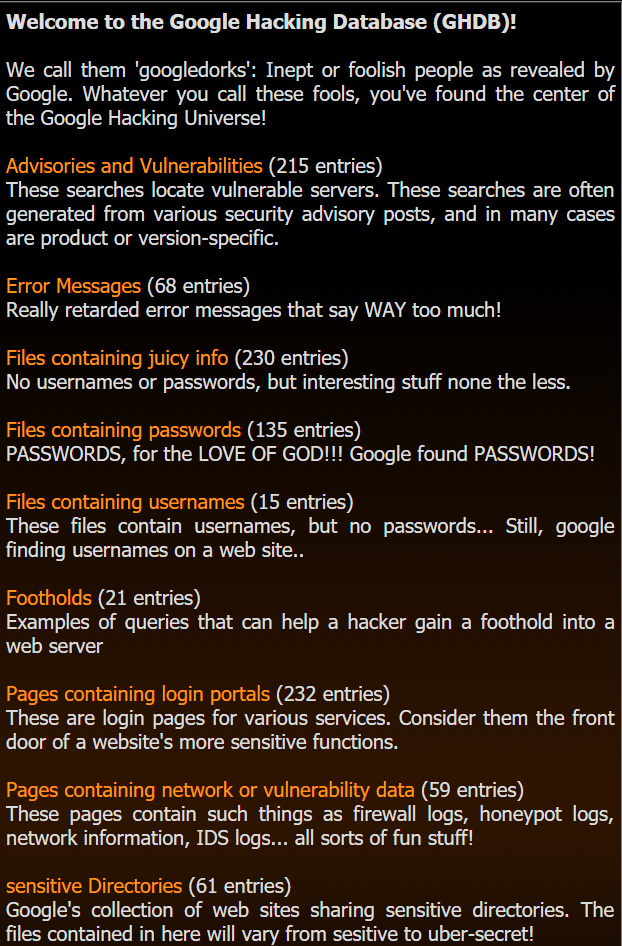
검색엔진 악용

1. 사고사례

#1. 검색에서 주소만 입력해도 관리자 페이지에 접속되는 등 사고사례가 있었음

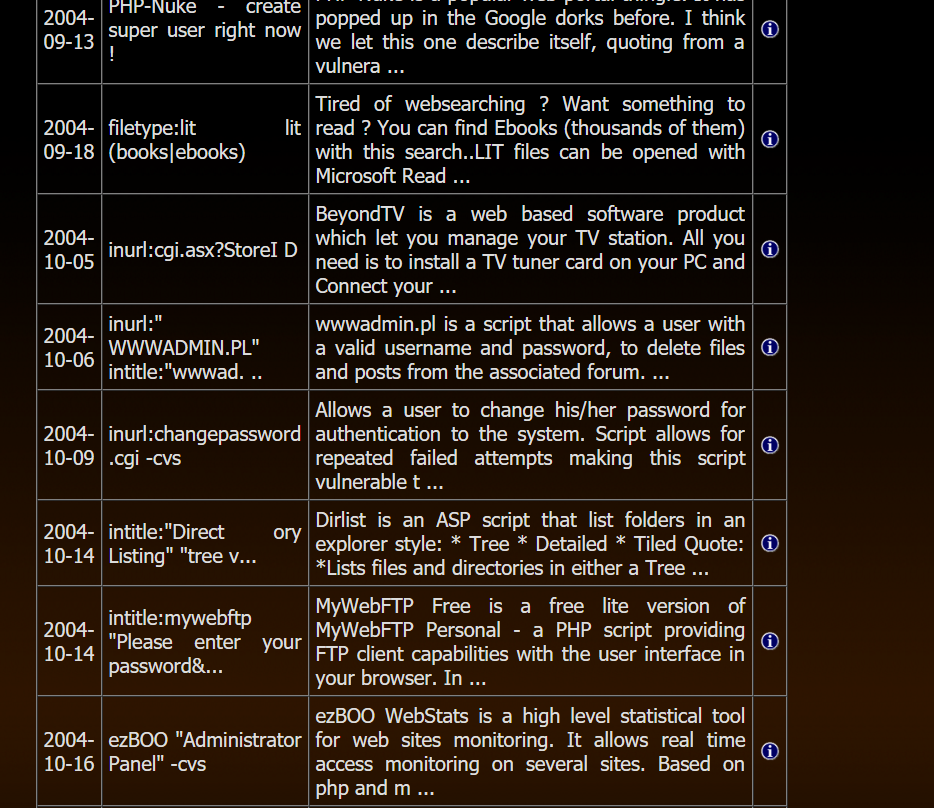
#2. 웹서버내 설정을 잘못하여 국내 방송사 홈페이지 관리자 정보 등 민감한 정보에 접근할 수 있는 것 확인.

