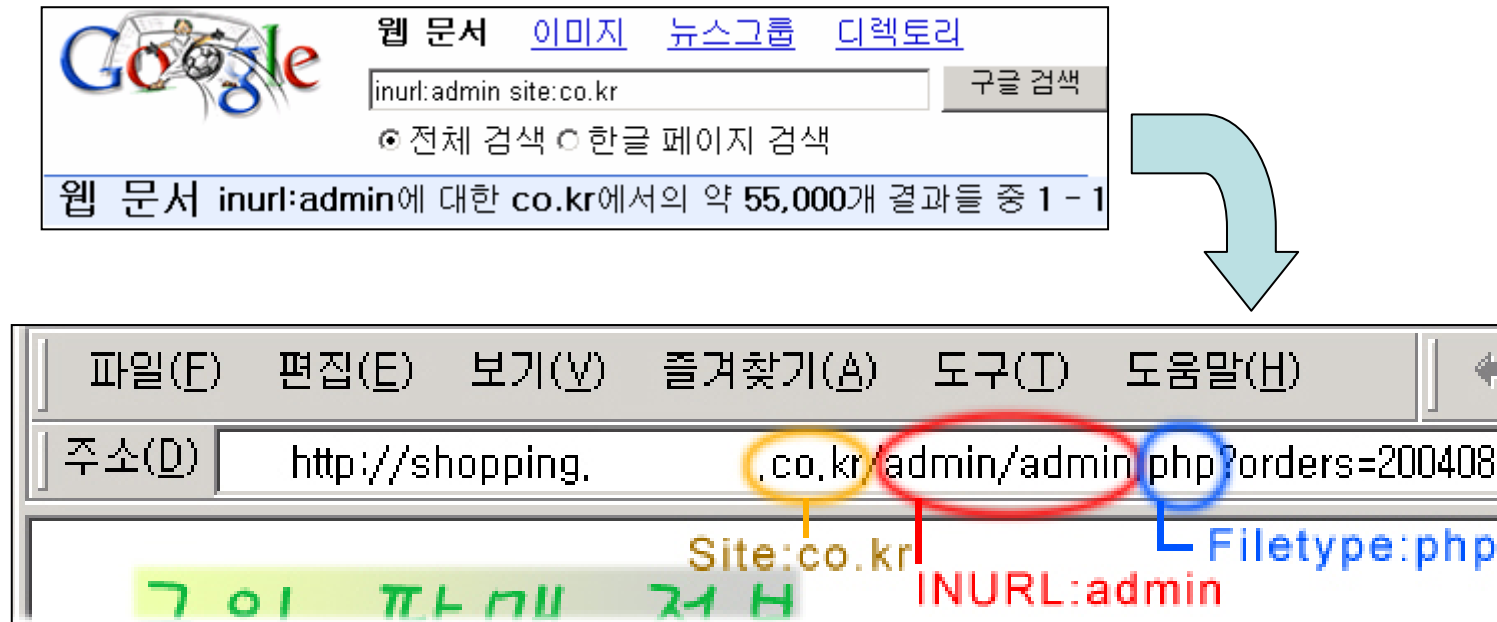


그림. 관리자 페이지의 주문 판매 정보 검색

구글 해킹 기초

- ✓ 서버에 직접 접속하지 않고 구글에 저장된 페이지로 접근하여 정보 획득
- ✓ 별도의 취약점 스캐닝 툴을 이용하지 않고 취약서버 수집 가능



구글 정보 획득 기술

■ 해킹에 이용되는 구글 검색 기술

13개로 분류된 약 500개 이상의 검색어구로 세분화 하여 계속 업데이트 중

“에러 메시지”, “파일내의 세부적인 정보”, “패스워드를 포함한 파일”,
“사용자 정보를 포함한 파일”, “특정 권한을 획득하기 위한 참조 파일”,
“로그인 페이지”, “네트워크 정보나 취약 데이터”, “민감한 디렉터리 및 파일”,
“숨겨진 디렉터리”, “임시 파일”, “취약 서버 목록”, “웹 서버 종류”,
“사회공학적 해킹 자료”

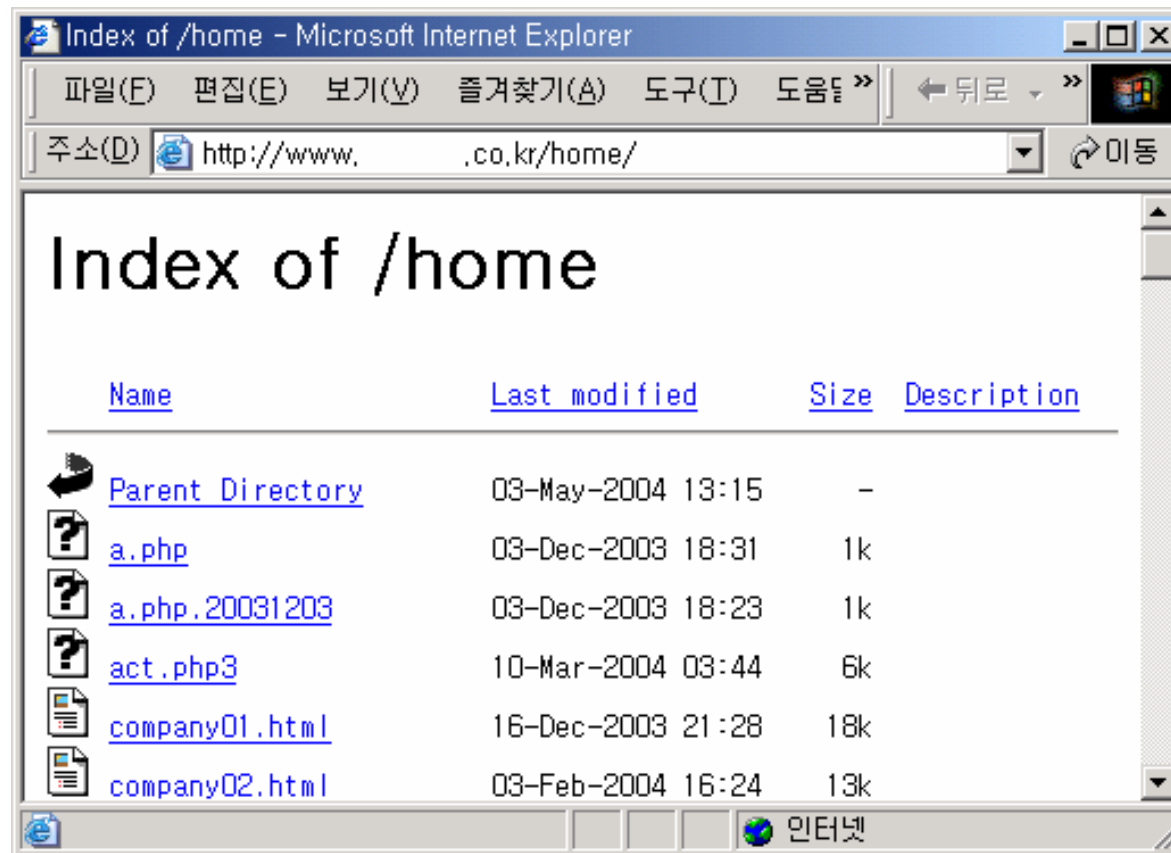
googledork web site: <http://johnny.ihackstuff.com>



디렉터리 목록화

■ 디렉터리 목록화(Directory Listing)

웹 서버의 소스 코드를 볼 수 있는 취약점

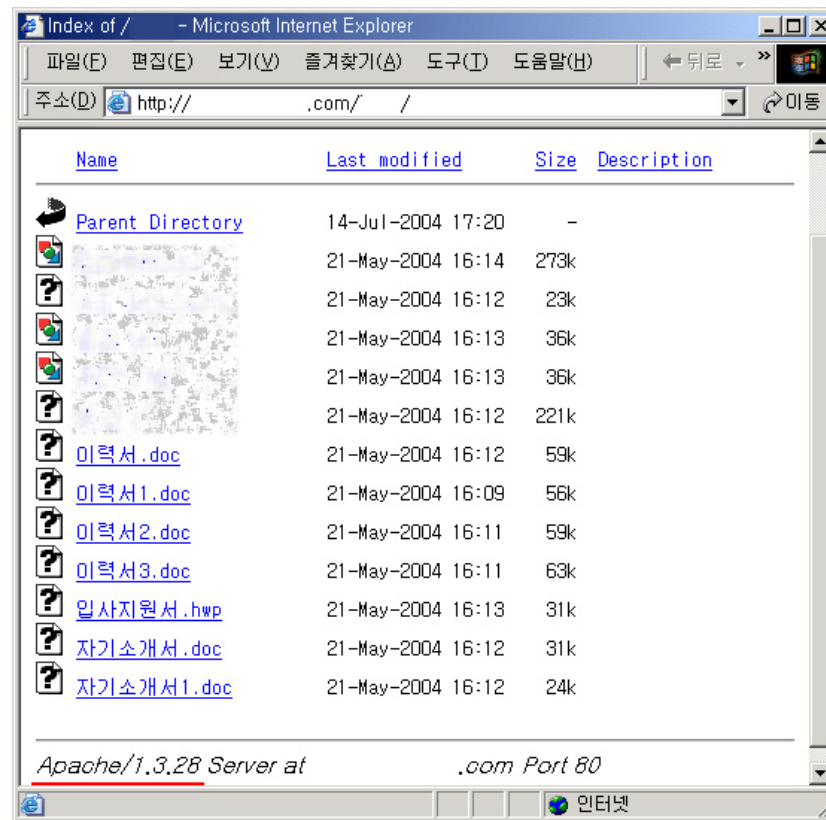


소스코드 노출 검색 `intitle:index.of/home inurl:co.kr`

디렉터리 목록화

■ 디렉터리 목록화(Directory Listing)

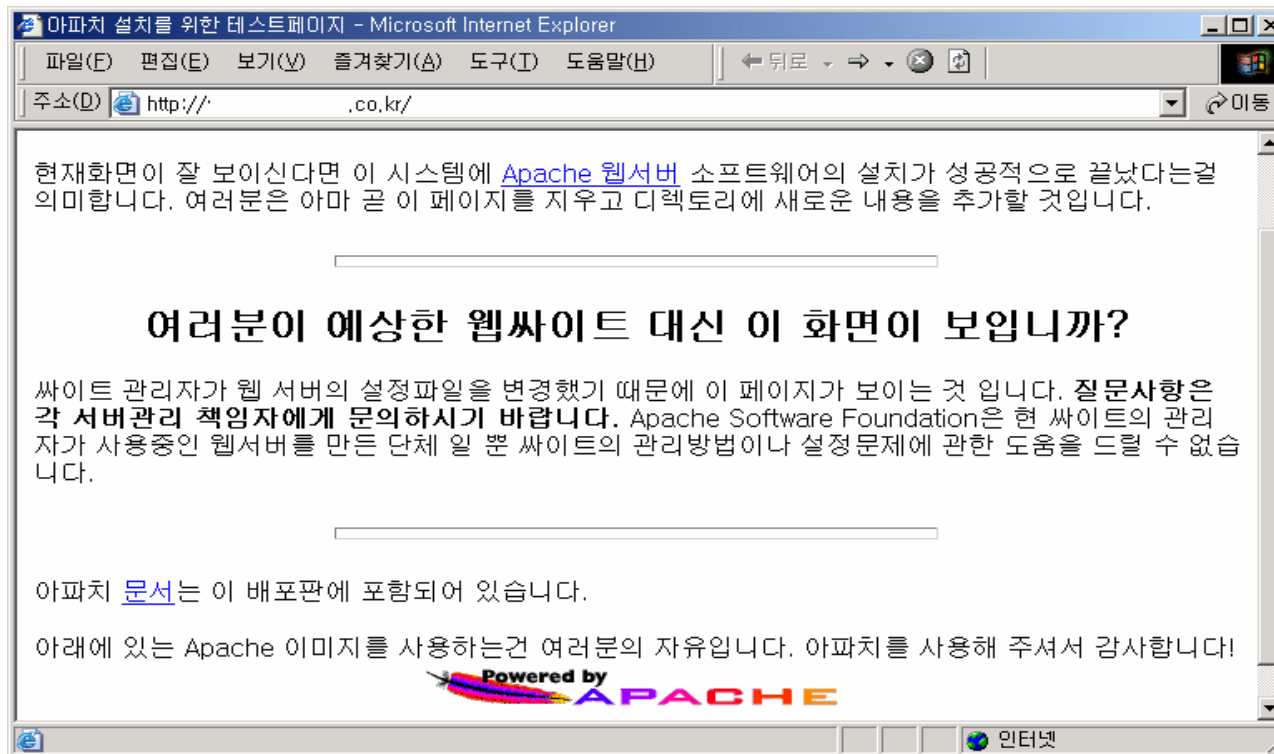
웹 서버의 민감한 데이터 다운로드 가능, 웹 서버 버전 확인 가능



민감한 데이터 검색 `intitle:"index of" intext:이력서`

서버 기본 페이지

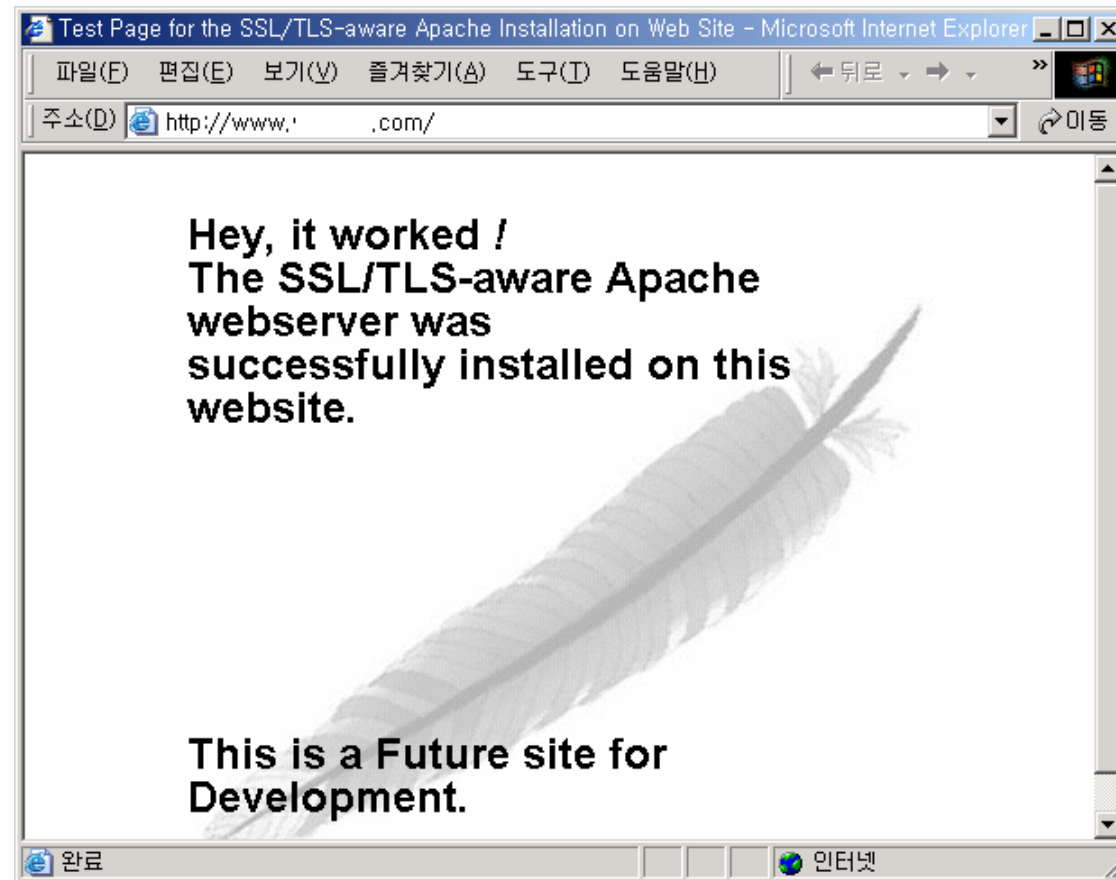
- ✓ 서버 기본 페이지가 존재한다는 것은 많은 공격자들로부터 침입 목표가 될 수 있다(서버 관리 미비로 취약점 다수 존재 가능성 높음).



아파치 기본 페이지 검색
intitle:"아파치 설치를 위한 테스트페이지"

서버 기본 페이지

- ✓ Apache SSL/TLS 서버 기본 페이지 검색

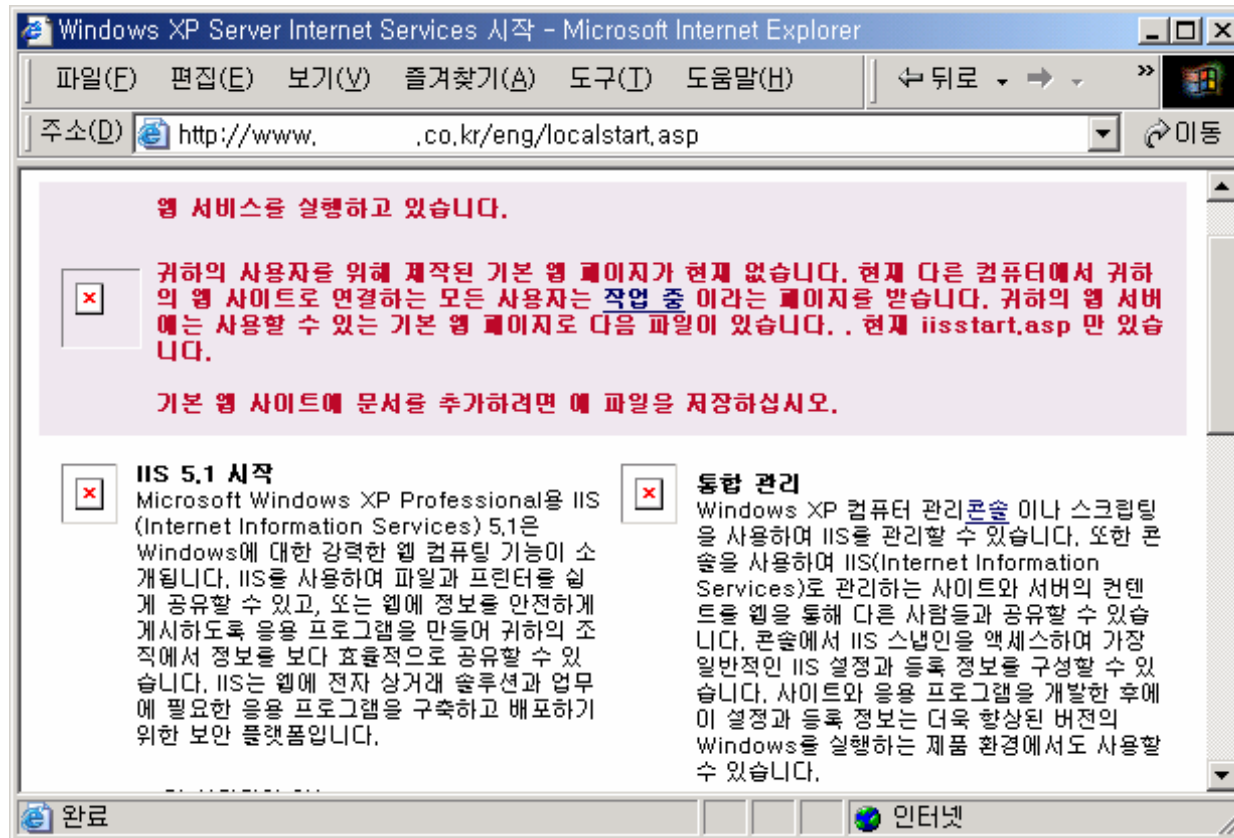


Apache SSL/TLS 기본 페이지 검색
intitle:test.page "Hey, it worked !" "SSL/TLS-aware"

서버 기본 페이지

■ IIS6.0(Windows XP Server)

서버 샘플 파일 미 삭제 정보 획득, 서버 디렉터리 구조 정보 획득



IIS 웹 서버 기본 페이지 검색

intitle:"Windows XP Server Internet Services 시작"

서버 기본 페이지

■ 웹 서버 기본 페이지 검색(영문)

웹 서버	영문 버전 검색
Apache 1.3.0–1.3.9	intitle:Test.Page.for.Apache It.worked! this.web.site!
Apache 1.3.11–1.3.26	intitle:Test.Page.for.Apache seeing.this.instead
Apache 2.0	intitle:Simple.page.for.Apache Apache.Hook.Functions
Apache SSL/TLS	intitle:test.page "Hey, it worked !" "SSL/TLS-aware"
IIS servers	intitle:welcome.to intitle:internet IIS
IIS 4.0	intitle:welcome.to.IIS.4.0 allintitle>Welcome to Windows NT 4.0 Option Pack allintitle>Welcome to Internet Information Server
IIS 5.0	allintitle>Welcome to Windows 2000 Internet Services
IIS 6.0	allintitle>Welcome to Windows XP Server Internet Services

서버 기본 페이지

■ 웹 서버 기본 페이지 검색(한글)

웹 서버	한글 버전 검색
Apache 1.3.0-1.3.8	intitle:Test.Page.for.Apache It.worked! this.web.site!
Apache 1.3.9-1.3.10	intitle:"Test Page for Apache Installation on Web Site!" Intitle:"Apache 1.x documentation"
Apache 1.3.11-1.3.32	intitle:"아파치 설치를 위한 테스트페이지" Intitle:"Apache 1.x documentation"
Apache 2.0	intitle:"아파치 설치 검사용 페이지" Intitle:"Apache HTTP Server Version 2.0 문서"
IIS 5.0	Intitle:"Windows 2000 인터넷 서비스 입니다." Intitle:"공사 중" intext:"현재 연결하려고 하는 사이트에 기본 페이지가 없습니다."
IIS 6.0	Intitle:"Windows XP 인터넷 서비스 입니다." Intitle:"준비 중" intext:"보려는 사이트에 현재 기본 페이지가 없습니다."

서버 프로파일

■ 서버 프로파일

그 외 다양한 웹 서비스 및 웹 응용프로그램 검색

Entries for category : All Categories / Web Server Detection
These links demonstrate Google's awesome ability to profile web servers..

Entry name	Dated	# of Hits	Author's Rating	Community Rating	How many found the entry helpful
"AnWeb/1.42h" intitle:index.of	19-Jul-2004	952		(none yet)	--
"CERN httpd 3.0B (VAX VMS)"	19-Jul-2004	308			--
"httpd+ssl/ktttd" * server at intitle:index.of	19-Jul-2004	81		(none yet)	--
"JRun Web Server" intitle:index.of	19-Jul-2004	198		(none yet)	--
"MaXX/3.1" intitle:index.of	19-Jul-2004	153		(none yet)	--
"Microsoft-IIS/* server at" intitle:index.of	19-Jul-2004	347		(none yet)	--
"Microsoft-IIS/4.0" intitle:index.of	19-Jul-2004	239		(none yet)	--
"Microsoft-IIS/5.0 server at"	19-Jul-2004	299		(none yet)	--
"Microsoft-IIS/6.0" intitle:index.of	19-Jul-2004	267		(none yet)	--
"Novell, Inc" WEBACCESS Username Password "Version *.*" Copyright - inurl:help -guides guide	26-Jul-2004	472		(none yet)	--
"OmniHTTPd/2.10" intitle:index.of	19-Jul-2004	156		(none yet)	--
"OpenSA/1.0.4" intitle:index.of	19-Jul-2004	426		(none yet)	--

그림. johnny.ihackstuff.com의 웹 서버 탐지 룰

에러 메시지

■ 에러 메시지

에러 메시지 검색 결과는 서버에 침입 경로를 상세히 제공해 줄 수 있는 취약점.



