Google Hacking

담당교수 : 신원
대상 : 정보보호학과 3/4학년
과목 : 해킹 및 악성코드 대응
학기 : 2020년 1학기

Definition

- Google hacking is a computer hacking technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites use
- Google hacking is a term that refers to the art of creating complex search engine queries in order to filter through large amounts of search results for information related to computer security
- In its malicious format, it can be used to detect websites that are vulnerable to numerous exploits and vulnerabilities as well as locate private, sensitive information about others, such as credit card numbers, social security numbers, and passwords
- Google Hacking involves using Google operators to locate specific strings of text within search results

Google Operators

- 구글은 다양한 검색 옵션을 제공
  - 사용자가 원하는 결과를 보다 정확하게 검색
- 기본 검색 옵션

옵션	예제	내용
intitle	intitle:Welcome	제목 중 "Welcome" 문자가 포함된 페이지 검색
inurl	inurl:admin	URL에 admin이 포함된 페이지 검색
site	site:abc.com	abc.com 사이트에서 검색
filetype	filetype:pdf	확장자가 pdf인 파일 검색
intext	intext:security	security 문자열이 포함된 페이지 검색
link	link:http://security	http://security 링크가 걸린 페이지 검색

- 기타 검색 옵션
  - allintitle:, allinurl:, daterange:, define:, phonebook:, related:, strings:

- 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
  - | / or : 또는
    - filetype:bak inurl:"htaccess|passwd|shadow|htusers"

- **구글 검색을 통해 알 수 있는 정보**
  - 시스템 및 어플리케이션의 잘못된 설정으로 인한 에러 메시지
  - 중요 파일의 세부 정보
  - 패스워드를 포함하는 파일
  - 사용자 정보를 포함하는 파일
  - 특정 권한을 획득하기 위한 참조 파일
  - 로그인 페이지
  - 네트워크 정보나 취약 데이터
  - 중요한 디렉터리 및 파일
  - 숨겨진 디렉터리
  - 백업 파일 및 임시 파일
  - 취약 서버 목록
  - 웹 서버 종류
  - 사회공학적 공격을 위한 각종 자료

- **디렉터리 목록화 (Directory Listing)**
  - 웹 서버의 소스 코드를 볼 수 있는 취약점
    - ex) intitle:index.of / home inurl:co.kr
    - ex) intitle:index.of "Parent Directory"
  - 웹 서버의 민감한 데이터 다운로드 가능, 웹 서버 버전 확인 가능
    - ex) intitle:"index of" intext:이력서
    - ex) intitle:index.of "server at"
- **서버 기본 페이지 (Server Default Page)**
  - 서버 기본 페이지가 존재하여 공격자들로부터 침입목표가 될 가능성 존재
    - ex) intitle:"아파치 설치를 위한 테스트페이지"
    - ex) intitle:test.page "Hey, it worked !" "SSL/TLS-aware"
    - ex) intitle:"Welcome to Windows 2000 Internet Services"

- **로그 파일**
  - 다양한 응용프로그램 로그파일을 검색 후 중요 정보 획득 (ID/PW, 시스템 정보, 서비스 정보, DB정보 등)
    - intitle:"index of" intext:(backup|백업|bak|dump)
  - 데이터 베이스 백업 로그 검색
    - !Hint: filetype:bak intext: , inurl:
- **로그인 페이지**
  - 웹 사이트 내에 감춰진 관리용 로그인 페이지를 검색하여 서버의 중요 정보를 획득하거나 서버 로컬 권한을 획득하는데 이용
    - inurl:/admin filetype:php (or asp, jsp)
    - intitle:"관리자로그인"
    - "VNC Desktop" inurl:5800 - VNC 원격 데스크톱 로그인
    - intitle: "Remote Desktop Web Connection" inurl:tsweb - 윈도우 터미널 원격 데스크톱 웹 로그인

- **내부 네트워크 접속 페이지**
  - 내부 네트워크 접속
    - intitle:"인트라넷"
    - intitle:"intranet"
    - intitle:"직원용"
    - intitle:"사내" index:로그인
- **관리자 로그인**
  - 소스보기 금지 우회 및 패스워드 노출 취약점
    - intitle:관리자 inurl:/admin filetype:html site:ac.kr
- **웹메일 서버 로그인**
  - 웹 메일 ID/PW 자동 로그인 취약점
    - intitle:"웹 메일 로그인" inurl:mail site:co.kr
    - intitle:"Web Mail Login" inurl:mail site:com

- **패스워드를 포함한 파일 검색**
  - DB, Application, Board, Server, FTP 등 손쉽게 서비스 및 서버 접근 권한 획득 가능
    - intext:mysql_connect+pass
    - intext:mysql_connect filetype:bak
    - intitle:index.of ws_ftp.ini
    - intitle:technote inurl:cgi-bin
- **중요 데이터**
  - 외부 공개가 금지된 중요한 데이터 검색
    - allintext:대외비 filetype:hwp
    - allintext:confidential filetype:pdf