1. 구글검색목록
   1. 구글검색 키워드

구글검색을 통한 중요 정보를 검색하기 위해 사용되는 키워드를 정리해 제공해주는 사이트http://www.hackersforcharity.org/ghdb/ 

( “구글해킹”이라는 책을 집필한 작가의 사이트)

|  |  |
| --- | --- |
| 분류 | 내용 |
| Advisories and Vulnerabilities | 보안권고사이트 등에서 제공된 정보를 찾는 등의 취약한 서버를 검색 |
| Error Messages | 에러 메세지를 검색 |
| File containing juicy info | 사용자 계정과 암호가 아닌 중요한 정보를 검색 |
| Files containing usernames | 사용자 계정을 검색 |
| Footholds | 해킹을 위한 다양한 정보를 검색 |
| Pages containing login portals | 다양한 서비스의 로그인 페이지를 검색 |
| Pages containing network or vulnerability data | 방화벽 로그 팟 로그 네트워크 정보 IDS로그등 네트워크 혹은 취약한 데이터를 검색 |
| Sensitive Directories | 민감한 디렉터리 검색 |
| Sensitive Online Shopping Info | 고객 데이터 공급업체 주문 카드번호 신용카드 정보 등 온라인 쇼핑 정보를 검색 |
| Various Onlie Devices | 프린터 비디오 카메라 등 모든 종류의 장치를 검색 |
| Vulnerable Files | 특정한 취약한 파일을 검색 |
| Vulnerable Servers | 특정한 취약점의 서버를 검색 |
| Web Serber Detection | 웹서버 및 버전정보를 검색 |





[GHDB](http://www.hackersforcharity.org/ghdb/) :: Vulnerable Files

intitle:"Index of /" modified php.exe

[http://www.hackersforcharity.org/ghdb_code/i.gif](http://www.hackersforcharity.org/ghdb?function=detail&id=296)

[intitle:"Index of /" modified php.exe](http://www.google.com/search?num=100&hl=en&lr=&ie=UTF-8&safe=off&q=intitle%3A%22Index+of+%2F%22+modified+php.exe&btnG=Search" \t "_blank)

구글검색에 사용되는 연산자.

|  |  |
| --- | --- |
| Intitle | 페이지 제목에서 검색한다(뒤 단어 하나) |
| Allinititle | 페이지 제목에서 검색한다(모든 단어와 구) |
| Inurl | URL에서 문자열을 검색한다Inrul: admin member ->모든 부분에 |
| Allinurl | URL에서 문자열을 검색한다 allInrul: admin member ->URL만 |
| Filetype | 특정종류의 파일을 검색한다. |
| Intext | 페이지 본문에서 문자열을 검색한다. |
| Allintext | 페이지 본문에서 문자열을 검색한다. 2단어 이상 검색 가능 |
| Site | 특정 사이트로 검색 범위를 제한한다. |
| Link | 페이지로의 링크를 검색한다. |
| Inanchor | 링크 문자열 내에서 검색한다 |
| Daterange | 특정 날자 사이에 배포된 페이지를 검색한다. |
| Numrange | 숫자 범위를 검색한다. |
| Cache | 캐시로 저장된 페이지를 검색한다. |
| Info | 사이트에 대한 요약 정보를 출력하며 사이트와 관련된 다른 구글 검색으로의 링크를 제공한다. |
| Related | 특정사이트와 관련되어있다고 판단되는 사이트를 출력한다. |
| Author | 뉴스그룹 게시물의 작성자를 검색한다.이후410 |
| Group | 뉴스그룹이름을 검색한다. 뉴스그룹 이름에서 페이지를 검색한다 |
| Insubject | 뉴스그룹 게시물의 주제를 검색한다. 페이지 제목을 검색한다. |
| Define | 용어의 정의를 검색ㅎ나다. |