Oracle DB 예외 처리 오류 검색

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

에러 메시지

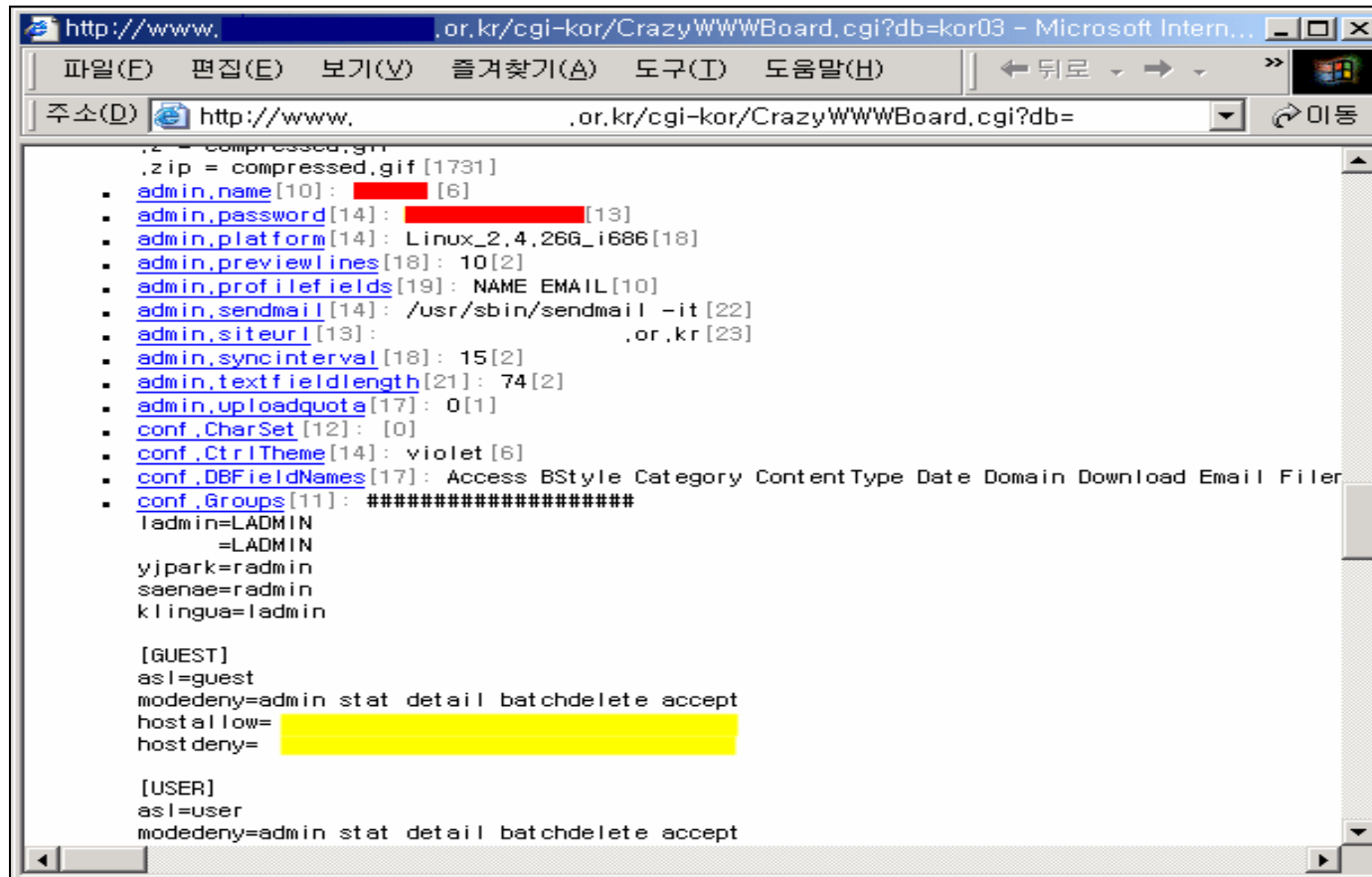
- 에러 메시지 검색
서버 AP설치 정보, ID/PW 정보, SQL Injection공격 등 정보 제공



DB ID검색 "access denied for user" "using password" site:co.kr

에러 메시지

- 에러 메시지
에러 메시지를 통한 서버 ID/PW 정보 획득



```
http://www. .or.kr/cgi-kor/CrazyWWWBoard.cgi?db=kor03 - Microsoft Intern...
파일(E) 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_2.4.26G_i686[18]
admin.previewlines[18]: 10[2]
admin.profilefields[19]: NAME EMAIL[10]
admin.sendmail[14]: /usr/sbin/sendmail -it [22]
admin.siteurl[13]: .or.kr [23]
admin.syncinterval[18]: 15[2]
admin.textfieldlength[21]: 74[2]
admin.uploadquota[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
klingua=ladmin

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

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

"HTTP_USER_AGENT=googlebot" site:or.kr

에러 메시지

■ 에러 메시지

에러 메시지를 통한 서버 설치 정보 획득, 공격 루트 확보

접속을 **실패**하였습니다. 접속을 **실패**하였습니다.
Warning: ocifetch(): supplied argument is not a valid OCI8-Statement resource in `/home/local/apache/htdocs/ /php/foreign/english2/common/inc/ /dbcon.php` on line 90

Warning: ociresult(): supplied argument is not a valid OCI8-Statement resource in `/home/local/apache/htdocs/ /php/foreign/english2/co`
접속을 **실패**하였습니다.

Warning: mysql_connect(): Can't connect to MySQL server on 'db2.netis.net' in `/home/ /korea_include/The_Class.php` on line 31

Warning: mysql_select_db(): supplied argument is not a valid MySQL-Link resource in `/home/ /korea_include/The_Class.php` on line 41

Warning: mysql_errno(): supplied argument is not a valid MySQL-Link resource in `/home/ /korea_include/The_Class.php` on line 90

Warning: MS SQL message: Unclosed quotation mark before the character string '39', (severity 15) in `N:W: 정보시스템wwwWociWoci8.php` on line 34

Warning: MS SQL message: Line 1: Incorrect syntax near '39', (severity 15) in `N:W: 정보시스템 wwwWociWoci8.php` on line 34

Warning: MS SQL: Query failed in `N:W: 정보시스템wwwWociWoci8.php` on line 34

Warning: Supplied argument is not a valid MS SQL-result resource in `N:W: 정보시스템 wwwWociWoci8.php` on line 61

Warning: pg_connect(): Unable to connect to PostgreSQL server: FATAL: database "tekno_db1" does not exist . in `/export/home/user1/ /public_html/board/_conf/info.php` on line 42

Warning: pg_exec(): supplied argument is not a valid PostgreSQL link resource in `/export/home/user1/ /public_html/board/read.list.php` on line 88

delete from TB_MYKBS where MYKEY=
Incorrect syntax near '';
죄송합니다. 데이터베이스 작업 중에 오류가 발생하였습니다.

Attack Scenarios

에러 메시지를 검색 결과에 따른
Oracle Database ID/PW 획득 시나리오
HP-UX 11.x 관리자 권한 획득 시나리오

로그 파일

■ 로그 파일

다양한 응용프로그램 로그파일을 검색 후 중요 정보 획득
(ID/PW, 시스템 정보, 서비스 정보, DB정보 등)

웹 문서 [이미지](#) [뉴스그룹](#) [디렉토리](#)

db filetype:log [고급 검색](#)
[환경설정](#)

전체 검색 한글 페이지 검색

db filetype:log에 대한 약 93개 한글 결과 페이지들 중 1 - 10. (0.40 초)

db filetype:log

웹 문서 [이미지](#) [뉴스그룹](#) [디렉토리](#)

intitle:"index of" intext:(backup|백업|bak|dump) [고급 검색](#)
[환경설정](#)

전체 검색 한글 페이지 검색

intitle:"index of" intext:(backup|백업|bak|dump)에 대한 약 147개 한글 결과

intitle:"index of" intext:(backup|백업|bak|dump)

로그 파일

- 로그 파일
데이터 베이스 백업 로그 검색

The screenshot shows a Microsoft Internet Explorer window displaying a MySQL backup file. The file content is a table with columns: no, user_id, password, name, email, and iumin. The password column contains several entries, with the second entry, '7310d16e62a80914', highlighted in red. A red arrow points from this entry to a 'mysqlHash_decode' dialog box. The dialog box has a title bar 'mysqlHash_decode' and a subtitle 'MySQL hash decoder v0.1'. It contains two input fields: 'hash' with the value '7310d16e62a80914' and 'decoder' with the value '7980'. There are two buttons: '확인' (OK) and '취소' (Cancel). The dialog box also includes the text 'by jjshim@hanaro.com'. A red text label '패스워드 디코딩' (Password Decoding) is positioned near the arrow.

no	user_id	password	name	email	iumin
2	bc	164	최		
3	yr	7310d16e62a80914	용		
4	er	615	스		
5	st	430	박		
6	yc	45e	연		
7	ys	16c	이		
8	ks	70e	가		
9	er	198	이		
10	er	4c5	정		
11	lit	637	김		
12	xc	081	김	mail.net	
13	ar	0fa4	안	.com	
14	ty	132	홍	mail.net	
15	ta	783	배	.com	
16	w	4ba	유	mail.net	
17	dl	1de	안	.com	
18	ye	5ca	김	il.net	
19	sc	4fe	진	mail.net	

mysql 백업 파일 검색
!Hint: filetype:bak intext: , inurl:

로그인 페이지

■ 로그인 페이지

- 웹 사이트 내에 감춰진 관리용 로그인 페이지를 검색하여 서버의 중요 정보를 획득하거나 서버 로컬 권한을 획득하는데 이용.
- 매우 일반적인 구글 검색만으로도 쉽게 찾을 수 있고, 대다수 서버가 알기 쉬운 패스워드를 사용하고 있음.

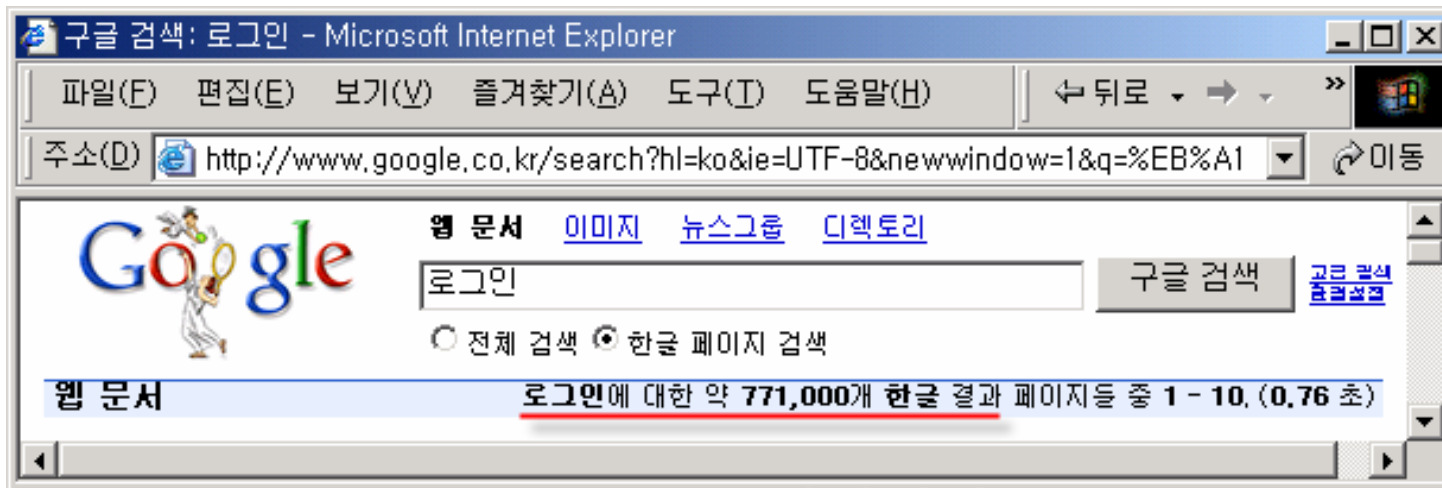


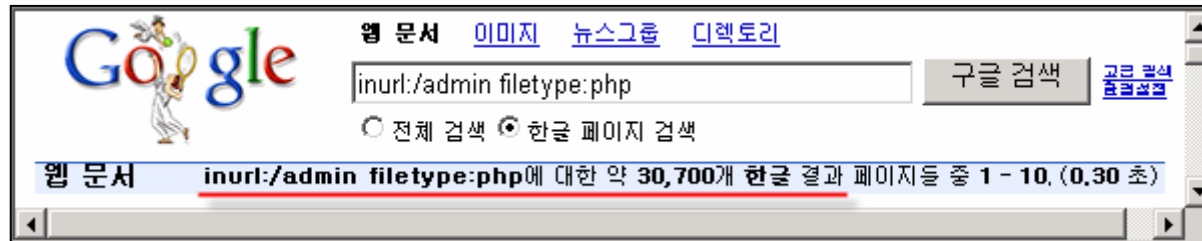
그림. 로그인

로그인 페이지

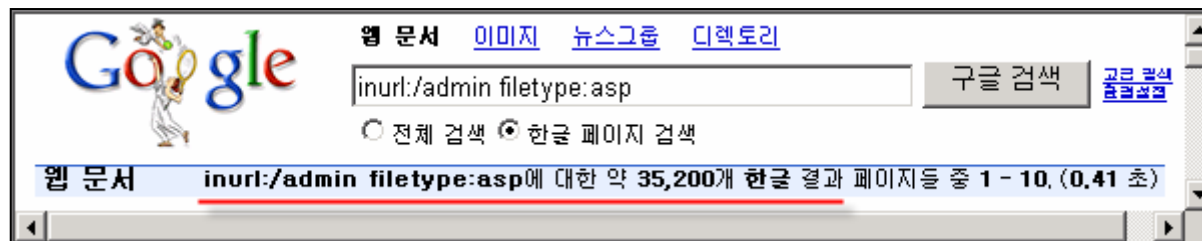
■ 관리용 로그인

- 웹 사이트 유지 보수를 위한 관리용 페이지 검색
- 웹 서버에 로컬 계정으로 직접 접근하기 위한 원격 로그인 페이지
- 게시판 관리자용 로그인 페이지 검색

(관리자 게시판은 대다수 파일 업로드, XSS 취약점 존재)



inurl:/admin filetype:php



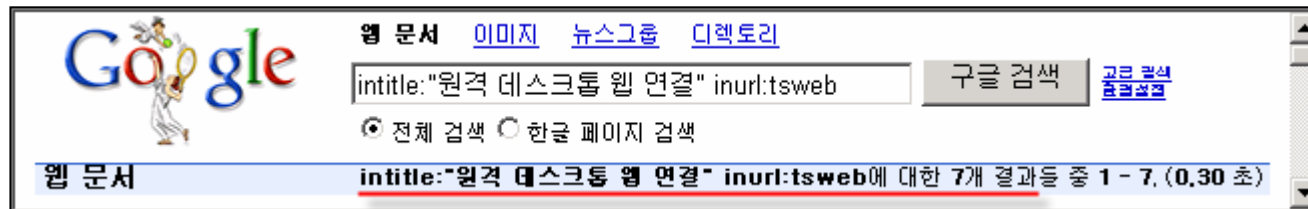
inurl:/admin filetype:asp

로그인 페이지

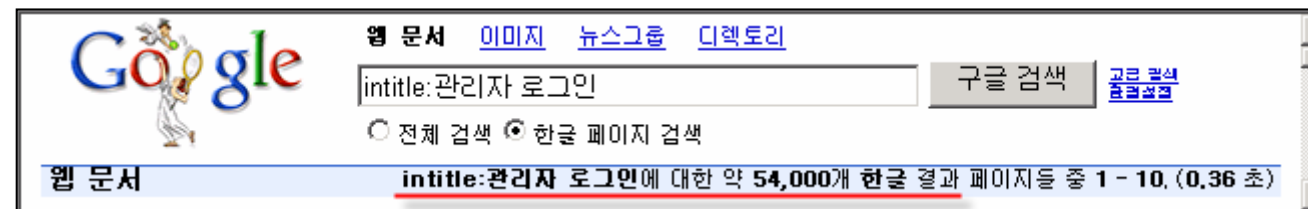
- VNC 원격 데스크톱 로그인("VNC Desktop" inurl:5800)



- 윈도우 터미널 원격 데스크톱 웹 로그인(intitle:"원격 데스크톱" inurl:tswb)

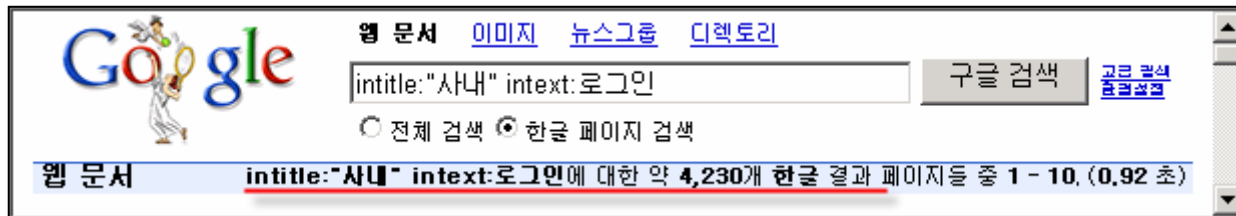
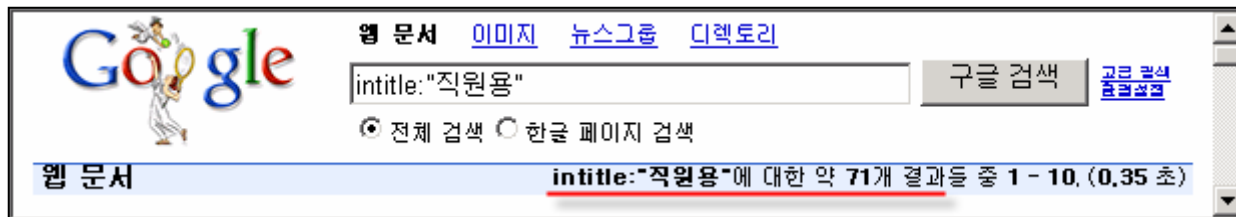
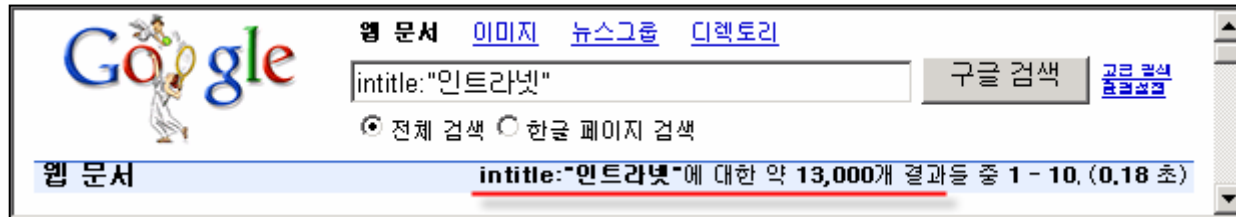


- 관리자 로그인 페이지(intitle:"관리자로그인")



로그인 페이지

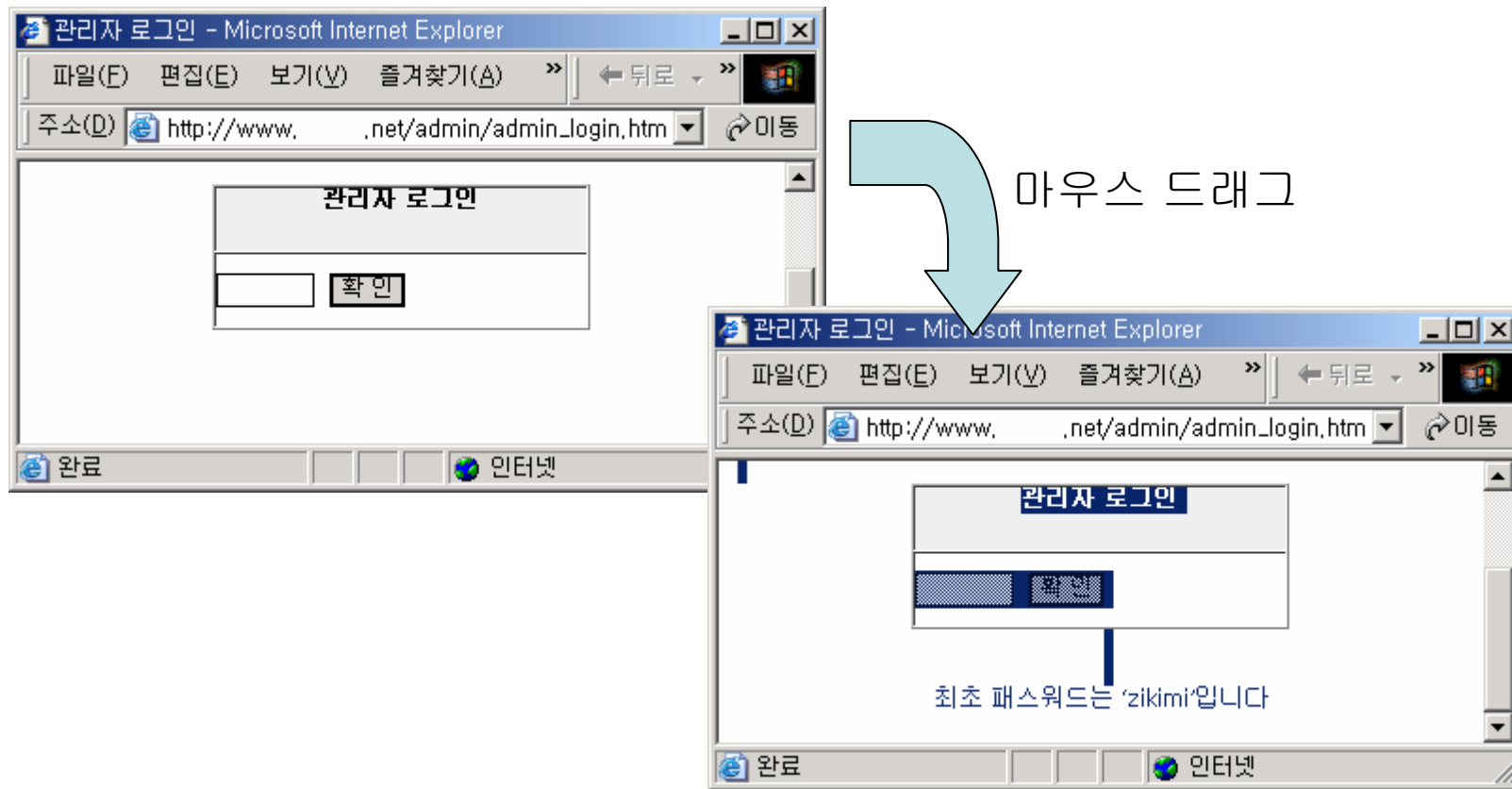
- 내부 네트워크 접속 페이지(intitle"인트라넷" or "intranet" 등등)



로그인 페이지

■ 관리자 로그인 취약점

소스보기 금지 우회 및 패스워드 노출 취약점

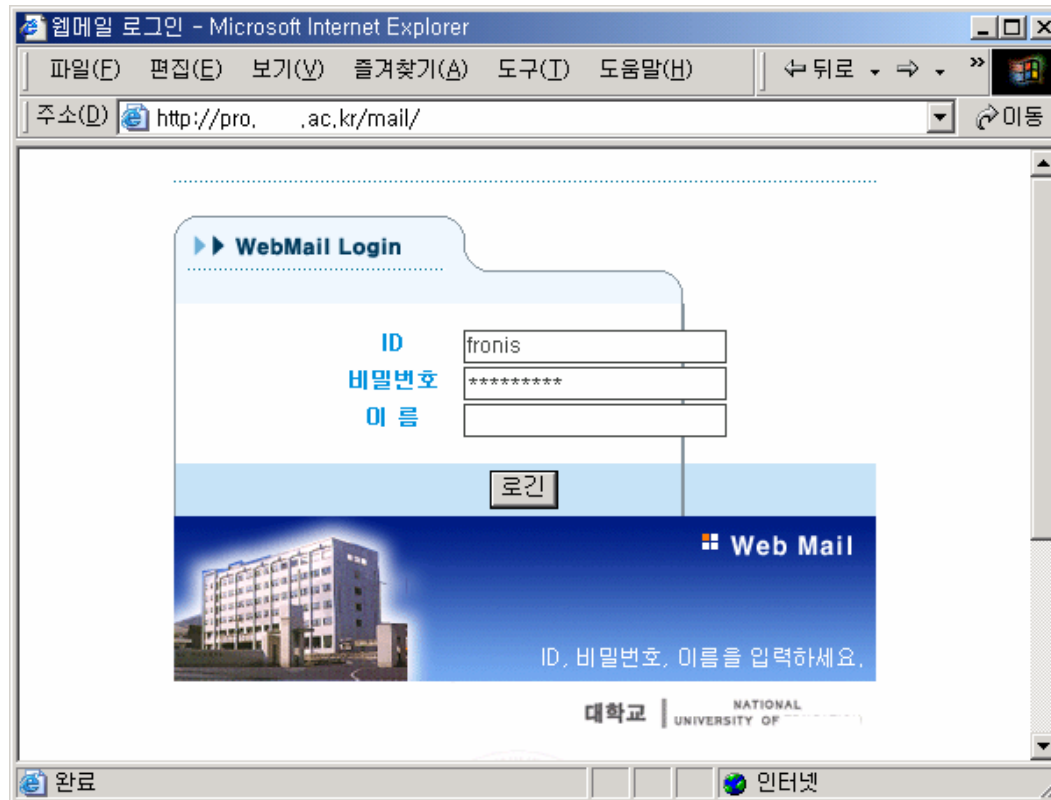


intitle: 관리자 inurl:/admin filetype:html site:net

로그인 페이지

■ 웹 메일 로그인 취약점

웹 메일 ID/PW 자동 로그인 취약점(SPAM 발송 서버로 이용 위험)

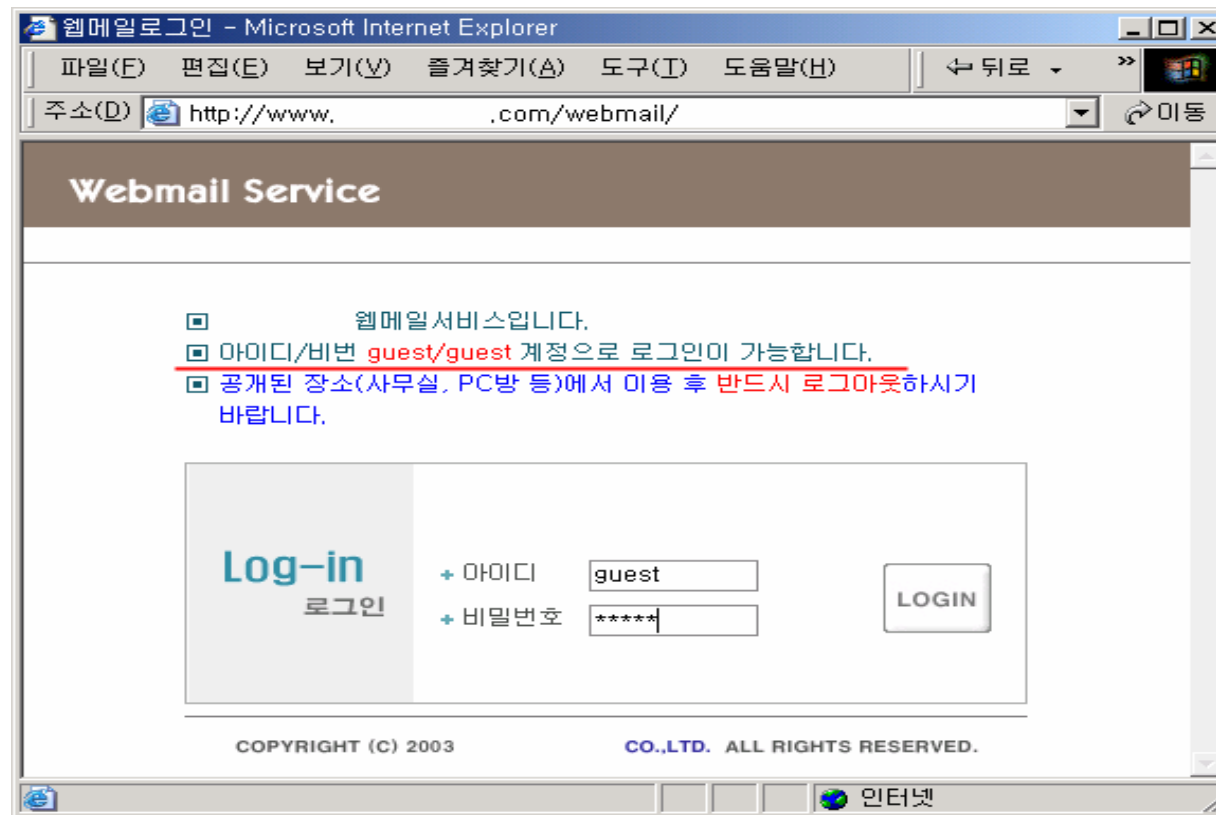


웹 메일 서버 디폴트 ID/PW 검색
intitle:"웹 메일 로그인" inurl:mail site:ac.kr

로그인 페이지

■ 웹 메일 로그인 취약점

웹 메일 ID/PW 디폴트 로그인 취약점(SPAM 발송 서버로 이용 위험)

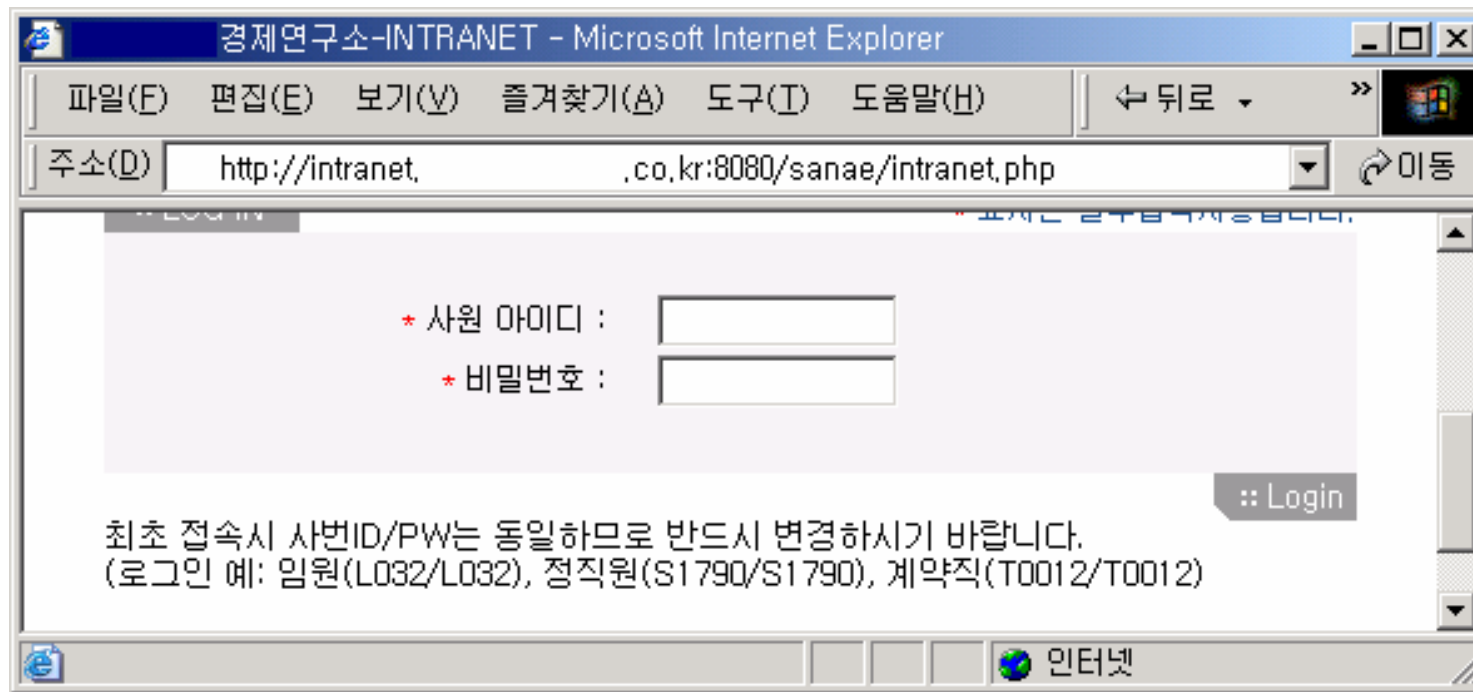


intitle:"웹 메일 로그인" inurl:mail site:com

로그인 페이지

■ 인트라넷 로그인 취약점

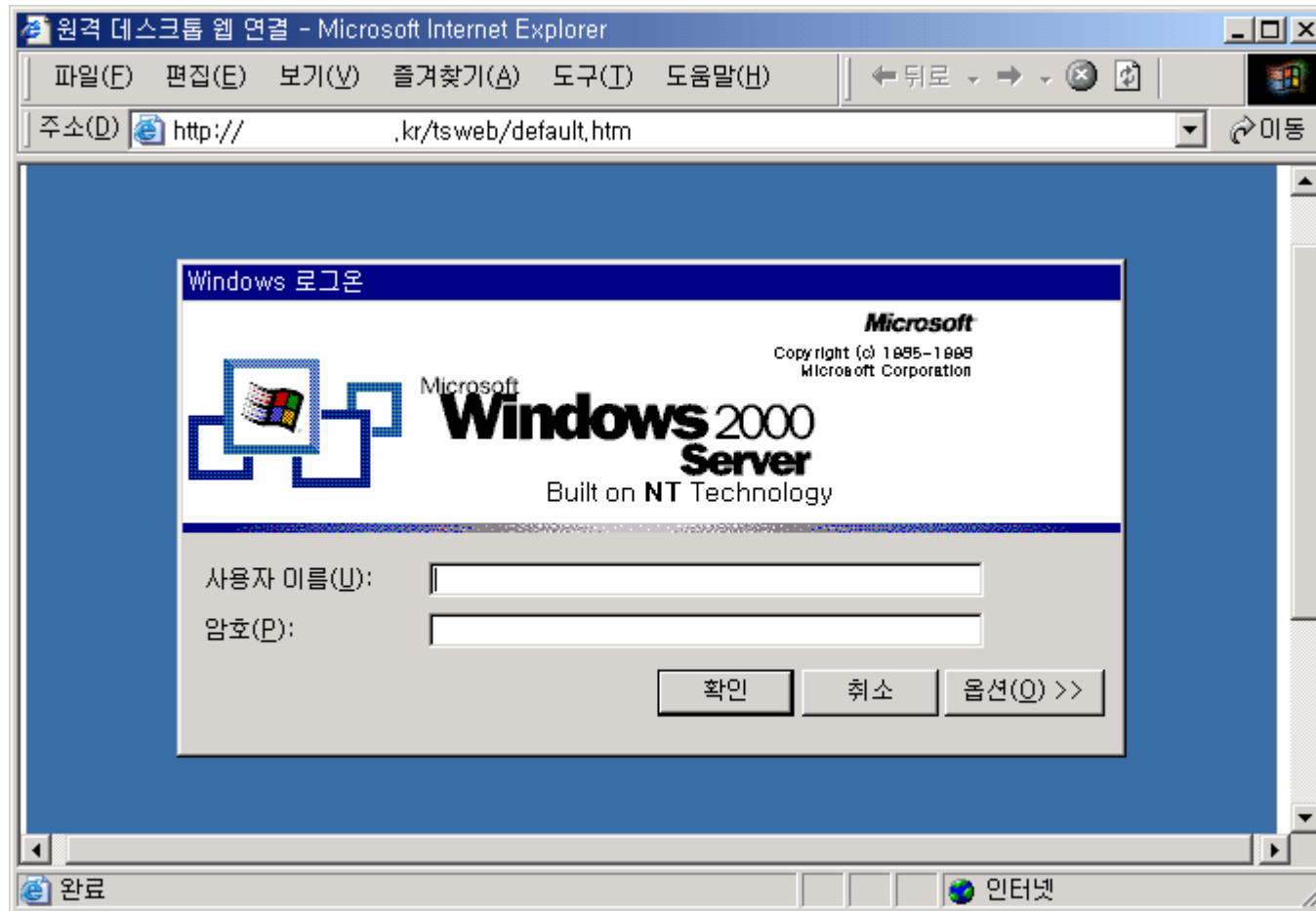
추측하기 쉬운 ID/PW 사용, 회사 내부망 접근 용이



사내 업무용 웹 서버 및 **guessing ID/PW** 검색
intitle:intranet inurl:sanae filetype:php site:co.kr

로그인 페이지

■ 원격 데스크톱 웹 연결



intitle:"원격 데스크톱" inurl:tsweb

로그인 페이지

■ 로그인 페이지 취약점은?

- ✓ 구글은 웹 로그인 페이지를 목록화 할 수 있는 최초의 스캐너
- ✓ 방화벽을 우회 하여 폐쇄망(기업 내부망)에 접근할 수 있는 경로제공
- ✓ 관리자 게시판을 통해 악성 코드 작성 후 서버 관리자 권한 획득 제공
- ✓ 관리용 사이트 접속 후 웹 페이지 위/변조 가능
- ✓ 개인 및 기업 정보 유출 제공
- ✓ 기타

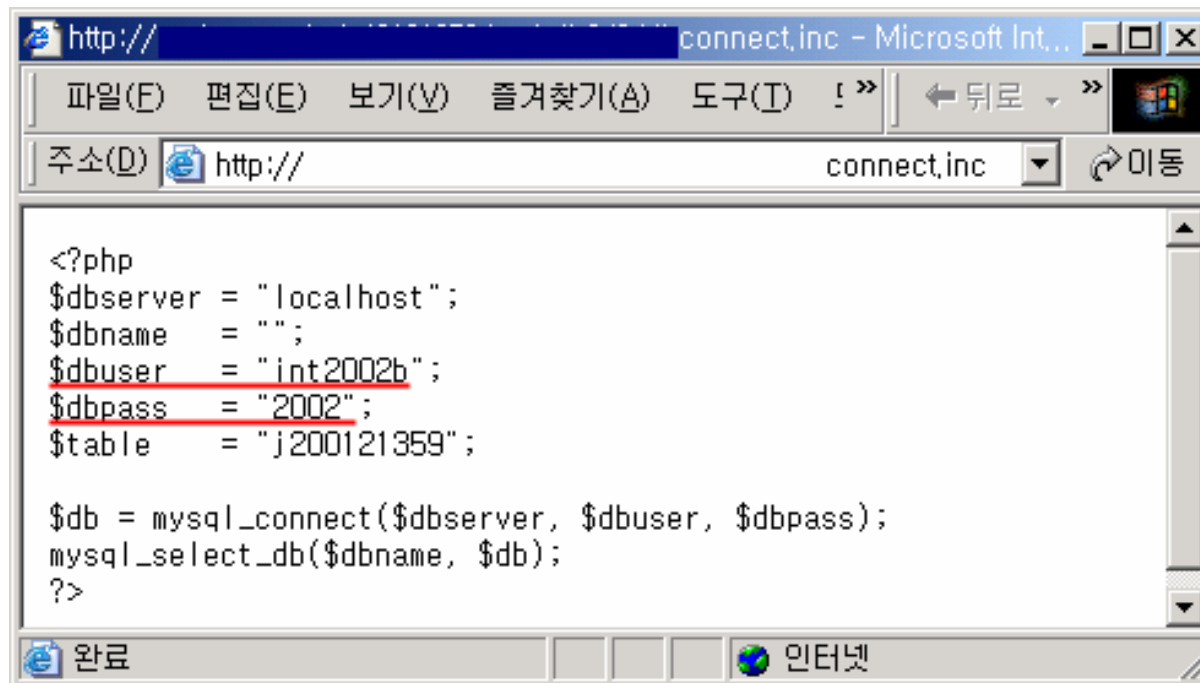
Attack Scenarios

게시판 로그인 페이지 인증 취약점 검색에 따른
RedHat Linux 9.x+PHP 4.x 관리자 권한 획득 시나리오

패스워드 파일

■ 패스워드 파일

- 패스워드를 포함한 파일 검색(DB, AP, Board, Server, FTP등)
- 손쉽게 서비스 및 서버 접근 권한 획득



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

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

MySQL DB ID/PW 검색
intext:mysql_connect+pass

패스워드 파일

▶ 평문 패스워드 파일 검색

[name: = "jbhunt"; password: = "jbhunt"; URL: = "http://home.nc.rr.](#)
[name: = "jbhunt"; password: = "jbhunt"; URL: = "http://home.nc.rr.com/clay123/ref23.html"; Beth Haas name: = "BHaas"; password: = "Beth Haas"; URL: = "http://rr.com/clay123/ref23.html"; name: = "apex"; password: = "apex"; URL: = "http://home.nc.rr.com/clay123/password.log - 2k - 추가 결과 - 저장된 페이지 - 비슷한 페이지](#)

[name: = "23202"; password: = "ilgf"; URL: = "address.htm"; name: = "23203"; password: = "ilgf"; URL: = "address.htm"; name: = "23204"; password: = "ilgf"; URL: = "address.htm"; name: = "23205"; password: = "ilgf"; URL: = "address.htm"; www.lib.nchu.edu.tw/groups/group21/password.log - 9k - 저장된 페이지 - 비슷한 페이지](#)

[name: = "tad"; password: = "homepage"; URL: = "http://www.dob.com.tw"; END_FILE](#)
[dob.tnc.edu.tw/authorHD/1/password.log - 1k - 저장된 페이지 - 비슷한 페이지](#)

[name: = "byrne"; password: = "liquefaction"; URL: = "mainfile.htm"](#)
[name: = "byrne"; password: = "liquefaction"; URL: = "mainfile.htm"; name: = "girl"; password: = "1234"; URL: = "user2.html"; END_FILE](#)
[www.civil.ubc.ca/home/sspark/password.log - 1k - 저장된 페이지 - 비슷한 페이지](#)

[name: = "admin"; password: = "computer"; URL: = "http://members.tripod.com/fr.htm"; name: = "paul"; password: = "papst"; URL: = "http://members.tripod.com/Rick_Cooper/fr.htm"; name: = "phil"; password: = "loop"; URL: = "http://mitglied.lycos.de/Rick_Cooper/mbr/password.log - 2k - 추가 결과 - 저장된 페이지](#)