- **포트 스캐닝**
  - 포트번호 이용하여 현재 사용중인 응용프로그램까지 유추 가능
    - "VNC Desktop" inurl:5800
    - inurl:":10000" intext:webmin
    - intitle:"Network query tool" filetype:php or inurl:nqt.php
    - intitle:"Nessus Scan Report" ext:html
    - "Generated by LANguard Network Security Scanner" site:kr
    - intitle:"report" ("qualys" | "acunetix" | "nessus" | "netsparker" | "nmap") filetype:pdf
- **해킹 파일 검색**
  - 이미 해킹당한 시스템에 남아 있는 해킹 관련 파일 검색
  - 업로드 실행 파일, 웜, 바이러스, 기타 해킹 파일 검색
    - intitle:"PHP Shell *" intext:Command filetype:php
    - "index of" /wp-content/uploads/shell.php
    - intext:文件 filetype:php inurl:up

- **에러 메시지 (Error Message)**
  - 에러 메시지의 검색 결과는 서버에 침입 경로 제공 가능
    - ex) "ORA-00921: unexpected end of SQL command" site:ac.kr
  - 서버 어플리케이션 설치 정보, SQL Injection 공격 등 정보 제공
    - ex) "access denied for user" "using password" site:ac.kr
  - 에러 메시지를 통한 서버 ID/PW 정보 획득, 서버 설치 정보 획득, 공격 루트 확보
    - ex) "HTTP_USER_AGENT=googlebot" site:com

구글 해킹 대응

- 웹 서버 중요 데이터 저장 금지
- 웹 서버 임시 파일 저장 금지
- 웹 서버와 DB서버 분리
- 잘 알려진 googledork 검색어를 통해 주기적인 보안
- 신규 Google Hacking Database 모니터링
  - http://www.exploit-db.com/google-hacking-database/
- 검색 결과 삭제 요청
  - http://www.google.com/remove.html
- 주의사항
  - 개인 - 회원 가입 시 최소한의 정보만을 기입
  - 관리자 - 웹 로그 참조 링크 정보 모니터링

- **What is Shodan?**
  - Shodan is a search engine for Internet-connected devices.
  - Web search engines, such as Google and Bing, are great for finding websites.
  - Traditional web search engines don't let you answer those questions.
    - But what if you're interested in measuring which countries are becoming more connected?
    - Or if you want to know which version of Microsoft IIS is the most popular?
    - Or you want to find the control servers for malware?
    - Maybe a new vulnerability came out and you want to see how many hosts it could affect?
  - Shodan gathers information about all devices directly connected to the Internet.
    - If a device is directly hooked up to the Internet then Shodan queries it for various publicly-available information.
    - The types of devices that are indexed can vary tremendously: ranging from small desktops up to nuclear power plants and everything in between.

기본 검색 옵션

옵션	예제	내용
city	apache city:"Seoul"	검색 결과를 주어진 도시내로 한정하여 보여준다
country	apache country:KR	검색 결과를 주어진 국가내로 한정하여 보여준다
org	org:"University"	검색 결과를 주어진 기관내로 한정하여 보여준다
geo	apache geo 37.5312,126.9147	특정 위도/경도 정보를 참고후, 근처에 있는 검색 결과를 보여준다
product	webcam product:"webcam 7 httpd"	특정 제품에 대한 검색 결과를 보여준다
hostname	"Server: gws" hostname:google	검색 결과에서 주어진 호스트 네임과 매칭 되는 결과를 보여준다
net	net:216.219.143.0/24	특정 주소 대역에 한정하여 검색 결과를 보여준다
os	microsoft-iis os:"windows 2003"	특정 OS에 대한 검색 결과를 보여준다
port	proftpd port:21	특정 포트에 대한 검색 결과를 보여준다
before/after	nginx before:11/03/2020	특정 날짜 전/후에 대한 검색 결과를 보여준다

사용 등록

1. 쇼단 API Code 얻기
   - 유료 결재를 통해 Shodan Add-on 항목에서 "Unlocked API" 를 구매
2. Python 라이브러리 설치하여 사용
   - shodan: The official Python library and CLI for Shodan 사이트 방문하여 다운로드
     - https://github.com/achillean/shodan-python
   - 또는 python pip 이용하여 다운로드
3. 검색을 위한 API 연동 및 python 코드 작성

무료/유료 서비스

- 계정(account)을 가지지 않은 일반 사용자 : 10개, 검색 창에서 필터(filter) 기능 지원 안함
- 계정(account)를 가진 사용자 : 약 20개
- 비용을 지불하는 사용자
  - 월(month) 지불 비용에 따라 다름($59: 1 million개, $299: 20 million개, $899: 무제한)
  - $299부터 보안취약점 filter 인 "vuln" 사용 가능