@ GHDB(Google Hacking Database)

- 구글 검색 엔진을 이용하여 정보를 수집하는 방법
- exploit-db 사이트에서도 제공함(https://www.exploit-db.com/google-hacking-database)

Ex1) 관리자 페이지 검색

inurl:admin site:co.kr

Ex2) 소스 코드 노출 검색

intitle:index.of/home inurl:co.kr

Ex3) 특정 데이터/파일 검색 및 디렉토리 검색

intitle:"index of" intext:이력서
intitle:index.of intext:passwd.txt
index.of "Parent Directory"

Ex4) 특정 파일 형식 검색

site:com filetype:pdf ccna dump

Ex5) 웹-서버 검색

intitle:test.page "Hey, it worked !" "SSL/TLS-aware"
intitle:Test.Page.for.Apache it.worked! this.web.site!
intitle:"Test Page for Apache installation on Web Site!"
intitle:Test.Page.for.Apache seeing.this.instead
intitle:"아파치 설치를 위한 테스트페이지"
intitle:Apache 1.x documentation
intitle:"아파치 설치 검사용 페이지"
intitle:Apache HTTP Server 2.0 문서
intitle:Welcome.to.IIS.4.0
allintitle:Welcome to Windows NT 4.0 Option Pack
allintitle:Welcome to Internet Information Server

[참고] 검색 카테고리

Advisories and Vulnerabilities
취약점 서버 검색 및 보안 권고 게시물 검색

Error Messages
에러 메세지 검색

Files containing juicy info
아이디/패스워드가 없어도 해킹 가능한 파일 검색

Files containing passwords
암호화된 파일 검색

Files containing usernames
아이디에 대한 패스워드 설정이 없는 파일 검색

Footholds
웹-서버 및 기타 해킹을 하기 위한 초기 작업 검색

Pages containing login portals
로그인 페이지를 포함한 포털 사이트를 이용한 검색

Pages containing network or vulnerability data
네트워크 및 취약한 데이터를 포함한 페이지 검색

sensitive Directories
공유된 민감한 디렉토리 검색

sensitive Online Shopping Info
온라인 쇼핑시 사용하는 고객정보, 주문내역, 카드번호 등 민감한 정보 검색)

Various Online Devices
웹-페이지에서 프린트, 비디오 카메라와 같은 다양한 온라인 장치 검색

Vulnerable Files
대량의 웹-사이트 취약한 파일 검색

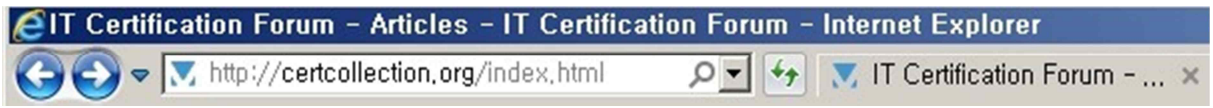
Vulnerable Servers

특정 취약점 서버 검색

Web Server Detection

취약점 웹-서버 검색

[참고] 구글 검색 명령어



- intitle -> IT Certification Forum - Articles - IT Certification Forum
- site -> certcollection.org
- inurl -> certcollection.org/index.html
- filetype -> html
- intext -> 페이지 안에 있는 문자열

[명령어 사용 예제]

명령어	예제	내용
intitle:	intitle:ccie	title 에 'ccie'가 포함된 파일을 검색한다.
inurl:	inurl:ccie	주소에 'ccie'가 포함된 파일을 검색한다.
intext:	intext:ccie	페이지 내용이 'ccie' 문자가 포함된 파일을 검색한다.
site:	site:http://ccie	http://ccie 사이트에서 파일을 검색한다.
filetype:	filetype:pdf	확장자가 'pdf'인 파일을 검색한다.
link:	link:http://ccie	http://ccie 링크가 걸린 파일을 검색한다.
inanchor:	inanchor:http://ccie	http://ccie 가 텍스트로 된 파일을 검색한다.
numrange:	numrange:1000-2000	1000-2000 숫자 범위 결과를 검색한다.
location:	location:korea	대한민국 범위 내에서 검색한다.

[참고] 명령어 사용 형식

http://www.googleguide.com/advanced_operators_reference.html#ext

[연산 명령어 사용 예제]

명령어	예제	내용
AND +	"A" & "B" "A" "B" "A" AND "B" "A+B"	"A"와 "B" 문자열이 모두 포함된 파일을 검색한다.
OR |	"A" OR "B" "A" | "B"	"A" 또는 "B" 문자열이 포함된 파일을 검색한다.
NOT -	"A" NOT "B" "A" -"B"	"A" 문자열은 포함하고, "B" 문자열을 제외한 파일을 검색한다.
" "	"A"	" " 사이에 있는 A 문자를 검색한다.
~	~A	동의어 또는 관련 검색어를 검색한다.
*	AB*	AB 문자열 다음에 올수 있는 모든 문자열을 검색한다.
.	A.	한 단어를 포함한 모든 단어를 검색한다.
..	2012..2016	2012 부터 2016 숫자를 검색한다.

Ex6) GHDB 실습

- 웹-서버의 소스 코드 검색

intitle:"index of" site:.co.kr
intitle:index of/home inurl:co.kr
intitle:index of/etc site:net
intitle:"index of" intext:passwd

- 웹-서버의 민감한 데이터/로그 검색

intitle:"index of" intext:(backup|백업|dump)
intitle:"index of" intext:(backup|bak) inurl:com.au
intitle:"index of" intext:백업 location:korea
site:naver.com filetype:hwp 검색
inurl:seoul filetype:hwp
intitle:"index of" "DCIM"

- 관리자 로그인 페이지 검색

inurl:/admin filetype:asp
inurl:admin + filetype:asp
intitle:관리자 로그인
intitle:관리자 inurl:/admin filetype:html site:co.kr

- Intranet 로그인 검색

intitle:intranet filetype:php site:co.kr
intitle:("인트라넷"|"intranet"|"직원용"|"사내") intext:로그인

- 원격 데스크톱 웹 연결 검색

intitle:"원격 데스크톱" inurl:co.kr

- 데이터베이스 로그인 검색

intext:mysql_connect filetype:bak
inurl:wp-config -intext:wp-config "'DB_PASSWORD'"

- 아이디/패스워드 포함 파일 검색

inurl:etc -intext:etc ext:passwd
intext:passwd.txt filetype:txt
ntext:shadow intitle:index.of
filetype:xls "username | password"
intext:charset_test= email= default_persistent=

- 패스워드가 포함된 파일 검색

filetype:log intext:password | pass | pw

- 전화 번호, 아이디, 패스워드 검색

inurl:"wvdial.conf" intext:"password"

- CAM 검색

inurl:/view/viewer_index.shtml

- FTP 검색

filetype:ini wcx_ftp
intitle:index.of ws_ftp.ini

- 게시판 관리 검색

intitle:technote inurl:cgi-bin

- 이-메일 및 패스워드 검색

intext:charset_test= email= default_persistent=

- Wordpress Passwords 검색

inurl:wp-config -intext:wp-config "'DB_PASSWORD'"

[참고] 검색 정보 삭제 요청

https://www.google.com/webmasters/tools/removals?hl=ko