```
'set db = server.createobject("ADODB.connection") 'db.Provider ...
<% 'set db = server.createobject("ADODB.connection") 'db.Provider = "Microsoft.Jet.
OLEDB.4.0" 'db.ConnectionString = "Data Source=c:\winetpub\wwwroot\bontec.mdb"
'db.Open set db = server.createobject("ADODB.connection") db.Open "sjmc","sjmc" ...
```

[www.sjmc.co.kr/sunjin_board/qna/dbopen.inc - 1k - 추가 결과 - 저장된 페이지 - 비슷한 페이지](#)

```
php $dbserver = "localhost"; $dbname = ""; $dbuser = "int2002b" ...
<?php $dbserver = "localhost"; $dbname = ""; $dbuser = "int2002b"; $dbpass = "2002";
$table = "1200121359"; $db = mysql_connect($dbserver, $dbuser, $dbpass);
mysql_select_db($dbname, $db); ??
cs.hcc.ac.kr/~i0121359/webdb2/8/dbconnect.inc - 1k - 추가 결과 - 저장된 페이지 - 비슷한 페이지
```

[db.hyomok-lib.daegu.kr/oci8.inc](#)
파일 타입: 불분명한 타입 - HTML 버전
추가 결과 - 비슷한 페이지

[db.hyomok-lib.daegu.kr/new/oci8.inc](#)
파일 타입: 불분명한 타입 - HTML 버전
추가 결과 - 비슷한 페이지
[db.hyomok-lib.daegu.kr에서 검색]

[www.hanshin.ac.kr:8080/imsi/html/include/db.inc](#)
파일 타입: 불분명한 타입 - HTML 버전
추가 결과 - 비슷한 페이지

[www.namunet.co.kr/db/visit/connect.inc](#)
파일 타입: 불분명한 타입 - HTML 버전
추가 결과 - 비슷한 페이지

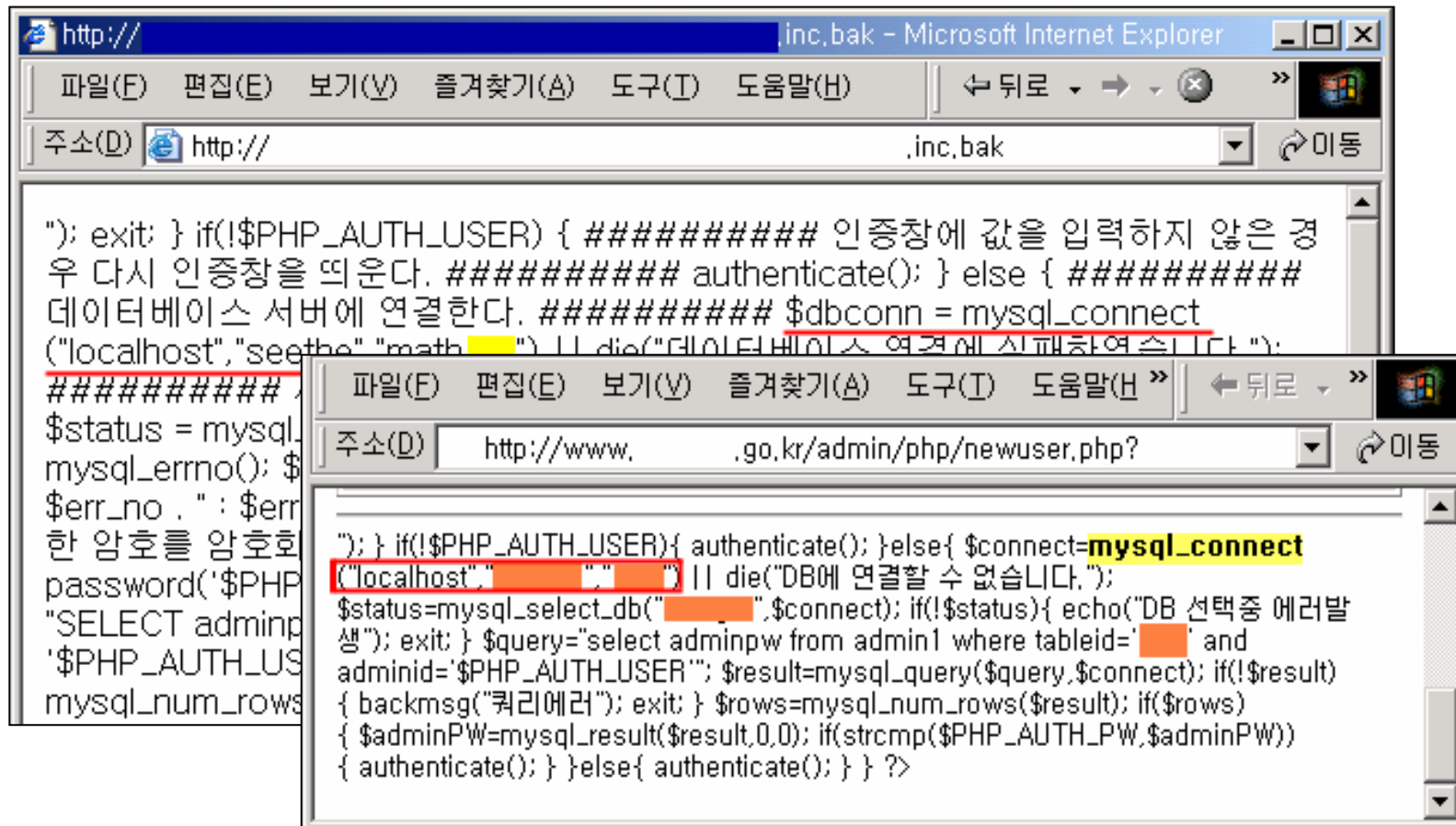
[www.namunet.co.kr/db/board/connect.inc](#)
파일 타입: 불분명한 타입 - HTML 버전
추가 결과 - 비슷한 페이지

```
$host="localhost"; $user=""; $passwd=""; $db=""; ...
<? $host="localhost"; $user=""; $passwd=""; $db=""; $table="cat";
$system_passwd=""; $tb_bgcolor="#F3F3F3"; $fd_color1="#FFFFFF"; $fd_color2="#
FFFFFF"; $tr_bgcolor="#FFFFFF"; $th_bkpc="#FFFFFF"; $tbl="#444343"; $ulink
```

!Hint: filetype:, intext:

패스워드 파일

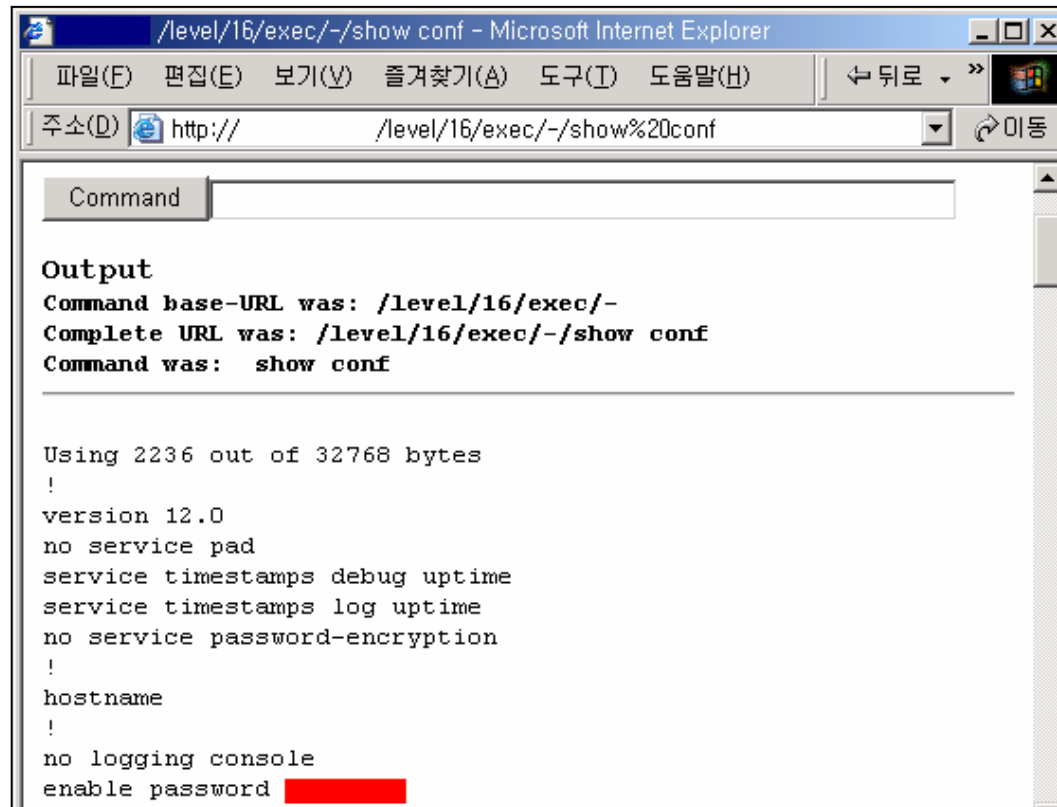
■ 데이터 베이스 로그인 ID/PW 검색



intext:mysql_connect filetype:bak

패스워드 파일

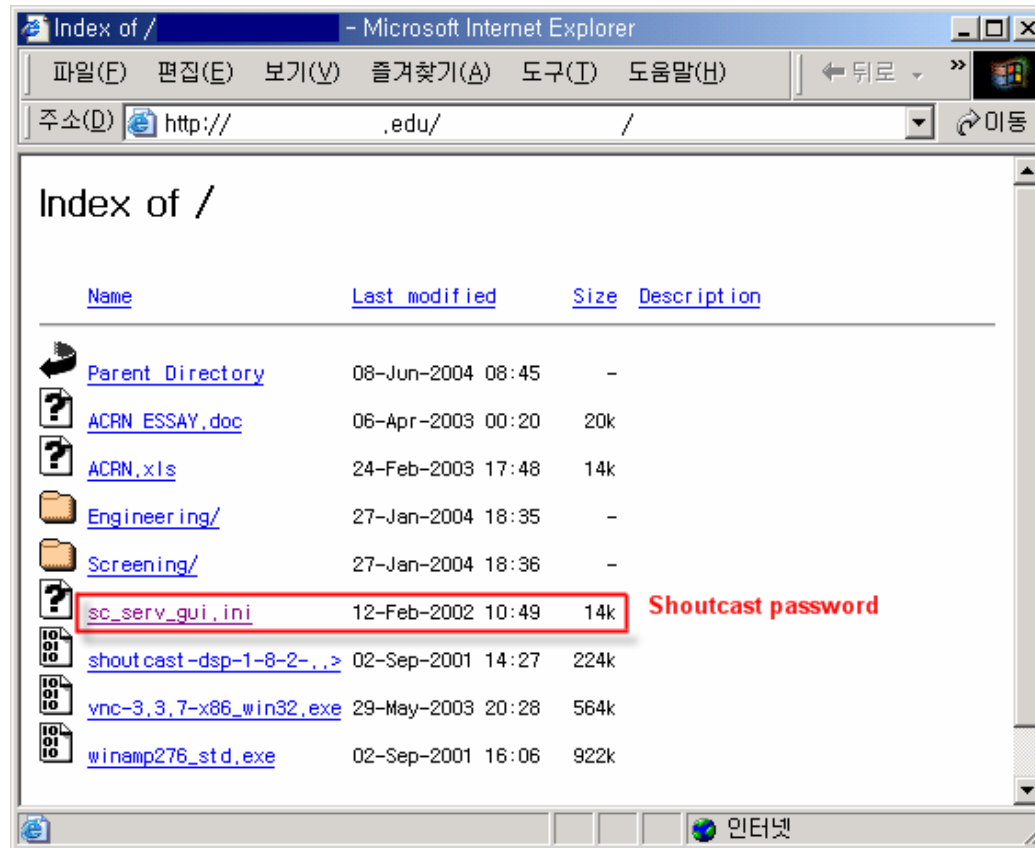
- 스위치 취약점
Cisco IOS HTTP 인증 취약점 검색



Cisco 웹 인증 취약점 enable패스워드 검색
inurl:"/level/*/exec/" intext:password

패스워드 파일

- Shoutcast server
winamp 음악 방송 서버 패스워드 파일 검색

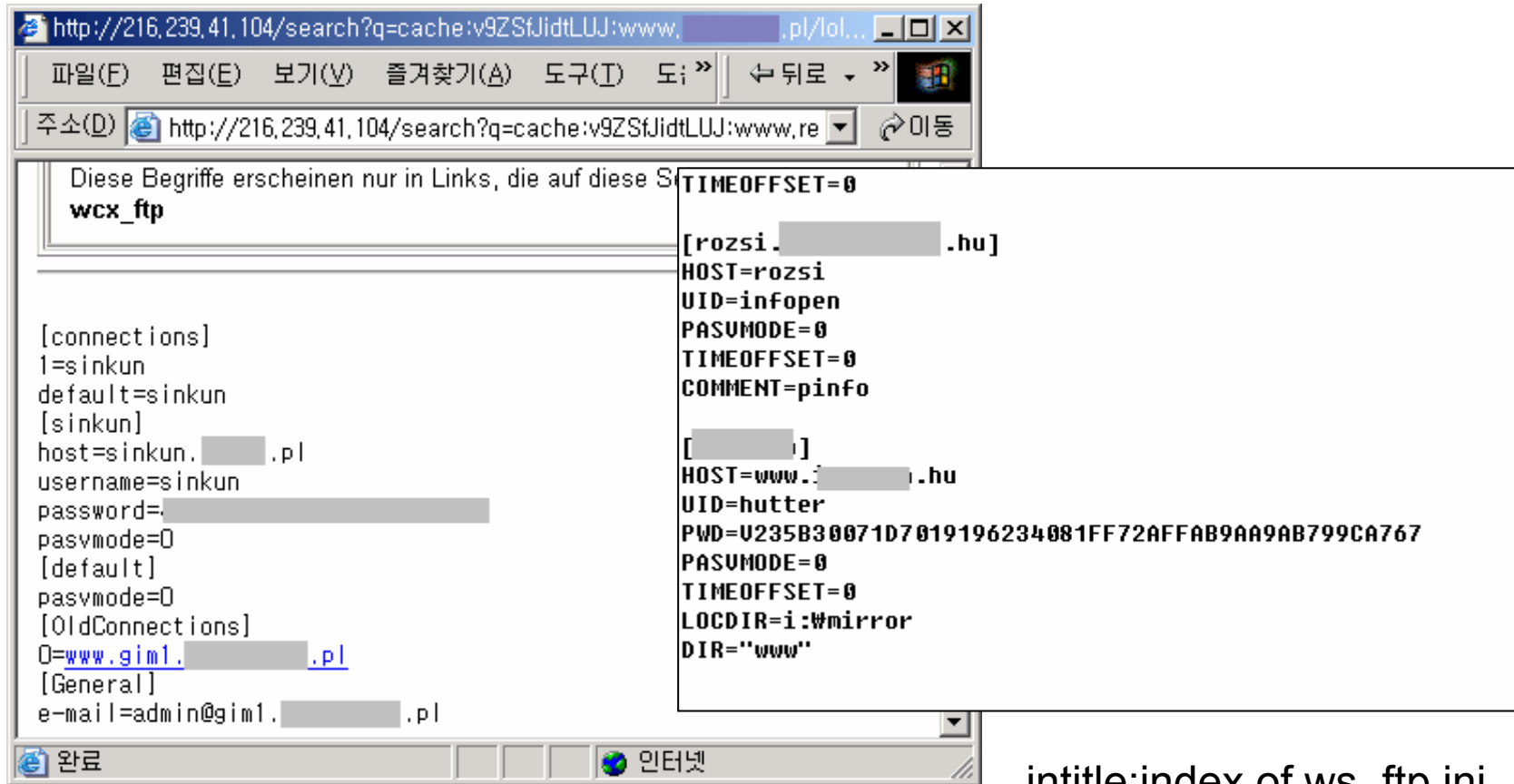


Shoutcast ID/PW 검색
intitle:index.of intext:sc_serv_gui.ini

패스워드 파일

■ FTP

FTP 서버 접속 ID/PW 검색

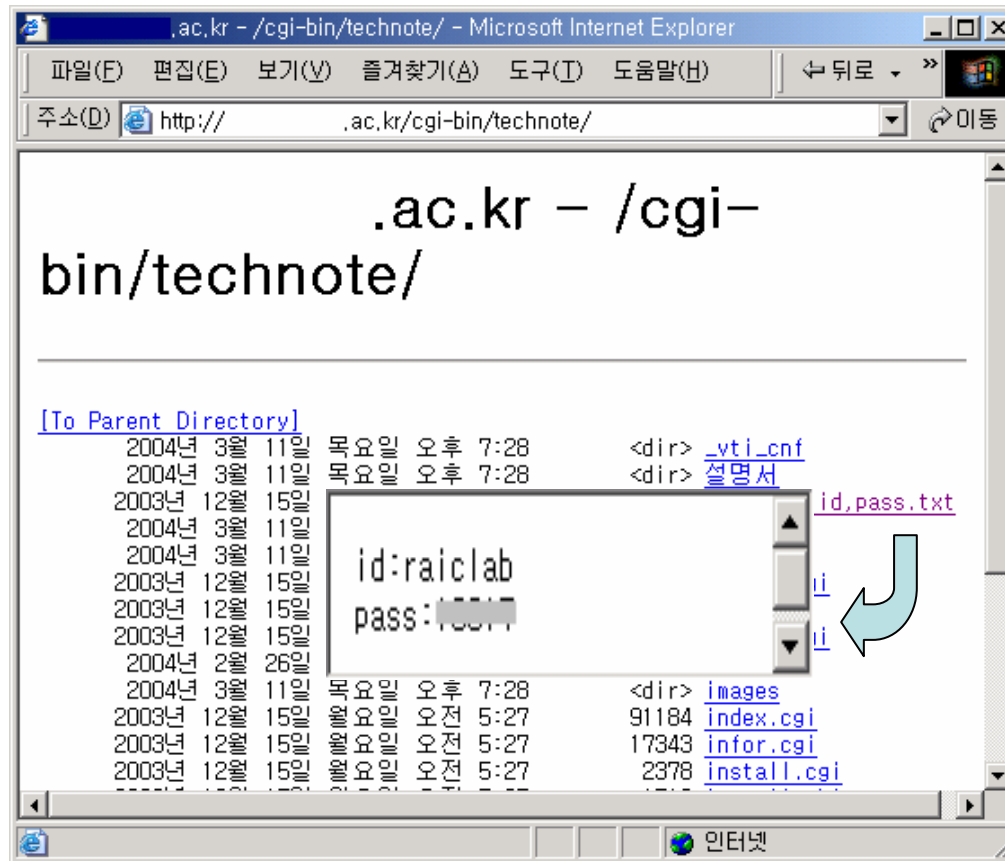


filetype:ini wcx_ftp

intitle:index.of ws_ftp.ini

패스워드 파일

- 게시판
게시판 관리자 접속 ID/PW 검색



intitle:technote inurl:cgi-bin

Attack Scenarios

Cisco HTTP 인증 취약점 검색을 통한 switching 무력화
악성 서버에서 모든 네트워크 트래픽 Sniffing 시나리오

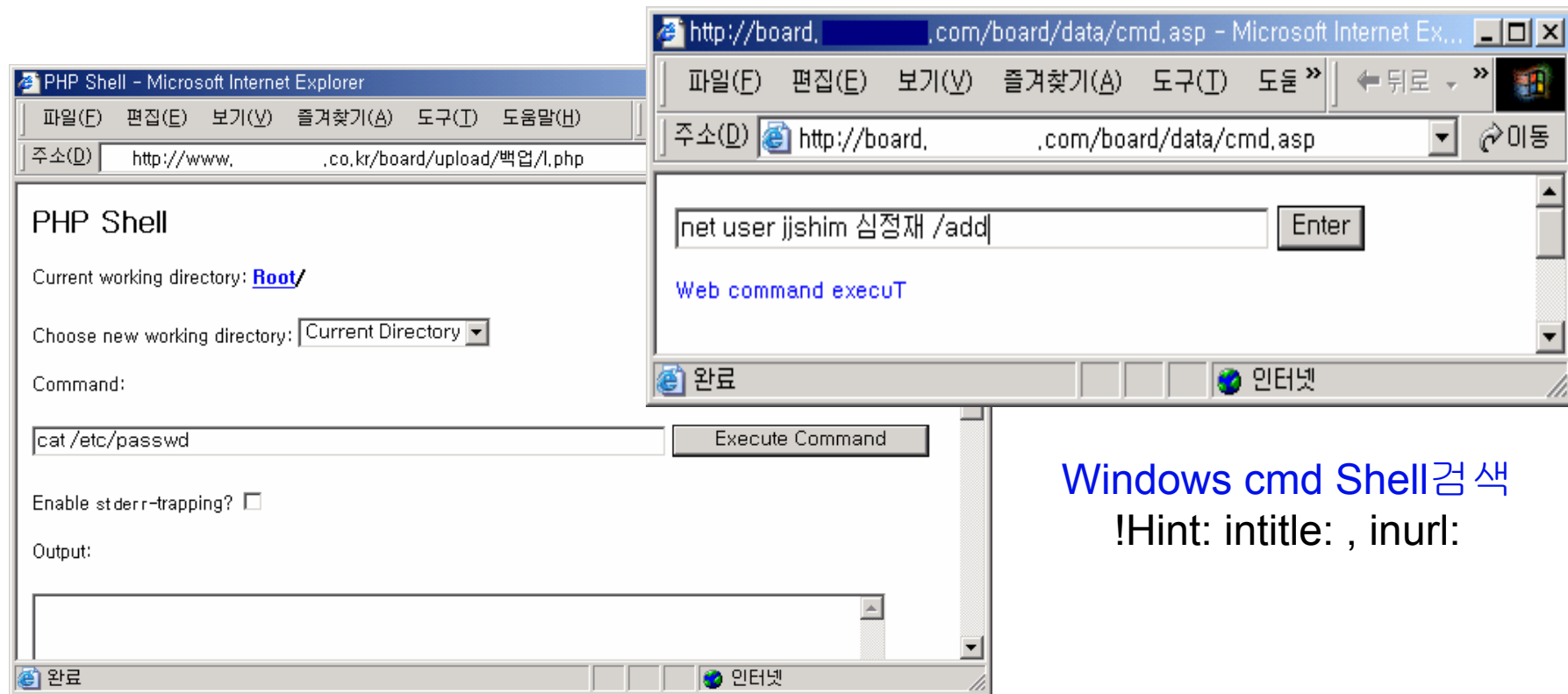
Attack Scenarios

Serv-U 환경 설정 파일 검색 결과에 따른
Windows XP Professional(SP1), Serv-U4.3
서버 관리자 권한 획득 시나리오

해킹 파일

■ 해킹 파일 검색

피해 시스템에 남아 있는 해킹 관련 파일 검색



Windows cmd Shell 검색

!Hint: intitle: , inurl:

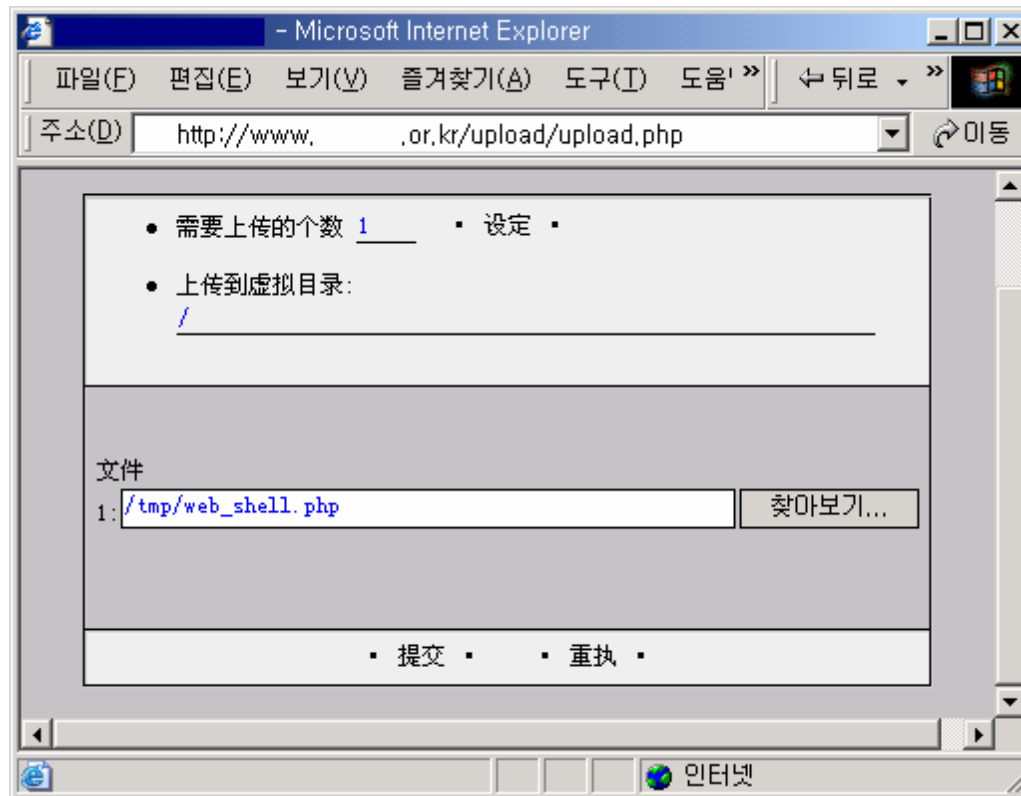
PHP Shell 검색

intitle:"PHP Shell *" intext:Command filetype:php

해킹 파일

■ 해킹파일 검색

업로드 실행 파일, 웜, 바이러스, 기타 해킹 파일 검색



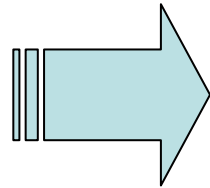
php uploader 검색
intext:文件 filetype:php inurl:up

CGI 스캐너

■ CGI 스캐너

- 많은 웹 서버 취약점을 찾기 위해 공격자들은 CGI 스캐너를 이용.
- 구글 검색 엔진을 통해 보다 정확한 취약 서버 수집 가능

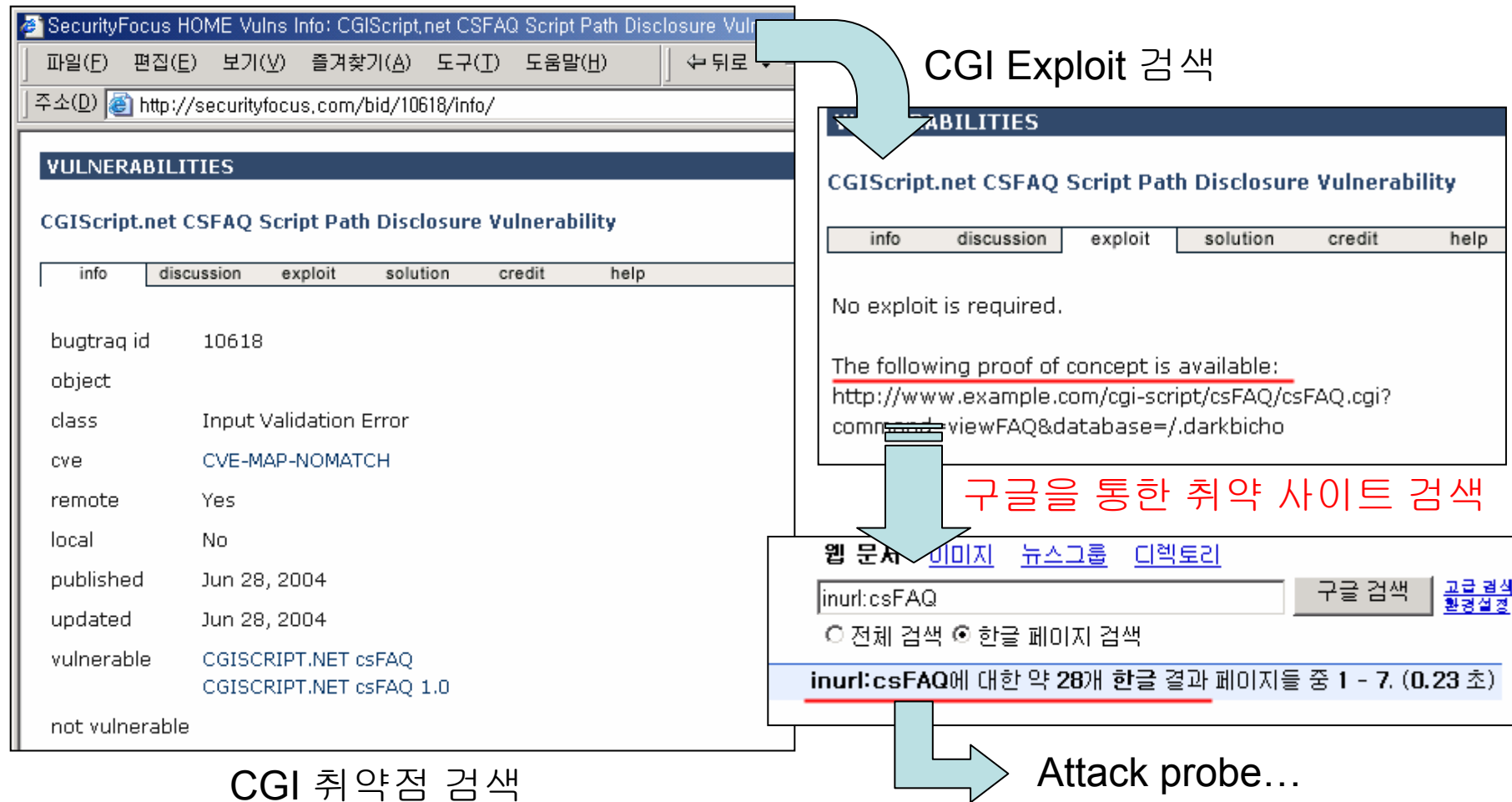
CGI 스캐너
/_vti_bin/shtml.exe
/cgi-bin/finger
/cgi-bin/guestbook.pl
/_vti_pvt/admin.pwd
/phpBB/search.php
/zeroboard/login.php
/cgi-bin/14all.cgi



구글 검색
inurl:/_vti_bin/shtml.exe
inurl:/cgi-bin/finger
Inurl:cgi-bin/guestbook.pl
Inurl:/_vti_pvt/admin.pwd
Inurl:/phpBB/search.php
Inurl:/zeroboard/login.php
inurl:/cgi-bin/14all.cgi

CGI 스캐너

■ 보안 사이트에서 CGI 관련 취약점 정보 획득



CGI 스캐너

■ Other Vulnerable?

그 외 다양한 취약점 구글 검색을 통해 스캐닝 가능

VULNERABILITIES

by vendor by title by keyword by bugtraq id by cve id by published date

Published Date: 2004 August 04 Submit

04-08-2004: StackDefender ObjectAttributes Invalid Pointer Dereference Vulnerability

04-08-2004: StackDefender BaseAddress Invalid Pointer Dereference Denial Of Service Vulnerability

04-08-2004: Pete Stein GoScript Remote Command Execution Vulnerability

04-08-2004: eNdongia Search Form Cross-Site Scripting Vulnerability

04-08-2004: DGen Emulator Symbolic Link Vulnerability

04-08-2004: Jetbox One Plaintext Password Storage Vulnerability

04-08-2004: Jetbox One Remote Server-Side Script Execution Vulnerability

04-08-2004: WackoWiki TextSearch Cross-Site Scripting Vulnerability

04-08-2004: Acme httpd Directory Traversal Vulnerability

04-08-2004: PHP-Nuke Delete God Admin Access Control Bypass

04-08-2004: Multiple Free Web Chat Denial Of Service Vulnerability

04-08-2004: YaST2 Utility Library File Verification Shell Code Injection Vulnerability

웹 문서 이미지 뉴스그룹 디렉토리

inurl:"go.cgi" 구글 검색 고급 검색 환경설정

전체 검색 한글 페이지 검색

inurl:"go.cgi"에 대한 약 853개 한글 결과 페이지들 중 1 - 10. (1.08 초)

웹 문서 이미지 뉴스그룹 디렉토리

inurl:"mod.php" 구글 검색 고급 검색 환경설정

전체 검색 한글 페이지 검색

inurl:"mod.php"에 대한 약 1,490개 한글 결과 페이지들 중 1 - 10. (0.09 초)

웹 문서 이미지 뉴스그룹 디렉토리

inurl:"phpnuke/admin.php" 구글 검색 고급 검색 환경설정

전체 검색 한글 페이지 검색

inurl:"phpnuke/admin.php"에 대한 약 116개 결과들 중 1 - 10. (0.07 초)

Attack Scenarios

Securityfocus.com bid DB 취약 정보 수집

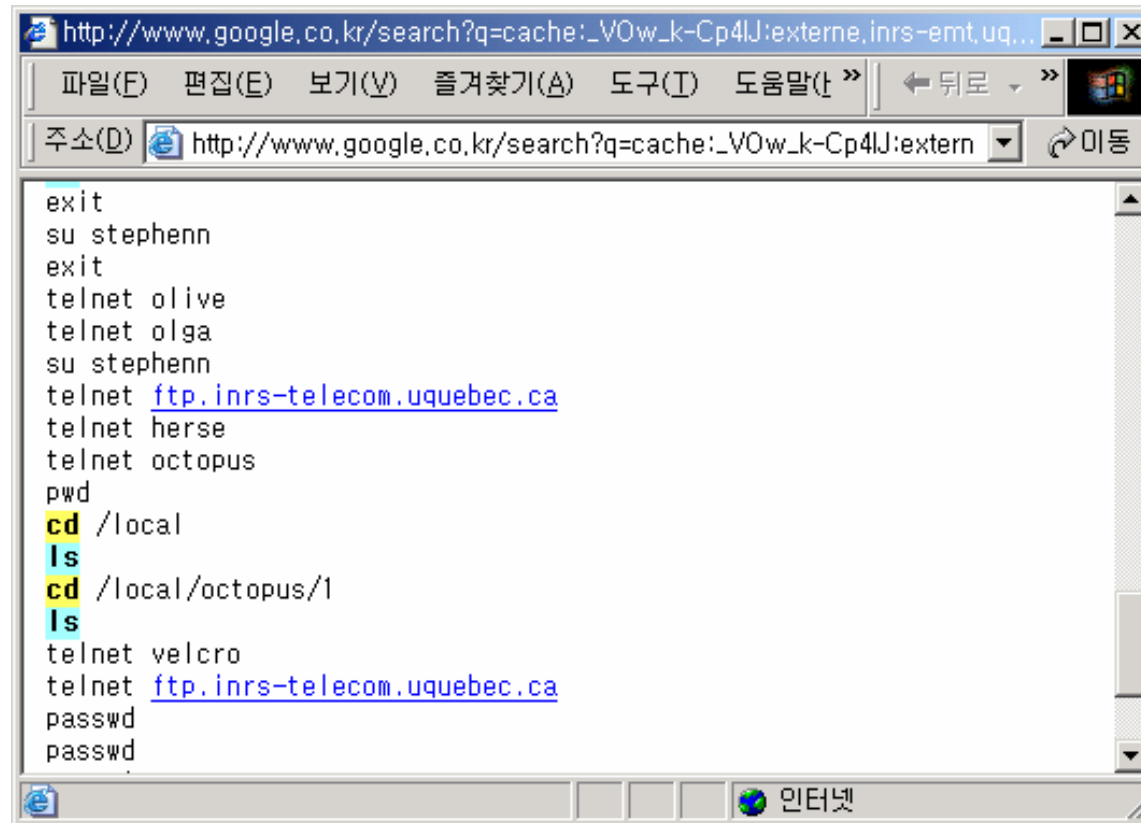
구글 취약 서버 스캐닝

phpBB 2.0.10 관리자 패스워드 획득 시나리오

민감한 데이터

■ 민감한 데이터

외부 공개가 금지된 민감한 데이터 검색



```
http://www.google.co.kr/search?q=cache:_V0w_k-Cp4IJ:externe.inrs-emt.uq...
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H) >>
주소(D) http://www.google.co.kr/search?q=cache:_V0w_k-Cp4IJ:extern
미동

exit
su stephenn
exit
telnet olive
telnet olga
su stephenn
telnet ftp.inrs-telecom.quebec.ca
telnet herse
telnet octopus
pwd
cd /local
ls
cd /local/octopus/1
ls
telnet velcro
telnet ftp.inrs-telecom.quebec.ca
passwd
passwd
```

Linux Bash Shell History 파일 검색

intitle:index.of .bash_history or index.of .sh_history

민감한 데이터

■ 민감한 데이터

외부 공개가 금지된 민감한 데이터 검색

The image displays four screenshots of Google search results, each showing a search query and the number of results found. The results are as follows:

- Query: `intext:대외비 filetype:doc`. Results: 약 25개 결과들 중 1 - 10, (0,20 초)
- Query: `intext:대외비 filetype:pdf`. Results: 약 141개 결과들 중 1 - 10, (0,11 초)
- Query: `intext:confidential filetype:pdf`. Results: 약 191개 한글 결과 페이지들 중 1 - 10, (0,87 초)
- Query: `intext:confidential filetype:doc`. Results: 약 56개 한글 결과 페이지들 중 1 - 10, (0,18 초)

민감한 파일 검색
allintext:대외비

포트 스캐너

■ 포트 스캐닝

포트번호 포함하여 몇 개의 구글 키워드를 사용하면 현재 사용중인 응용프로그램 이름까지 검색 가능



Google 웹 문서 이미지 뉴스그룹 디렉토리

"VNC Desktop" inurl:5800

전체 검색 한글 페이지 검색

웹 문서 **"VNC Desktop" inurl:5800에 대한 약 102개 결과들 중 1 - 10, (0.46 초)**

[Ultr@VNC Desktop \[daibert\]](#) ----- Ultr@VNC Home Page is http ...
파일 타입: 불분명한 타입 - HTML 버전
[daibert.dynu.net:5800/](#) - [비슷한 페이지](#)

[VNC desktop \[sunbeam\]](#)
파일 타입: 불분명한 타입 - HTML 버전
[sunbeam.uoregon.edu:5800/](#) - [비슷한 페이지](#)

[VNC desktop \[computer\]](#)
파일 타입: 불분명한 타입 - HTML 버전
[usha.dyndns.org:5800/](#) - [추가 결과](#) - [비슷한 페이지](#)

[VNC desktop \[scitest01\]](#)
파일 타입: 불분명한 타입 - HTML 버전
[solidview.solidconcepts.com:5800/](#) - [비슷한 페이지](#)

[VNC desktop \[moobert\]](#)
파일 타입: 불분명한 타입 - HTML 버전
[moobert.2y.net:5800/](#) - [비슷한 페이지](#)

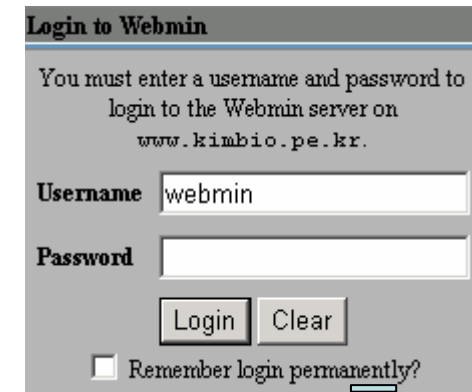
"inurl:5800" 은
검색오류 높음

원격 터미널 VNC 검색
"VNC Desktop" inurl:5800

포트 스캐너

■ Webmin 스캐닝

웹을 이용한 시스템 관리 프로그램 webmin 구글 검색



Login!

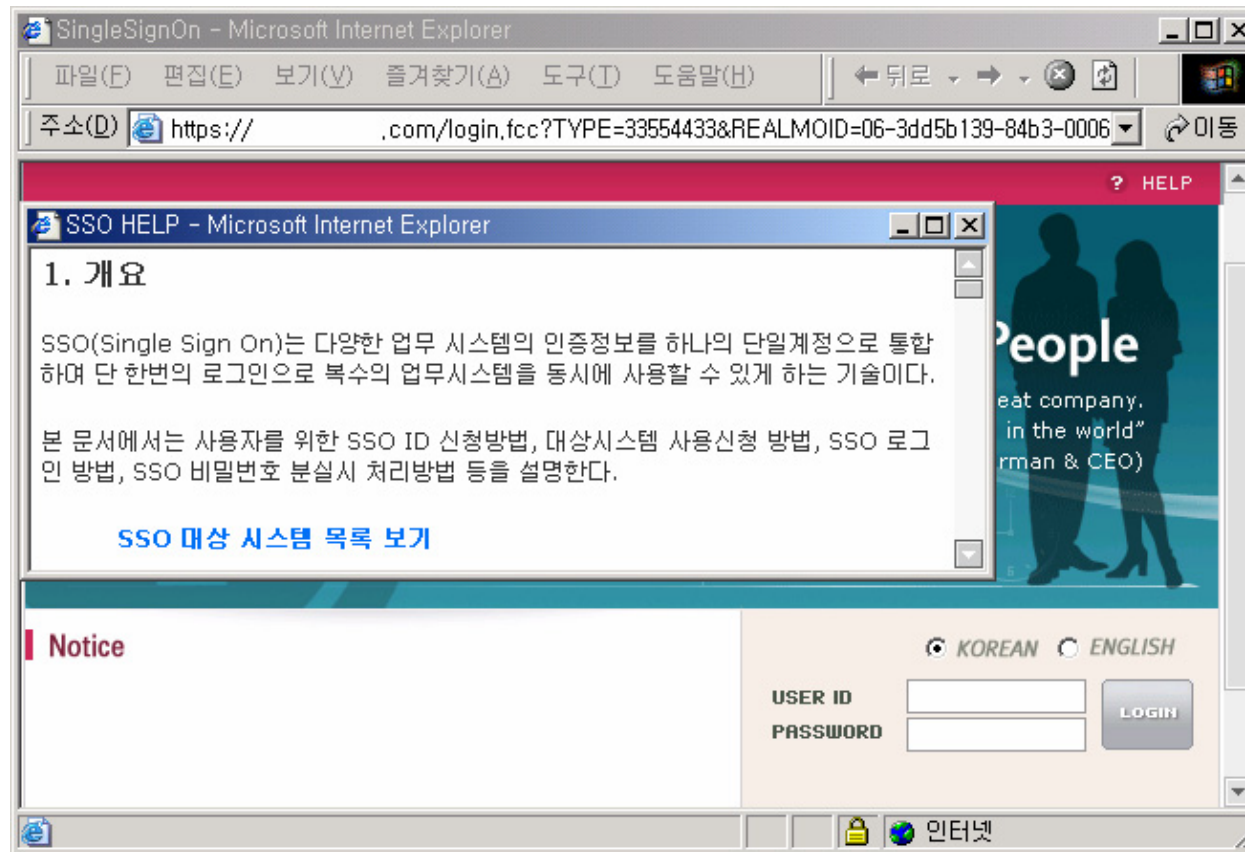


`inurl:':10000' intext:webmin`

포트 스캐너

■ 폐쇄 웹 서버 검색

외부에 공개되지 않는 웹 서버 검색

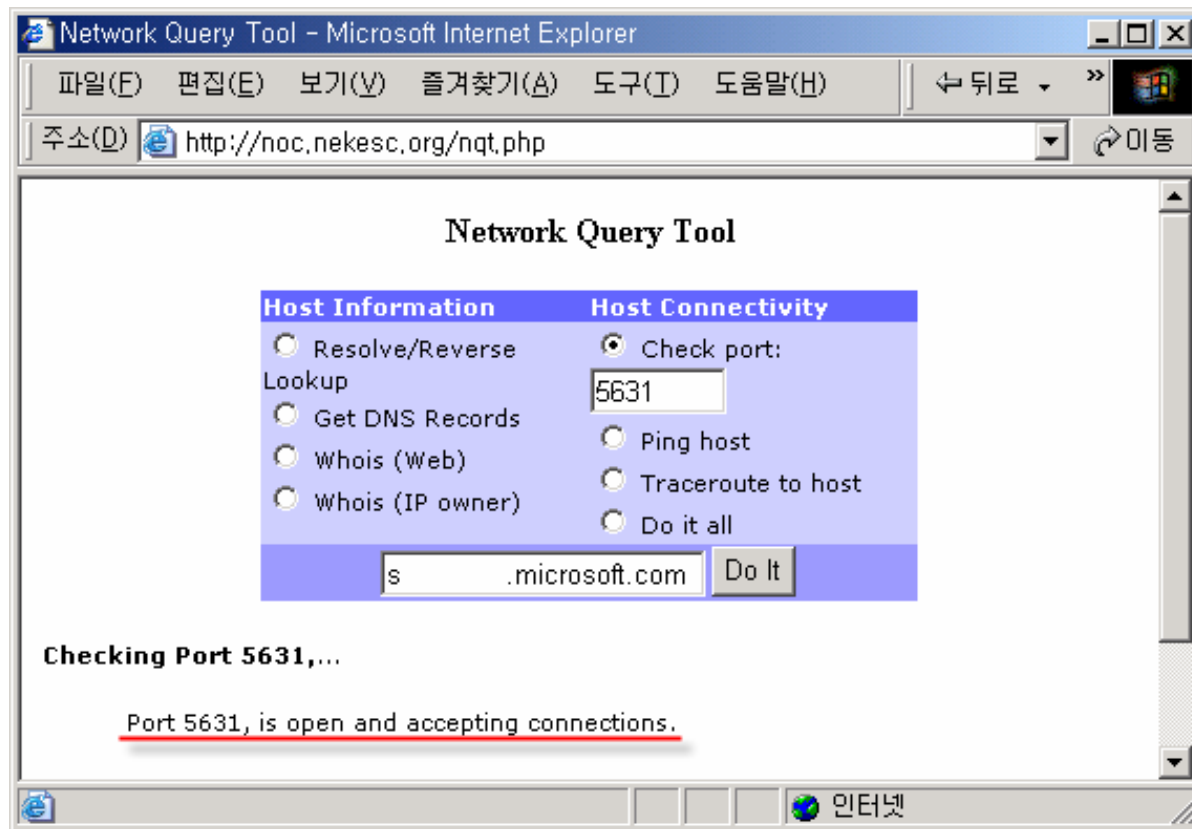


inurl:8080 -inurl:board -intext:8080 or inurl:8000 -inurl:board -intext:8000

포트 스캐너

■ 공개된 웹 포트 스캐너

웹에 공개된 다양한 스캐닝 도구 이용



intitle:"Network query tool" filetype:php or inurl:nqt.php

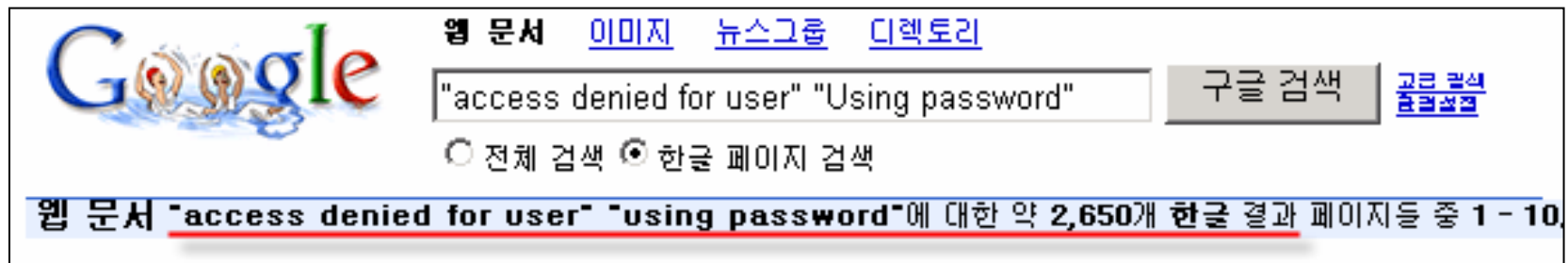
SQL 데이터 수집

■ SQL Data 수집

SQL 주입 공격이나 SQL DB 정보를 수집하기 위한 구글 검색

❖ SQL 로그인 사용자 ID검색

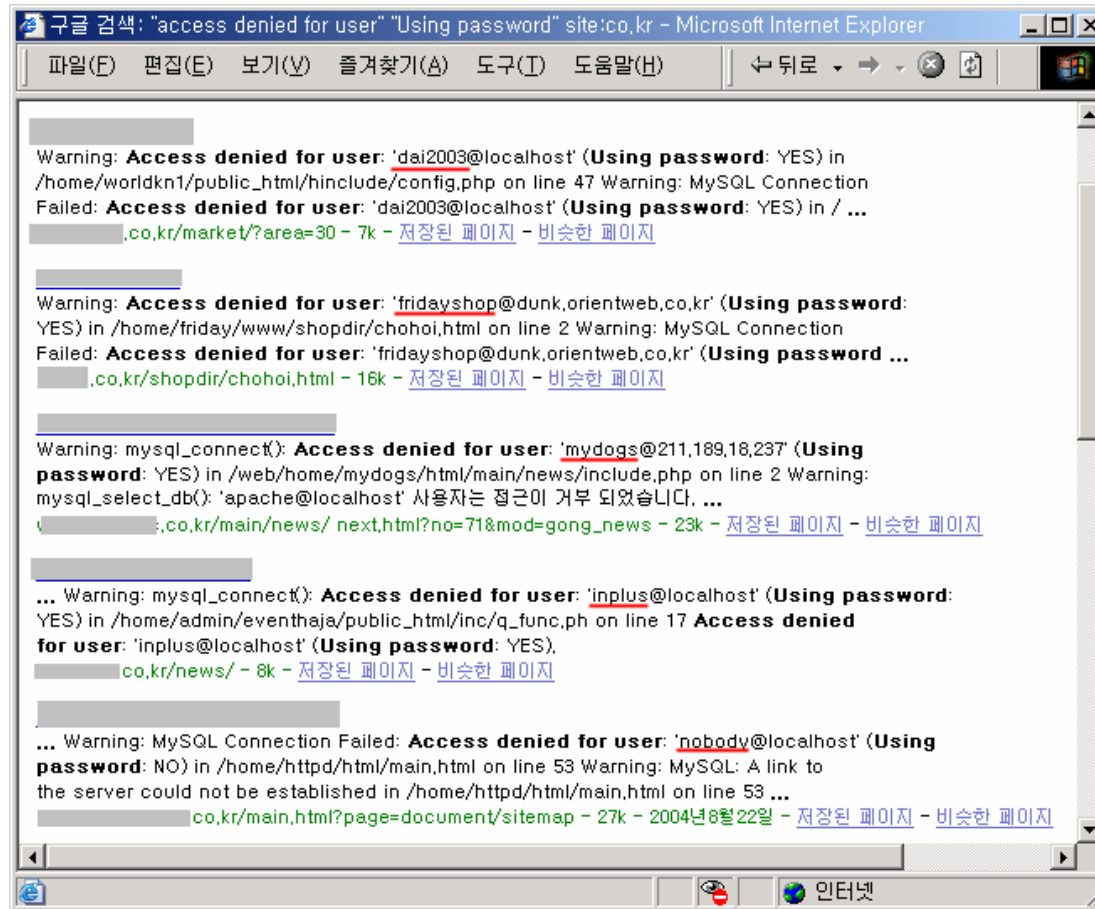
DB 오류 메시지를 기초로 하여 SQL DB 접근 ID 검색



"access denied for user" "using password"

SQL 데이터 수집

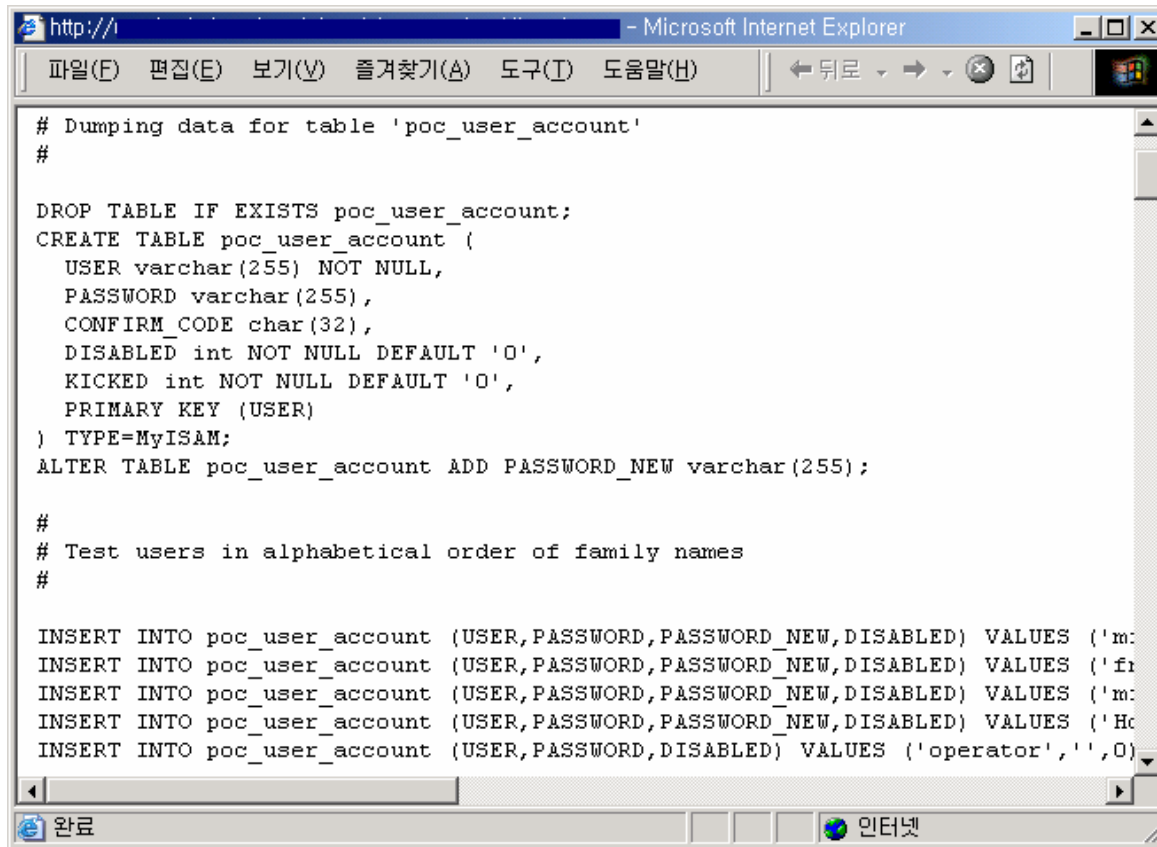
❖ SQL 사용자명 검색



"access denied for user" "using password" site:co.kr

SQL 데이터 수집

- ❖ SQL 스키마 검색
데이터 베이스 구성 정보를 획득



```
# Dumping data for table 'poc_user_account'
#

DROP TABLE IF EXISTS poc_user_account;
CREATE TABLE poc_user_account (
  USER varchar(255) NOT NULL,
  PASSWORD varchar(255),
  CONFIRM_CODE char(32),
  DISABLED int NOT NULL DEFAULT '0',
  KICKED int NOT NULL DEFAULT '0',
  PRIMARY KEY (USER)
) TYPE=MyISAM;
ALTER TABLE poc_user_account ADD PASSWORD_NEW varchar(255);

#
# Test users in alphabetical order of family names
#

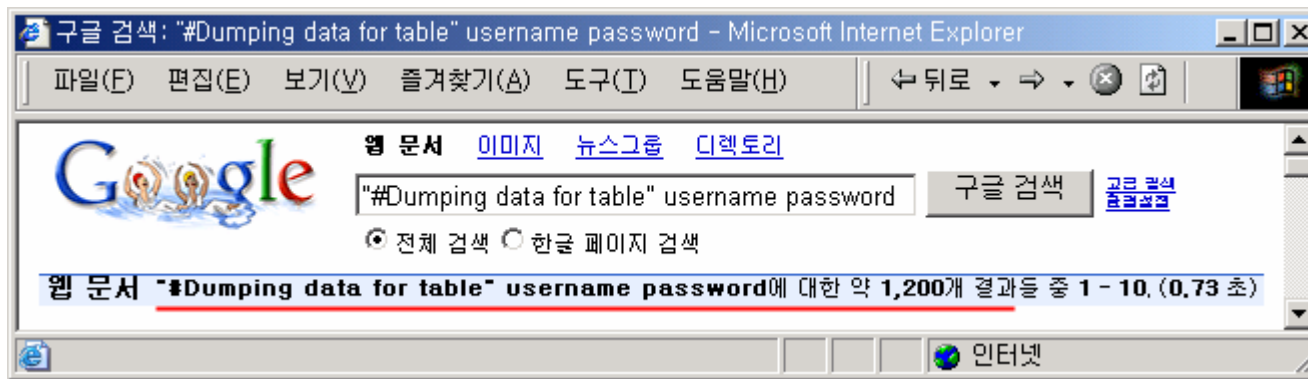
INSERT INTO poc_user_account (USER,PASSWORD,PASSWORD_NEW,DISABLED) VALUES ('m:
INSERT INTO poc_user_account (USER,PASSWORD,PASSWORD_NEW,DISABLED) VALUES ('fr
INSERT INTO poc_user_account (USER,PASSWORD,PASSWORD_NEW,DISABLED) VALUES ('m:
INSERT INTO poc_user_account (USER,PASSWORD,PASSWORD_NEW,DISABLED) VALUES ('Hc
INSERT INTO poc_user_account (USER,PASSWORD,DISABLED) VALUES ('operator','',0)
```

"# Dumping data for table"

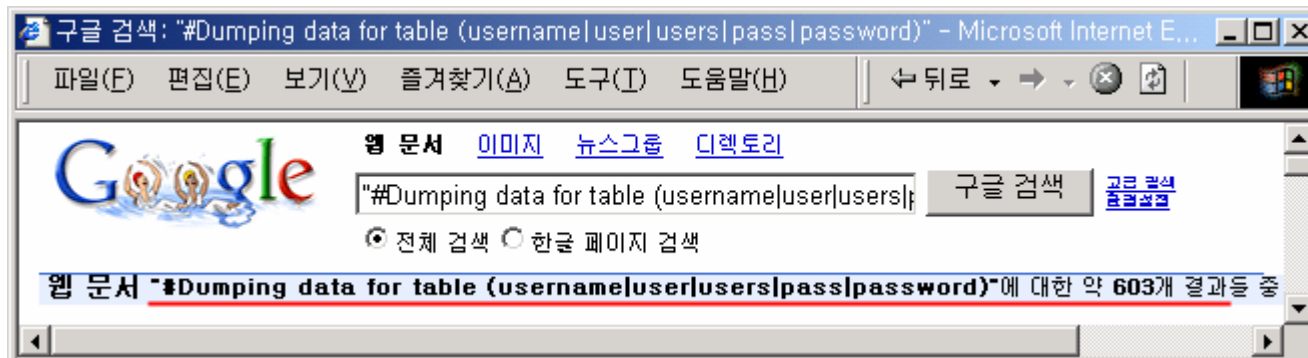
SQL 데이터 수집

❖ SQL 스크립트 검색

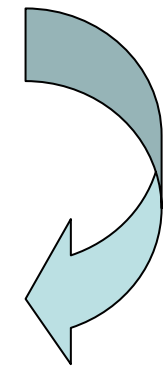
DB 백업 혹은 자동화 작업 과정에서 필요한 SQL 스크립트 검색 후 ID/PW 정보 획득



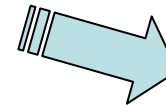
“# Dumping data for table” username password



“# Dumping data for table(username|user|pass|password|passwd)”



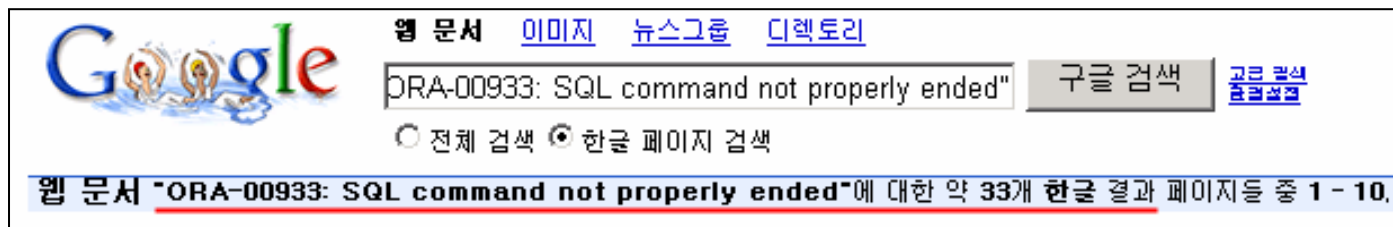
Detail



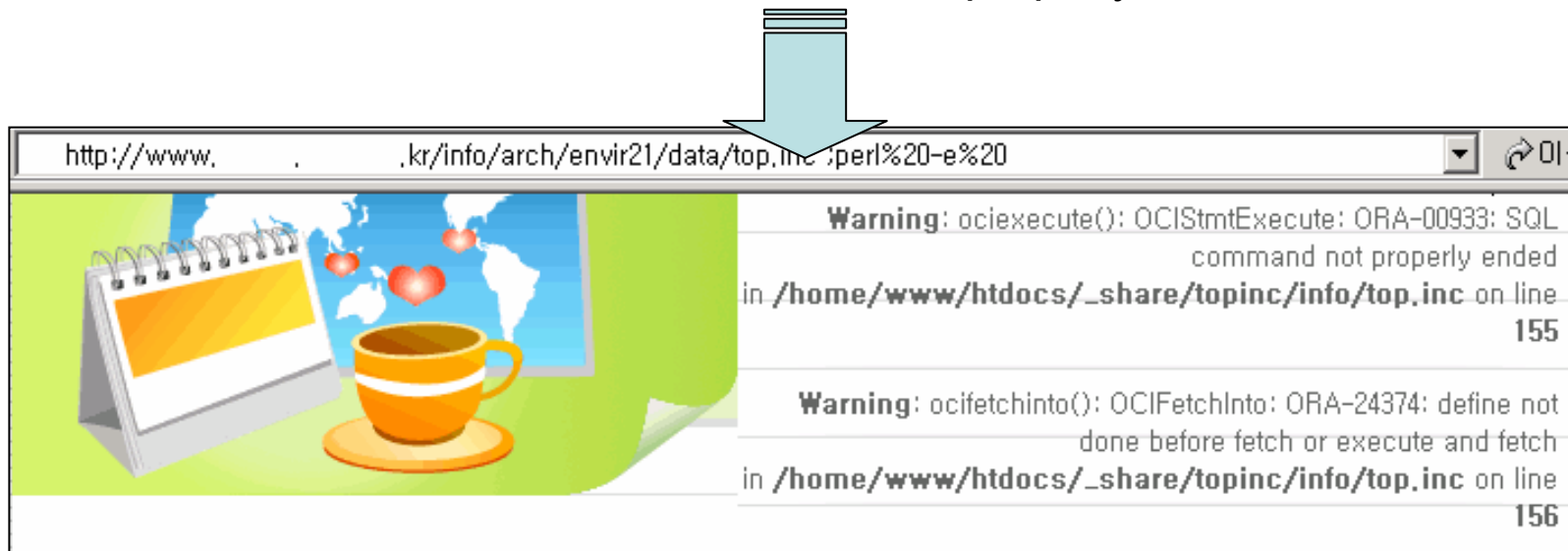
more?
filetype:

SQL 데이터 수집

- ❖ SQL Injection 검색
SQL Injection 공격 가능한 웹 서버 및 취약 파일 검색

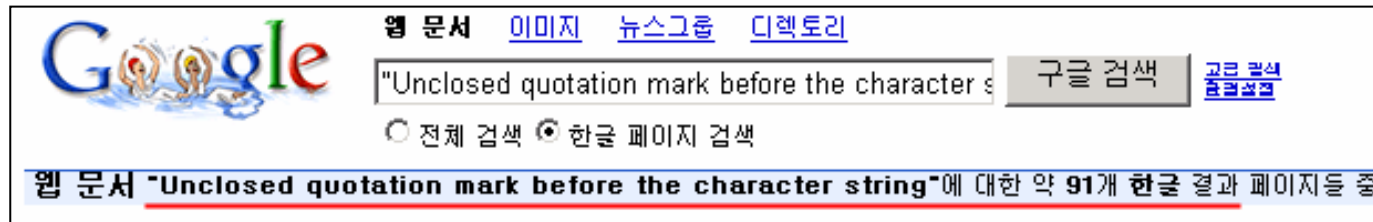


"ORA-00933: SQL command not properly ended"

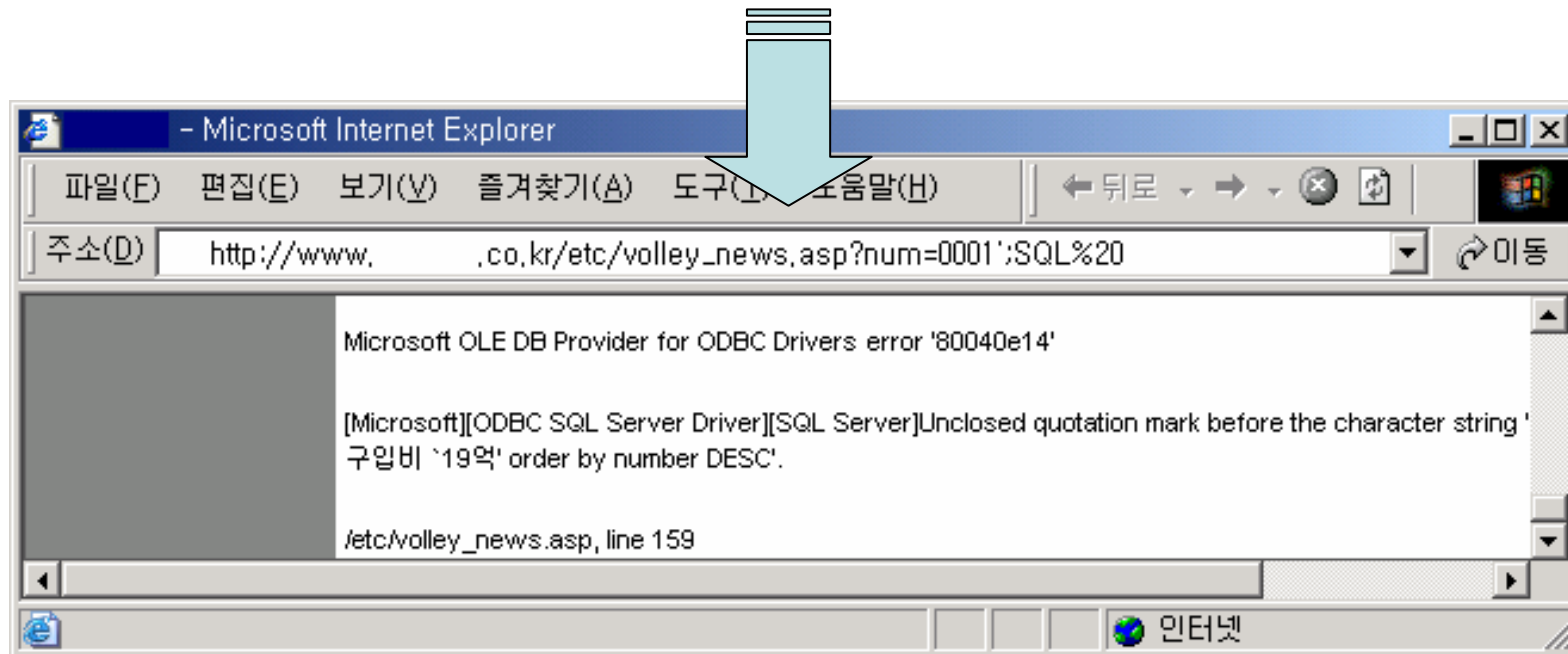


SQL 데이터 수집

❖ SQL Injection 취약 서버 검색



“Unclosed quotation mark before the character string”



SQL 데이터 수집

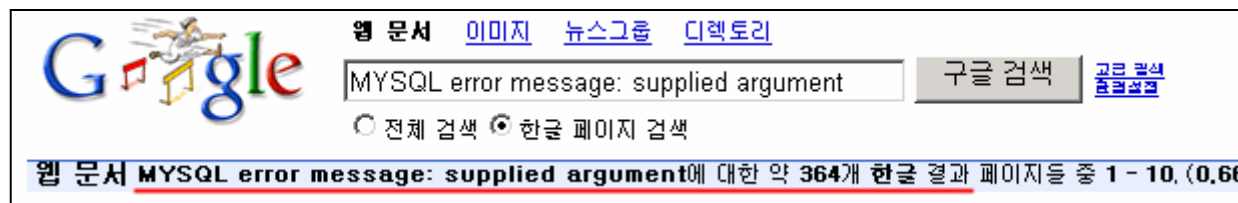
❖ SQL Injection 검색



`intitle:"에러" "에러 발생" filetype:asp`



`intitle:"Error" "에러 발생" filetype:asp`

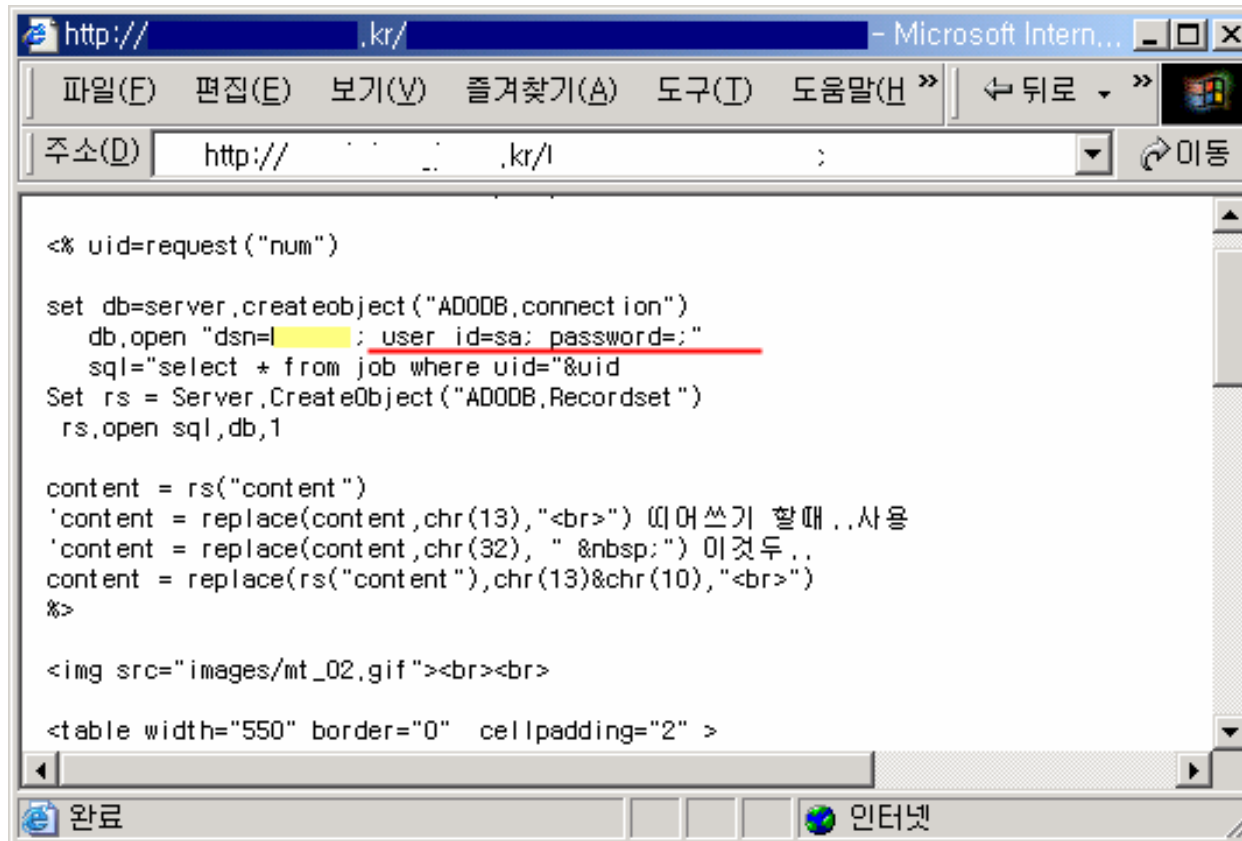


`Mysql error message: "supplied argument"`

SQL 데이터 수집

❖ SQL Injection 검색

이미 MS-SQL Injection 공격으로 침해 당한 파일 검색



The screenshot shows a Microsoft Internet Explorer browser window. The address bar contains a URL with a SQL injection payload: `http://.../kr/...?uid=request("num")&...&sql='select * from job where uid="'&uid`. The payload is highlighted in red. The main content area displays the rendered HTML output of the injection, including a table with a width of 550 and a border of 0.

```
<% uid=request("num")

set db=server.createObject("ADODB.connection")
  db.open "dsn=...; user id=sa; password=:"
  sql="select * from job where uid="'&uid
Set rs = Server.CreateObject("ADODB.Recordset")
rs.open sql,db,1

content = rs("content")
'content = replace(content,chr(13),"<br>") 띄어쓰기 할때 ..사용
'content = replace(content,chr(32), " &nbsp;") 이것두 ..
content = replace(rs("content"),chr(13)&chr(10),"<br>")
%>

<br><br>

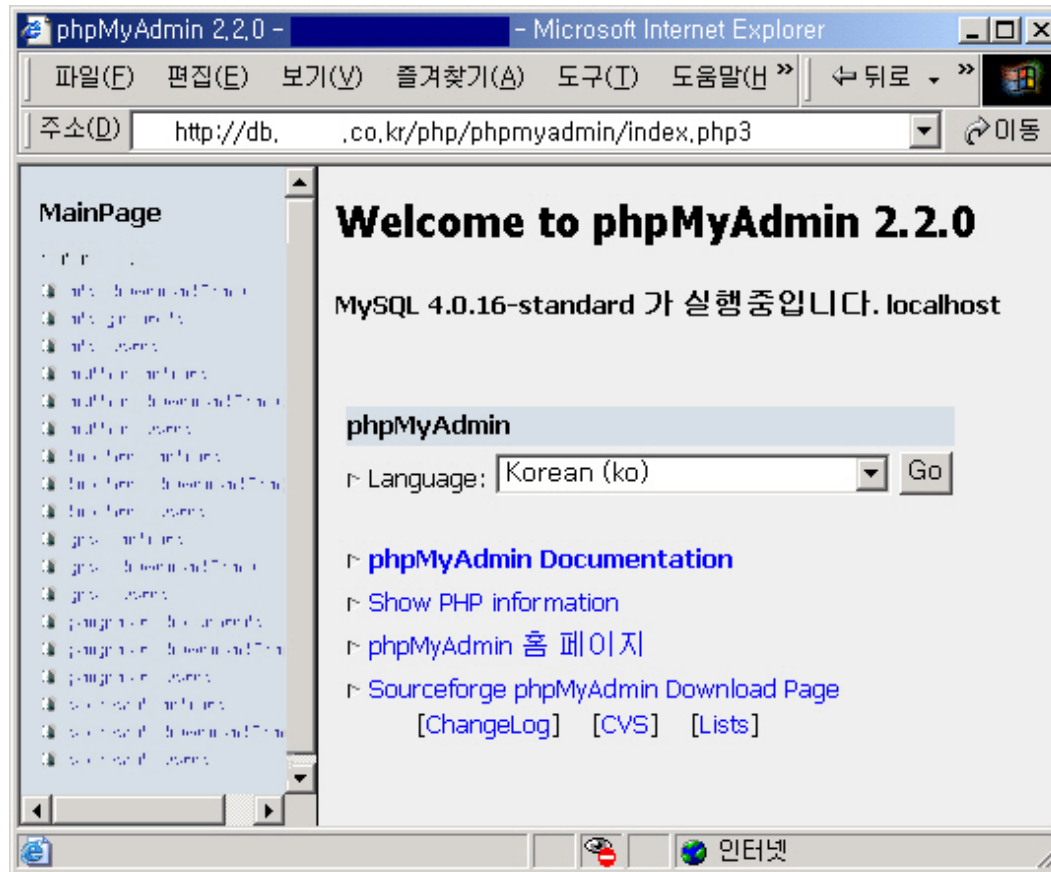
<table width="550" border="0" cellpadding="2" >
```

MS-SQL DB ID/PW 검색

!Hint: intext:(" |||") -inurl:

SQL 데이터 수집

- ❖ SQL 웹 관리 콘솔 검색
phpMyAdmin(MySQL WEB Management)검색



inurl:main.php3 Welcome to phpMyAdmin site:co.kr

SQL 데이터 수집

- ❖ SQL ID/PW 검색
DB 접속용 ID/PW 검색



filetype:inc dbconn



"IDENTIFIED BY"



filetype:sql +"IDENTIFIED BY" -cvs or filetype:dmp +"IDENTIFIED BY" -cvs

SQL 데이터 수집

❖ 그 외 SQL ID/PW 검색

```
filetype:"(sql | dmp | dump | inc)" password
```

```
filetype:mdb inurl:users.mdb
```

```
spwd.db / passwd
```

```
"Warning: pg_connect(): Unable to connect to PostgreSQL server: FATAL"
```

```
filetype:ldb admin
```

```
inurl:db intext:password filetype:sql
```

```
filetype:"(sql | dmp | dump | inc)" password
```

```
inurl:config.php dbname dbpass
```

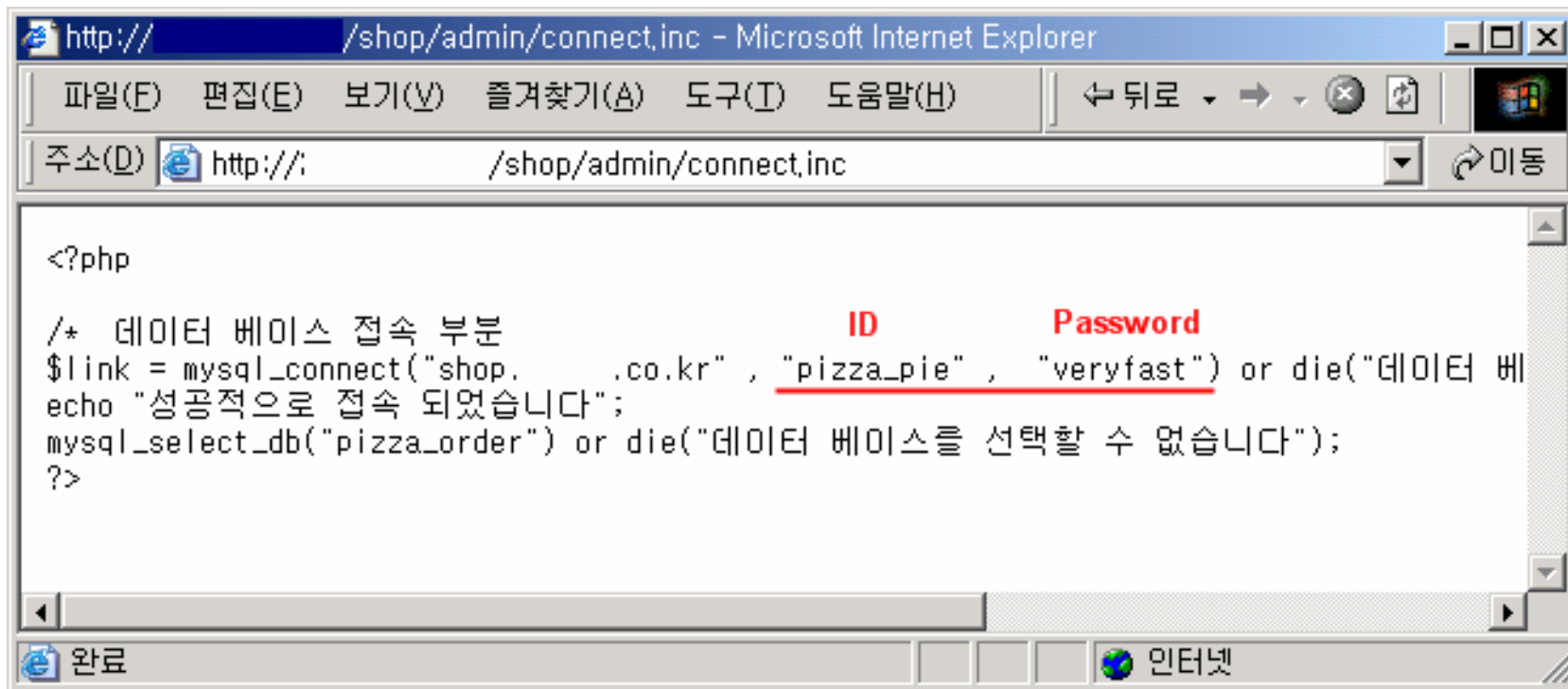
```
inurl:nuke filetype:sql -cvs
```



More and More

SQL 데이터 수집

- ❖ SQL ID/PW 검색
DB 접속용 ID/PW 검색

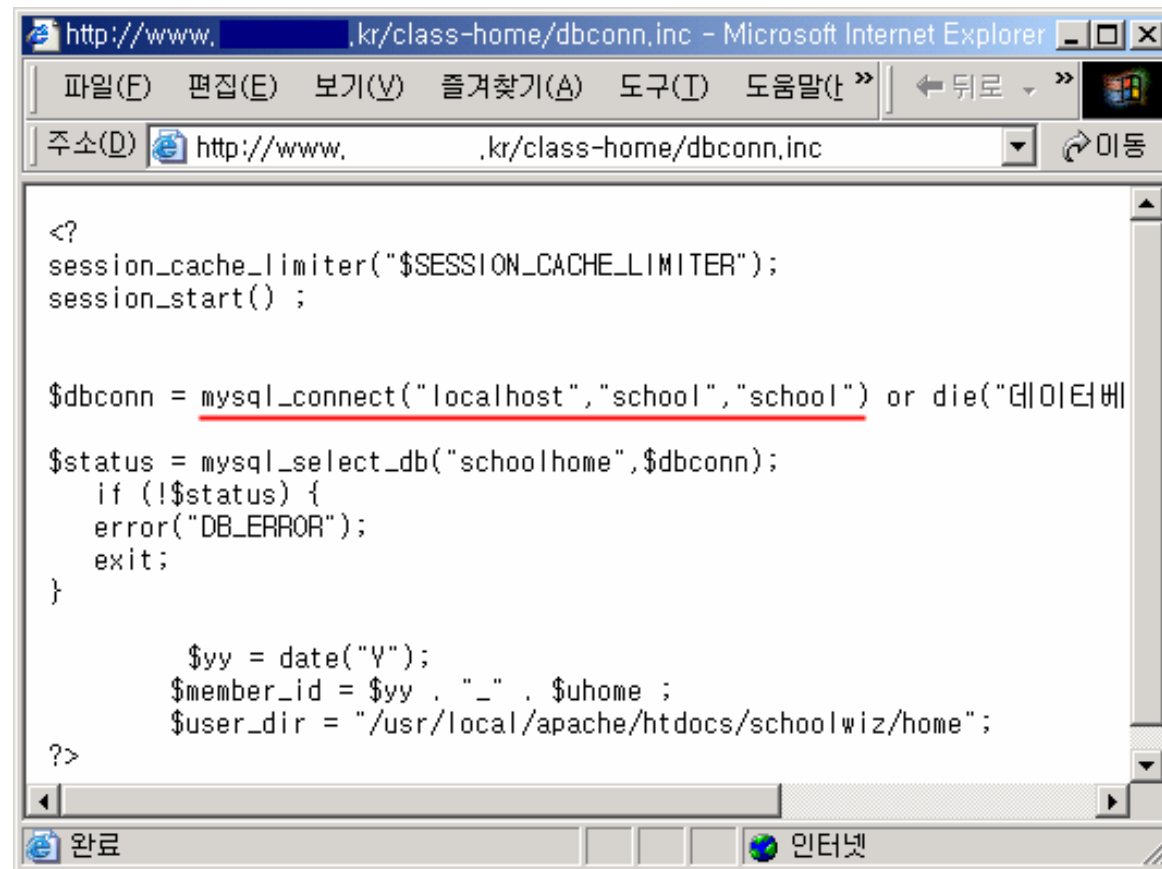


```
<?php
/* 데이터 베이스 접속 부분
$link = mysql_connect("shop. .co.kr" , "pizza_pie" , "veryfast") or die("데이터 베
echo "성공적으로 접속 되었습니다";
mysql_select_db("pizza_order") or die("데이터 베이스를 선택할 수 없습니다");
?>
```

filetype:inc intext:mysql_connect

SQL 데이터 수집

❖ SQL 패스워드 검색



The screenshot shows a Microsoft Internet Explorer browser window displaying a PHP script. The address bar shows the URL `http://www. .kr/class-home/dbconn.inc`. The script content is as follows:

```
<?
session_cache_limiter("$SESSION_CACHE_LIMITER");
session_start();

$dbconn = mysql_connect("localhost","school","school") or die("데이터베

$status = mysql_select_db("schoolhome", $dbconn);
if (!$status) {
    error("DB_ERROR");
    exit;
}

    $yy = date("Y");
    $member_id = $yy . "_" . $uhome ;
    $user_dir = "/usr/local/apache/htdocs/schoolwiz/home";

?>
```

filetype:inc dbconn site:kr

Attack Scenarios

MS-SQL DB ID/PW 검색을 통한

Windows 2000 Server(SP4)+MS-SQL 2000(SP3)

서버 관리자 권한 획득 시나리오

Attack Scenarios

SQL Injection 취약점 검색을 통한

MS-SQL 2000(SP3) 데이터 베이스 export 시나리오

인증서

■ 인증서(Certificates)

신뢰된 개인/사이트/공인 인증서 검색 후 신원 우회 공격에 이용



BEGIN(CERTIFICATE|RSA|DEA) filetype:key, or filetype:cer or filetype:der

인증서

❖ 개인 키 검색



filetype:pem PRIVATE -cvs

취약점 스캐너

■ Nessus Scan

Nessus 스캐닝 결과 보고서 검색



“This file was generated by Nessus” -site:ihackstuff.com

취약점 스캐너

❖ Nessus 스캐닝 결과 보고서

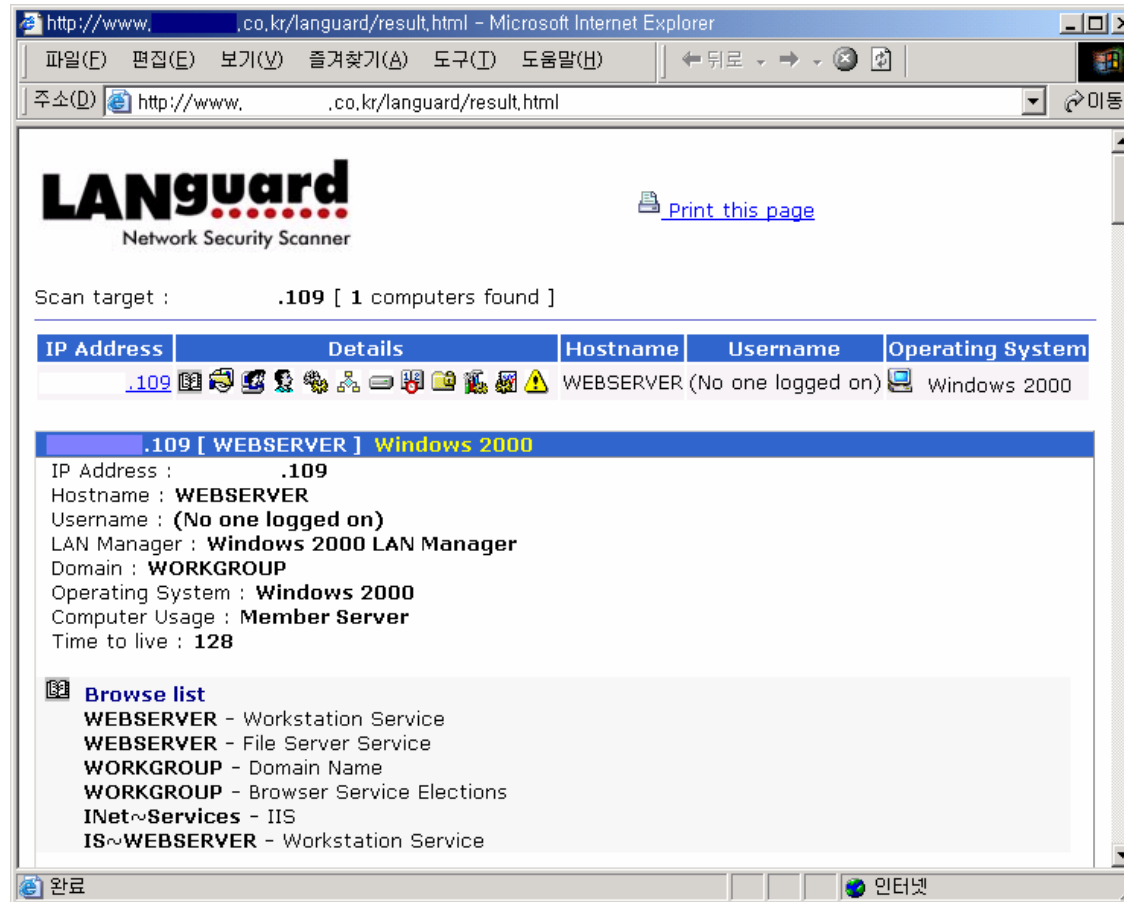
Analysis of Host	
Port/Service	Issue regarding Port
discard (9/tcp)	No Information
daytime (13/tcp)	Security warning(s) found
ftp (21/tcp)	Security warning(s) found
telnet (23/tcp)	Security warning(s) found
smtp (25/tcp)	Security notes found
time (37/tcp)	Security notes found
finger (79/tcp)	Security warning(s) found
www (80/tcp)	Security hole found
pop3 (110/tcp)	Security notes found
sunrpc (111/tcp)	Security notes found
general/tcp	Security hole found
general/icmp	Security warning(s) found
general/udp	Security notes found
ntp (123/udp)	Security warning(s) found
sunrpc (111/udp)	Security notes found

Vulnerability	www (80/tcp)	<p>A version of php which is older than 4.0.4 is running on this host.</p> <p>There is a buffer overflow condition in the IMAP module of this version which may allow an attacker to execute arbitrary commands with the uid of the web server, if this server is serving a webmail interface.</p> <p>Solution : Upgrade to PHP 4.0.4</p> <p>Reference : http://online.securityfocus.com/archive/1/166602</p> <p>Risk factor : High</p>
Vulnerability	www (80/tcp)	<p>The remote host appears to be vulnerable to the Apache Web Server Chunk Handling vulnerability.</p> <p>If Safe Checks are enabled, this may be a false positive since it is based on the version of Apache. Although unpatched Apache versions 1.2.2 and above, 1.3 through 1.3.24 and 2.0 through 2.0.36, the remote server may be running a patched version of Apache</p> <p>*** Note : as safe checks are enabled, Nessus solely relied on the banner to issue this alert</p> <p>Solution : Upgrade to version 1.3.26 or 2.0.39 or newer See also : http://httpd.apache.org/info/security_bulletin_20020617.txt http://httpd.apache.org/info/security_bulletin_20020620.txt</p> <p>Risk factor : High CVE : CAN-2002-0392</p>
Vulnerability	www (80/tcp)	<p>The remote host is running a version of PHP earlier than 4.1.2.</p> <p>There are several flaws in how PHP handles multipart/form-data POST requests, any one of which can allow an attacker to gain remote access to the system.</p> <p>Solution : Upgrade to PHP 4.1.2</p> <p>Risk factor : High CVE : CVE-2002-0081</p>

“This file was generated by Nessus” -site:ihackstuff.com

취약점 스캐너

❖ GFI LANguard 스캐닝 결과 보고서



“Generated by LANguard Network Security Scanner” site:co.kr

취약점 스캐너

❖ 국내 취약점 스캐너 결과 보고서

상세설명 & 해결책 - Microsoft Internet Explorer

주소(D) http://www. .or.kr/html/ssr.html

(취약점 탐지) - 요약 리포트

▶ 보고서 작성일자 : 2004년 06월 일

레포트 조건

- 레포트 시작일자 : 2004-
- 레포트 완료일자 : 2004-06-

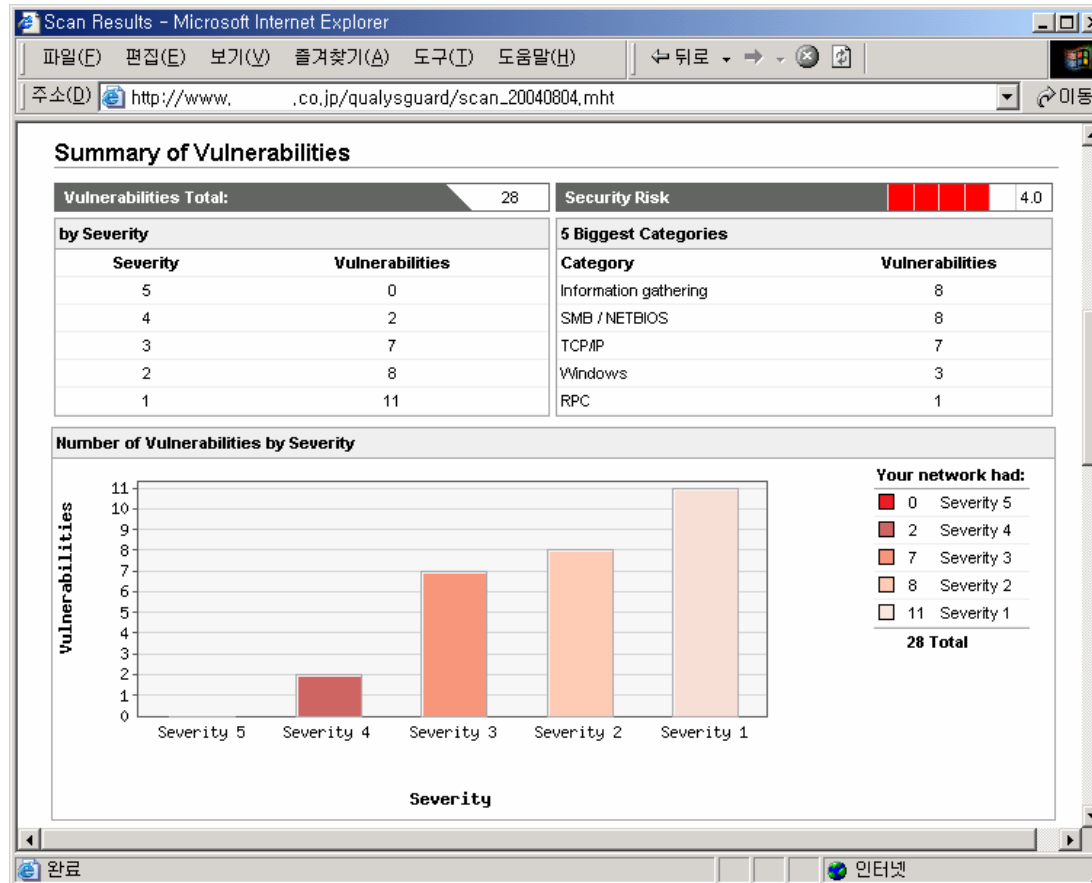
호스트 이름	호스트 IP	위험도			
		HIGH	MEDIUM	LOW	INFO
.2	.2	0	0	1	0
.4	.4	0	0	2	0
.5	.5	0	3	3	0
.12	.12	0	0	2	0
.23	.23	0	0	1	0
.24	.24	0	0	1	0
TOTAL	6	0	3	10	0

완료 인터넷

!Hint: intext: , -sample, -site:kr

취약점 스캐너

❖ QualysGuard 스캐너 결과 보고서



intext:"QualysGuard" -site:qualys.com

취약점 스캐너

❖ X-Scan 스캐너 결과 보고서

This report gives details on hosts that were tested and issues that were found.

Scan Result	
Hosts which were alive and responding during test	3
Number of security holes found	2
Number of security warnings found	3
Number of security notes found	34

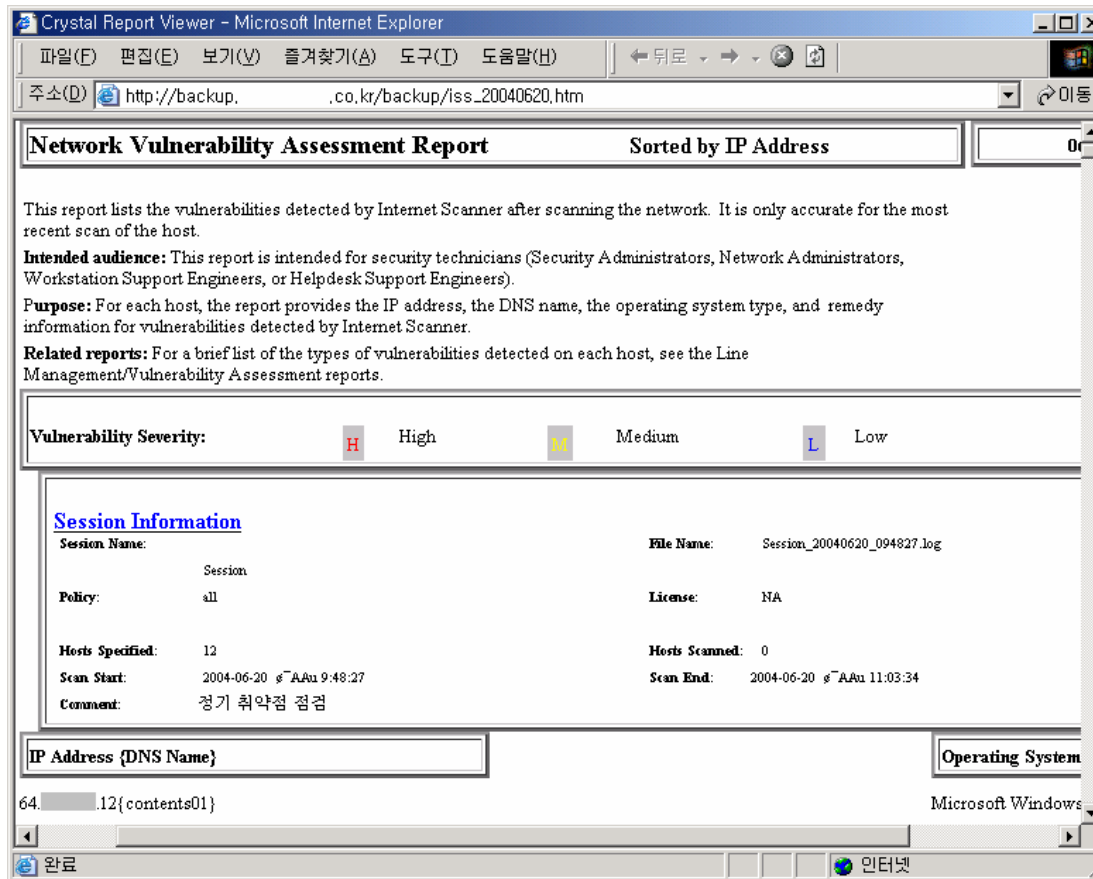
Host List	
Host(s)	Possible Issue
211. .	Security holes found
Host Summary - OS: Linux recent 2.4 (2) or OpenBSD 3.0-STABLE (X86); PORT/TCP: 21, 22, 25, 53, 80, 110, 443, 3306	
211. .	Security notes found
Host Summary - OS: F5 BigIP LB 4.1.x (sometimes FreeBSD) or OpenBSD 3.0-STABLE (X86); PORT/TCP: 13, 22, 25, 80, 110, 443, 3306	
211. .	Security notes found
Host Summary - OS: Windows 2000 (1) or Asante FriendlyNet FR3004 Series Internet Hub; PORT/TCP: 21, 25, 53, 80, 3389	

[\[return to top\]](#)

Intitle:"X-Scan Report" intext:"This file was generated by X-Scan"

취약점 스캐너

❖ ISS 스캐너 결과 보고서



"Network Vulnerability Assessment Report"

침입탐지 데이터

■ 침입탐지 데이터

침입탐지 시스템(Snort, ISA등) 로그 데이터 검색

The image shows two overlapping browser windows. The left window displays a Google search result for 'ACID "by Roman Danyliw" filetype:php', showing approximately 923 results. The right window shows the ACID web interface with a search query: 'Signature "[bugtraq][snort] WEB-PHP Title.php access"'. Below the search criteria, a table displays 17 alerts.

Queried DB on: Thu August 26, 2004 17:16:04

Meta Criteria: Signature "[bugtraq][snort] WEB-PHP Title.php access" ...clear...

IP Criteria: any

Layer 4 Criteria: none

Payload Criteria: any

Displaying alerts 1-17 of 17 total

< Src IP address >	FQDN	Sensor #	Total #	Unique Alerts	Dest. Addr.
175.38	5-38.dynamic.tfn.net.tw	1	2	1	1
153.39	adsl-tao.STATIC.so-net.net.tw	1	9	1	1
56.182	5-182.dynamic.hinet.net	1	3	1	1
99.155	9-155.dynamic.hinet.net	1	1	1	1
5.76.1	nsees.tyc.edu.tw	1	14	1	1
8.16.4	gate4.tp1rc.edu.tw	1	1	1	1
164.22	2.adsl.dynamic.seed.net.tw	1	3	1	1
167.22	2.adsl.dynamic.seed.net.tw	1	2	1	1
5.98.72	le to resolve address	1	1	1	1
45.167	7.adsl.dynamic.seed.net.tw	1	1	1	1
8.89.61	89-61.dynamic.hinet.net	1	3	1	1
10.184	84.adsl.dynamic.apol.com.tw	1	2	1	1
23.219	19.adsl.dynamic.apol.com.tw	1	7	1	1
58.196	8-196.dynamic.hinet.net	1	7	1	1
8.69.4	69-4.dynamic.hinet.net	1	5	1	1

ACID "by Roman Danyliw" filetype:php

SSH Key

■ SSH Key

Secure Shell 호스트 Key, Private key 검색

```
REGEDIT4

[HKEY_CURRENT_USER\SOFTWARE\SimonTatham\PuTTY\SshHostKeys]
"rsa2@22: [redacted]"="0x23,0xbd7b0d2aa91ed2b4ad55e210313e4045fdee1234d7551b3134d55b894d62c68eb51522f4b3765b6b4f8403c759c6d705db8f58e4a4c7f4644da17229d9232888b5d34ef107a6e1fe5145dace1d2083a4d94b2be3c2e9252bd5c66bdd0e0ca85ac9c4ed7bf15f0179d58cb9224a3f38f8f511ff270c2fbf73a2d0cbc8f91d19eb"
"rsa2@22: [redacted]"="0x23,0xf4e19bc87aaecb53569be9b11f4edb53c13dd7f3678edcb16f6f0048da16b07802ef7375ec9330d130564b8bf1e9b1a603dc072817820d41f35769ea4126a94bf57f3fe028262d54fe6b8b6435f2851a2a82128d104fb4d9d257b128a4853439c4d76dd576bb948bc5178f07e40439b06b9ccfc1347035dee0c05573624902b"

[HKEY_CURRENT_USER\SOFTWARE\SimonTatham\PuTTY\Sessions#1]
"Present"=dword:00000001
"HostName"="[redacted]"
"LogFileName"="putty.log"
"LogType"=dword:00000000
"LogFileClash"=dword:ffffffff
"Protocol"="ssh"
"PortNumber"=dword:00000016
"CloseOnExit"=dword:00000001
"WarnOnClose"=dword:00000001
"PingInterval"=dword:00000000
"PingIntervalSecs"=dword:00000000
"TCPNoDelay"=dword:00000001
"TerminalType"="xterm"
```

filetype:reg ssh and
filetype:key private.key

```
"BugPlainPW1"=dword:00000000
"BugRSA1"=dword:00000000
"BugHMAC2"=dword:00000000
"BugDeriveKey2"=dword:00000000
"BugRSAPad2"=dword:00000000
"BugDHGEx2"=dword:00000000

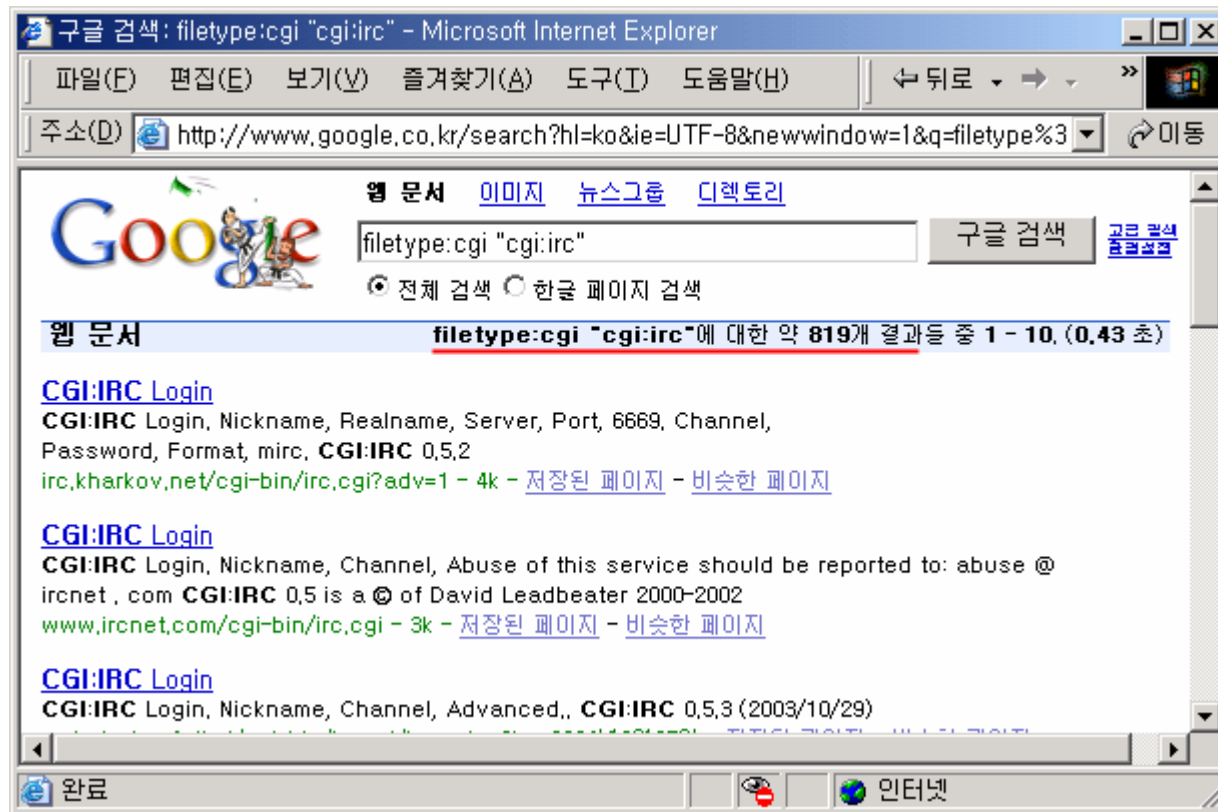
[HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\SshHostKeys]
"rsa2@22: [redacted]"="0x23,0xc8d1cc8051cdf2233d694f50b43b06c
"rsa2@22: [redacted]"="0x23,0xcb9ebf2e4133e96dae0a07917db71
"rsa2@22: [redacted]"="0x23,0xcef3d3ff76dcc75184a217c48745ee
"rsa2@22: [redacted]"="0x23,0xf623769051b70fd053110d8c38efbce
"rsa2@22: [redacted]"="0x23,0xf623769051b70fd053110d8c38efbce6fde3a7d271e7d7
"rsa2@22: [redacted]"="0x23,0xf623769051b70fd053110d8c38efbce6fde3a7d271e7d7"
```

filetype:reg reg HKEY_CURRENT_USER SSHHOSTKEYS

IRC

■ IRC

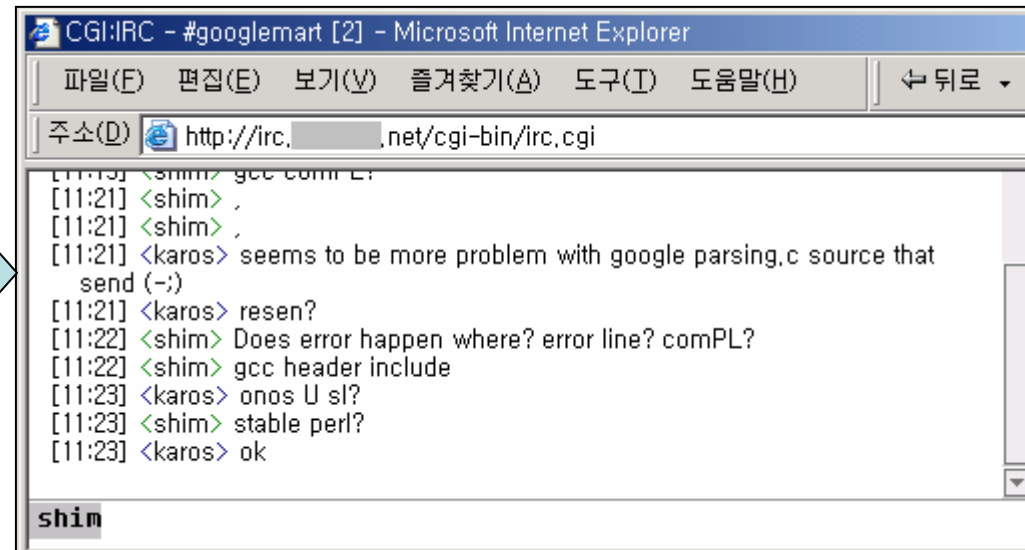
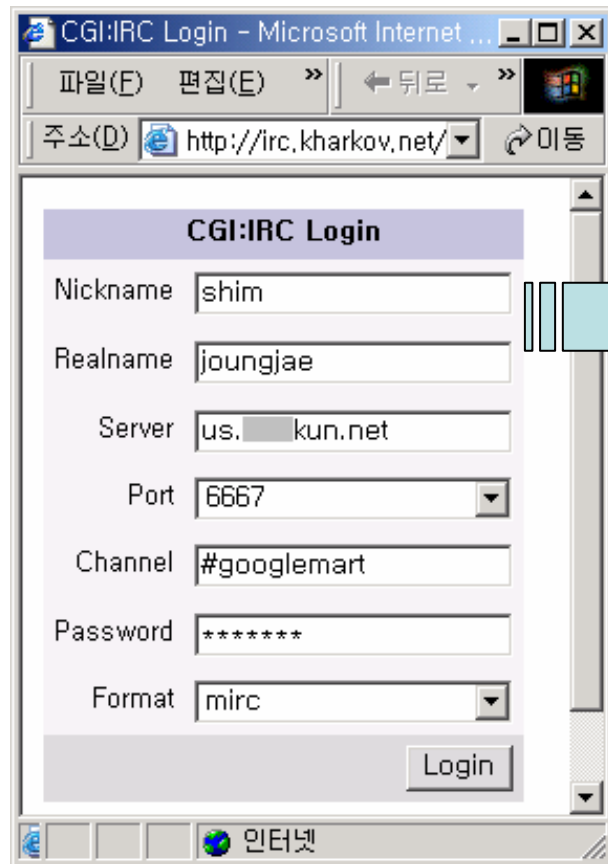
웹 인터넷 릴레이 채팅 접속 클라이언트 검색



filetype:cgi "cgi:irc"

IRC

- ❖ 사이트 중에 일부는 IRC 서버를 임의로 변경 가능(Proxy)

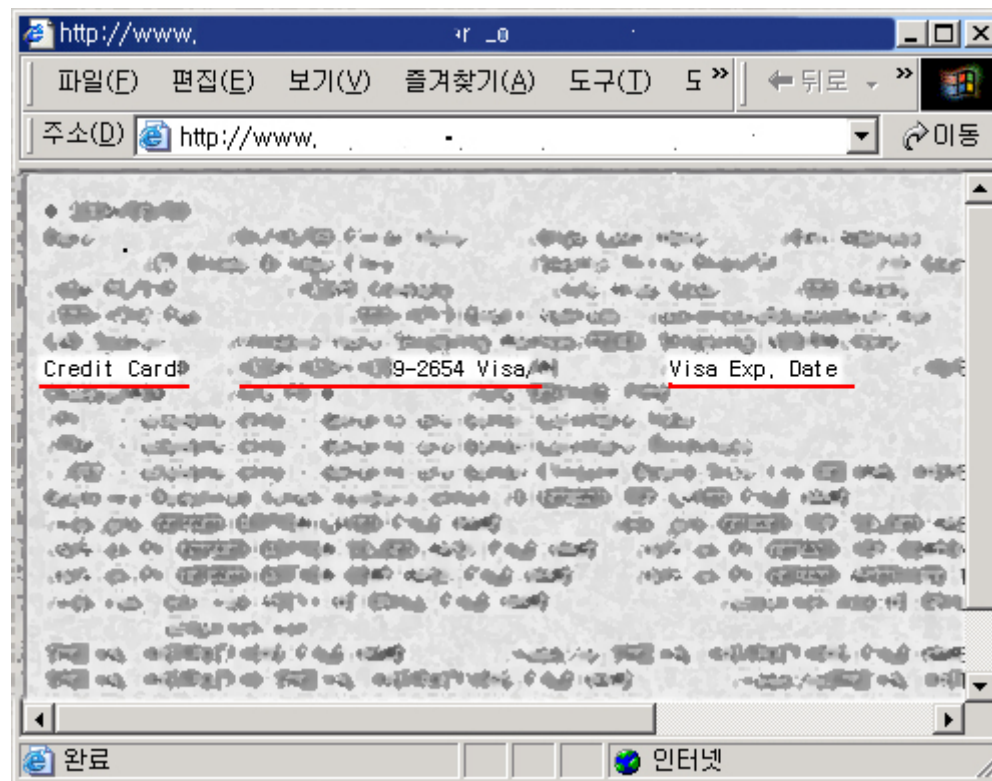


filetype:cgi "cgi:irc"

Credit Card

■ Credit Card

신용카드 종류, 번호, 만료기간 등의 정보를 담고 있는 파일 검색
최근 미국에서는 인터넷 신용카드 범죄에 상당수가 웹에서 pillaging

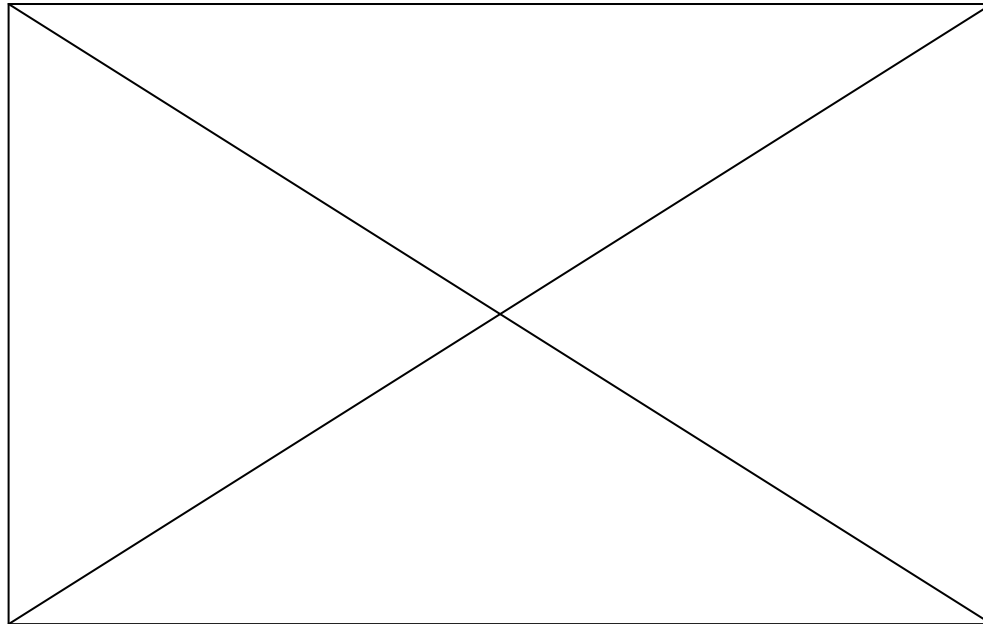


!hint: cache:, intext:, -inurl:form, -intext:

개인 정보

■ 개인 정보

구글을 통해 개인의 정보(사회보장 번호, 주민등록번호, 주소, 이름, ID, 비밀번호 등등) 검색

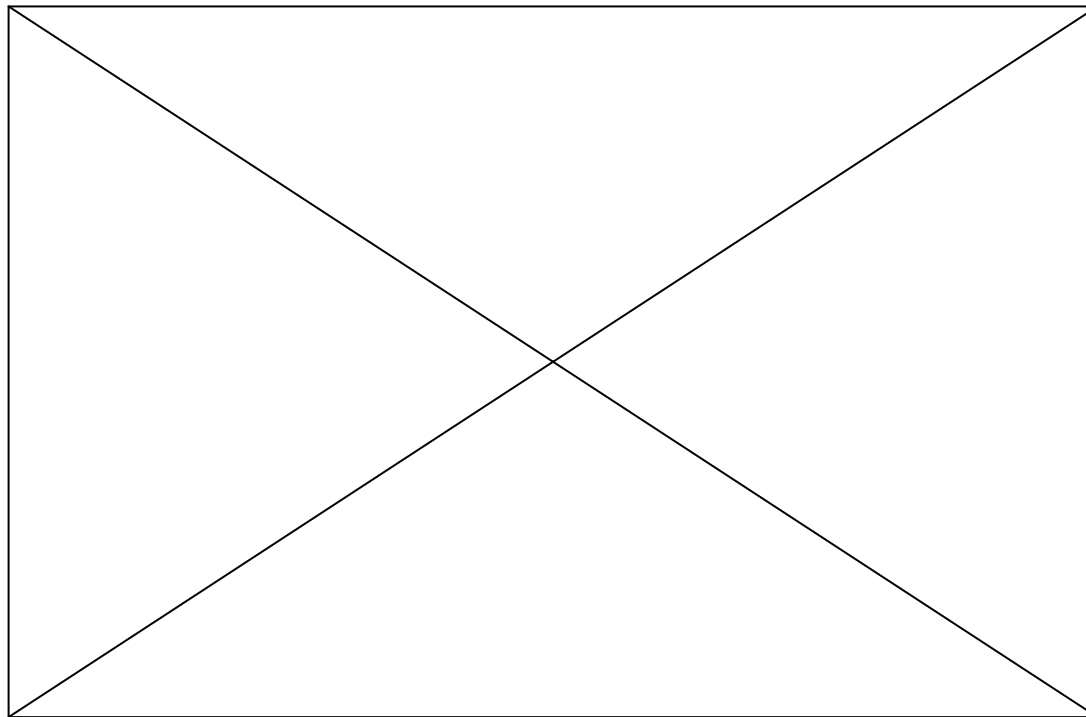


개인 정보 DB 검색
!hint: cache:, intext:, filetype:

개인 정보

■ 개인 정보

포탈 사이트 ID/PW 검색

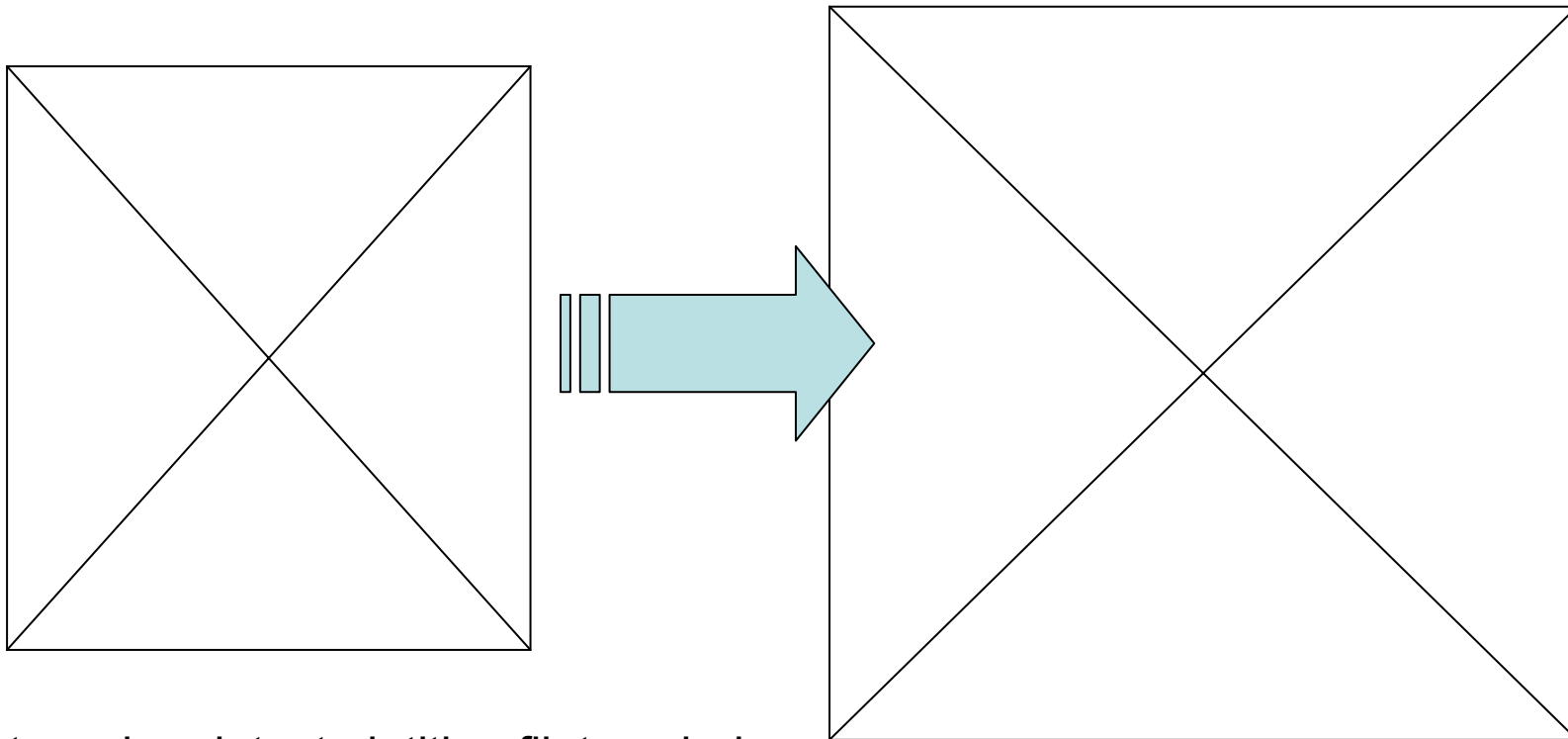


Social engineering gathering
!hint: cache:, intext:, intitle:

개인 정보

■ 개인 정보

인터넷을 통한 대다수 개인 정보는 회원 가입시 입력한 DB 및 게시판 등을 통해 검색



`!hint: cache:, intext:, intitle: filetype:bak`

Attack Scenarios

개인정보 검색에 따른
국내 TOP10 포탈 사이트 로그인 시나리오

방어(Prevention)

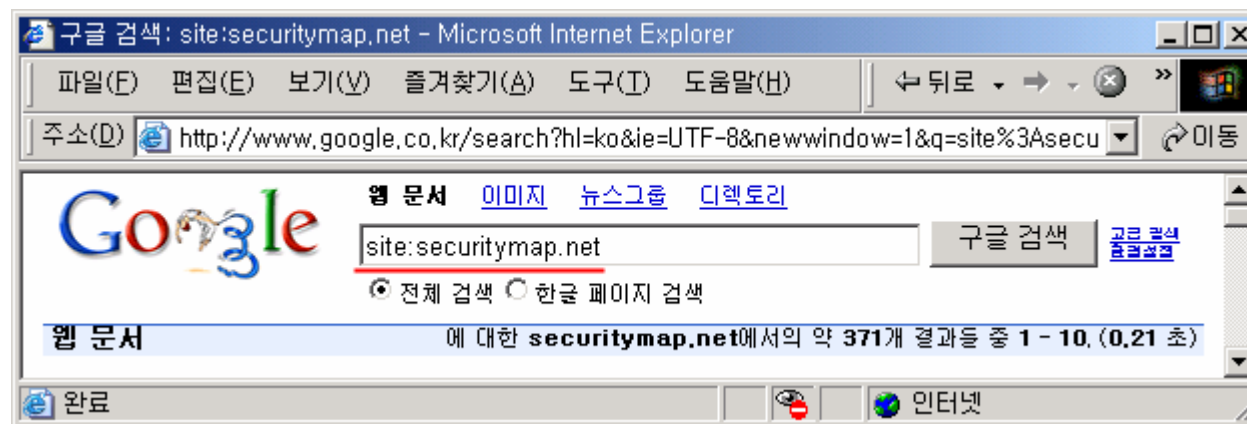
■ Googledork Prevention

- ✓ 웹 서버 중요 데이터 저장 금지
- ✓ 웹 서버 임시 파일 저장 금지
- ✓ 웹 서버와 DB서버 분리
- ✓ 잘 알려진 googledork 검색어를 통해 주기적인 보안
- ✓ 신규 googledork 검색어 모니터링(<http://johnny.ihackstuff.com/>)
- ✓ 한글 googledork 검색어 모니터링(<http://www.insecure.co.kr/>)
- ✓ 검색 결과 삭제 요청: <http://www.google.com/remove.html>
- ✓ 개인 - 회원 가입 시 최소한의 정보만을 기입
- ✓ 관리자 - 웹 로그 참조 링크 정보 모니터링

방어(Prevention)

■ Googledork Prevention

- ✓ “site:” 구글 옵션을 사용하여 자신의 웹 사이트 검색
- ✓ “link:” 구글 옵션을 사용하여 중요 정보가 타 사이트에 링크되어 있는지 점검
- ✓ IP 주소나 도메인 명을 입력하여 모든 구글 검색 결과 모니터링
- ✓ FQDN 보다는 DN 검색
(X) site:www.securitymap.net
(O) site:securitymap.net

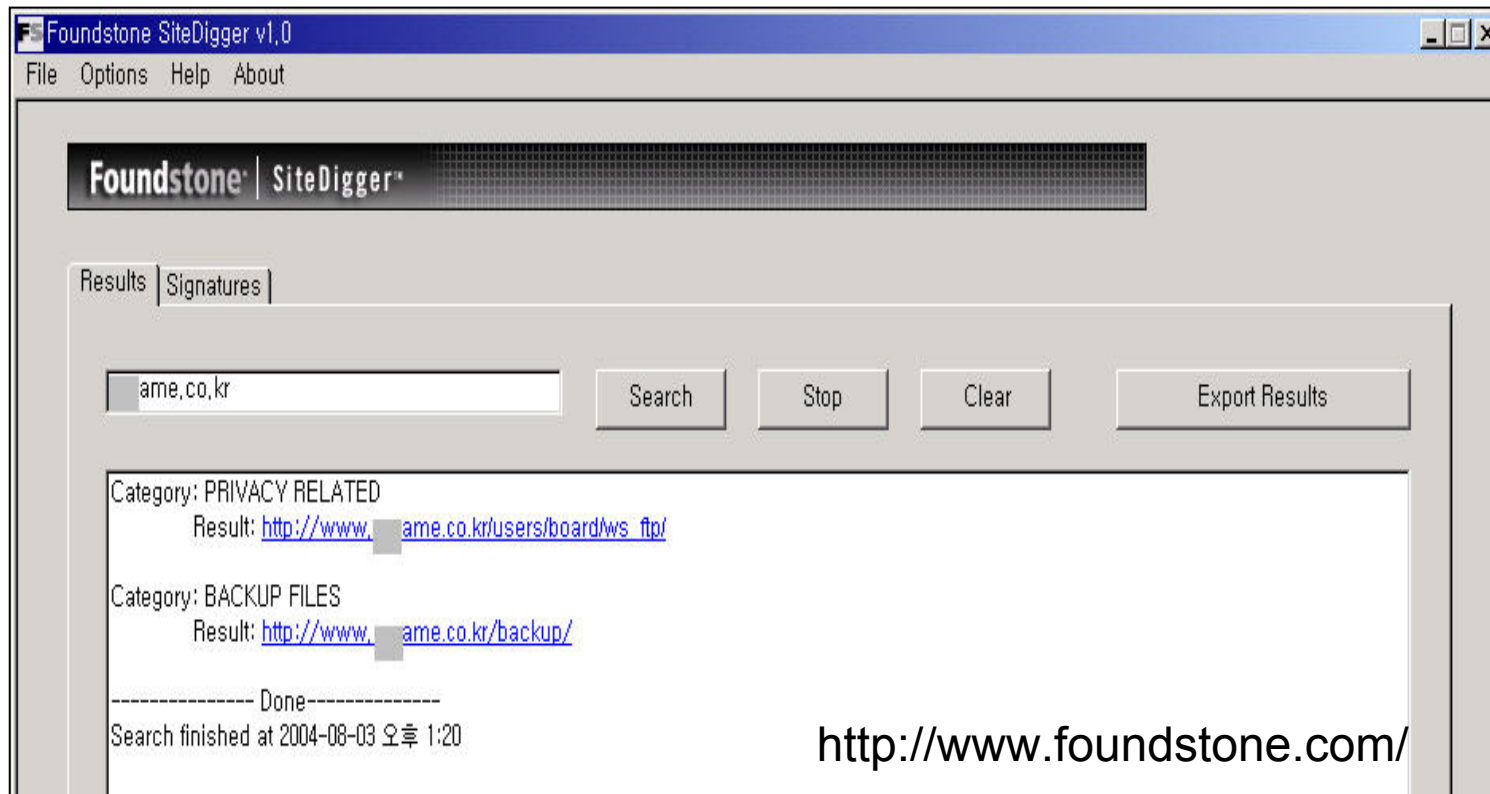


구글 검색 결과 보호 되어야 할 정보가 있는지 확인

방어(Prevention)

■ Googledork Prevention

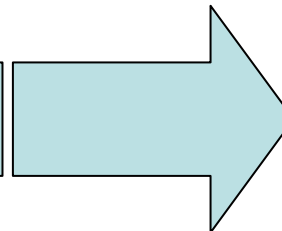
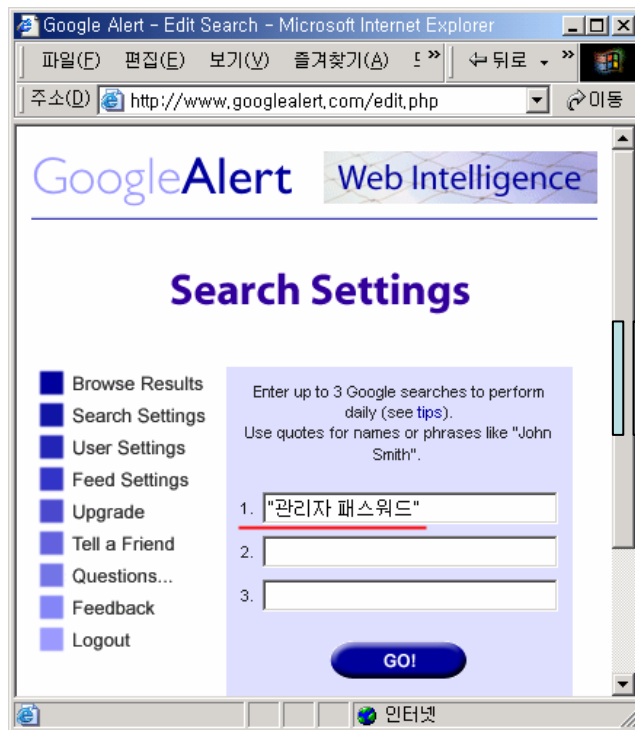
자동 검색 툴을 이용한 방어(FoundStone, Inc. SiteDigger)



방어(Prevention)

■ Googledork Prevention

자동 검색 툴을 이용한 방어(GoogleAlert, Inc. <http://www.googlealert.com/>)



43 results from **August 27th, 2004** for search 2: "관리자 패스워드"

ZNet Korea... 잃어버린 패스워드 찾는 「필수 ... (Google rank 1)
... 필자는 IT 담당 직원이 회사를 그만두었는데 후임 직원이 관리자 패스워드를 모른다며 패스워드를 알아내 달라는 ...
<http://www.zdnet.co.kr/techupdate/lecture/network/0,39024995,10067728,00...> - cached

관리자 패스워드 입력 (Google rank 2)
관리자 패스워드를 입력해 주세요. [BACK]. BBS NOTE 7.0a22 세니시 BASIC2 Client Program (C)(shi-cyan) Client Program ...
<http://www.hikin.com/bbsnote/bbsnote.cgi?fc=admin> - cached

자주 묻는 질문의 답변 (Google rank 4)
Blmail 에서 관리자 패스워드 변경법을 알려주세요. 관리자 URL로 접속한 후, [기타]-[관리자정보]-[패스워드 ...
http://www.blueweb.co.kr/faq/faq_answer.html?faqid=53&searchkey=&page=1... - cached

관리자 패스워드 화면 (Google rank 6)
수원지사 user ID, password.
<http://www.bandonet.co.kr/bandojob/branchshop/suwon/password7.asp> - cached

관리자 패스워드 화면 (Google rank 7)
성남지사 user ID, password.
<http://www.bandonet.co.kr/bandojob/branchshop/sungnam/password8.asp> - cached

성숙한 네티즌이 만들어 가는 Secure Korea Network!! (Google rank 8)
... 오른쪽 버튼을 눌러서 "패스워드 설정" @ 메뉴를 클릭 합니다. <관리자 패스워드 변경>, ... <관리자 패스워드의 재확인>, ...
http://www.dreamline.co.kr/save_infor/sub2.html - cached

웹호스팅 XY.NET - Upload Your Dream. That comes true! (Google rank 9)
... 게시판 관리자 패스워드는 기본적으로 'board'로 되어 있습니다. 게시판 관리자 패스워드가 있는 파일 경로입니다. ...
http://x-y.net/manual CGI_xy.php - cached

방어(Prevention)

■ Googledork Prevention

자동 검색 툴을 이용한 방어(gooscan <http://johnny.ihackstuff.com/>)

```
[root@          gooscan-v0.9]# ./gooscan
gooscan <-q query | -i query_file> <-t target>
        [-o output_file] [-p proxy:port] [-v] [-d]
        [-s site] [-x xtra_appliance_fields]

-----
(query)      is a standard google query (EX: "intitle:index.of")
(query_file) is a list of google queries (see README)
(target)     is the Google appliance/server
(output_file) is where the HTML-formatted list of results goes
(proxy:port) address:port of a valid HTTP proxy for bouncing
(site)       restricts search to one domain, like microsoft.com
(xtra_appliance_fields) are required for appliance scans
-v turns on verbose mode
-d hex-encodes all non-alpha characters
Friendly example:
gooscan -t google.fda.gov -q food
        -x "&client=FDA&site=FDA&output=xml_no_dtd&oe=&lr=&proxystylesheet=FDA"
Google terms-of-service violations:
gooscan -t www.google.com -q "linux"
gooscan -t www.google.com -q "linux" -s microsoft.com
gooscan -t www.google.com -f gdork.gs

Gooscan google scanner by jOhnny http://johnny.ihackstuff.com
[root@          gooscan-v0.9]#
```

-f 옵션을 사용하려면 gooscan.c 파일 수정

Conclusion

- 구글은 취약 서버를 찾는 가장 좋은 **Stealth** 스캐너
- 검색엔진과 결합된 악성 프로그램(바이러스, 웜)이 점차 확대
- 개인 정보를 손쉽게 획득 할 수 있는 수단
- 보안상 위험한 검색결과를 보여준다면 협력적인 빠른 대응 필요.
- 다양한 침입탐지 시스템 혹은 웹 모니터링 프로그램 회피 가능 검색
(Ex: 비밀번호는 → 비밀번호는)

참고 사이트

- SECURITY FORUMS

<http://www.security-forums/>

- johnny ihackstuff

<http://johnny.ihackstuff.com/>

- Defcon

<http://www.defcon.org/>

- Google Alert

<http://www.googlealert.com/>

- Google Hacks (O'REILLY book)

<http://www.oreilly.com/catalog/googlehks/>

Q & A

Thanks



<http://johnny.ihackstuff.com>

"I'm Johnny. I hack stuff."