1. 모의실습

|  |  |
| --- | --- |
| 구분 | 내용 |
| 테스트 대상 | 외부사이트 |
| 테스트 도구 | 구글페이지 www.google.co.kr |

* 1. 구글해킹 키워드 검색 410 부터
     1. 디렉토리 노출 검색

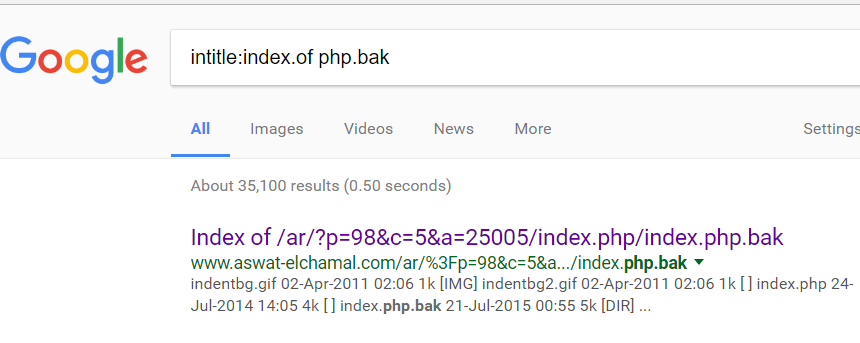
intitle:index.of "parent directory" inurl:admin

디렉터리 노출을 검사하며, URL정보는 관리자 페이지에서 자주 사용되는 키워드

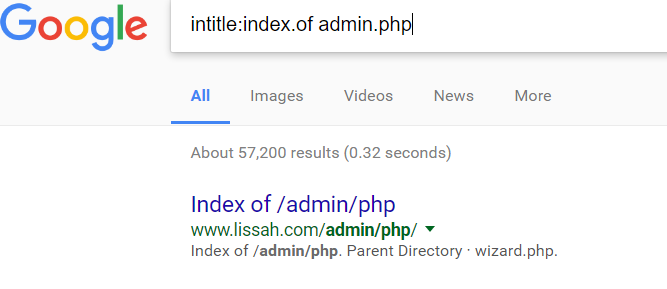


* + 1. 특정파일 검색

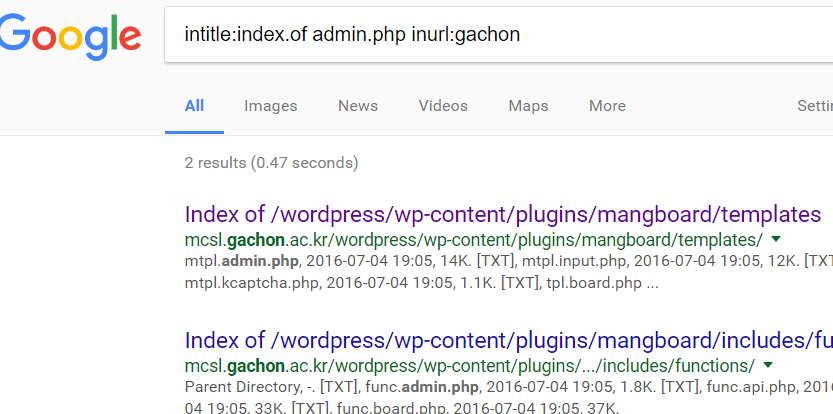
|  |  |
| --- | --- |
| 확장자 | 설명 |
| Bak | 백업파일 |
| Cgi | Cgi 스크립트 파일 |
| Log | 로그파일 |
| Mdb | 마이크로소프트 액세스 데이터베이스 |
| Mdf | 마이크로소프트 MS-SQL Master 데이터베이스 파일 |



디렉터리 노출 내에 php.bak파일을 검색하기 위해 사용되는 키워드



관리자 페이지 정보를 얻을 수 있다.



* 1. 구글해킹 키워드 자동검색

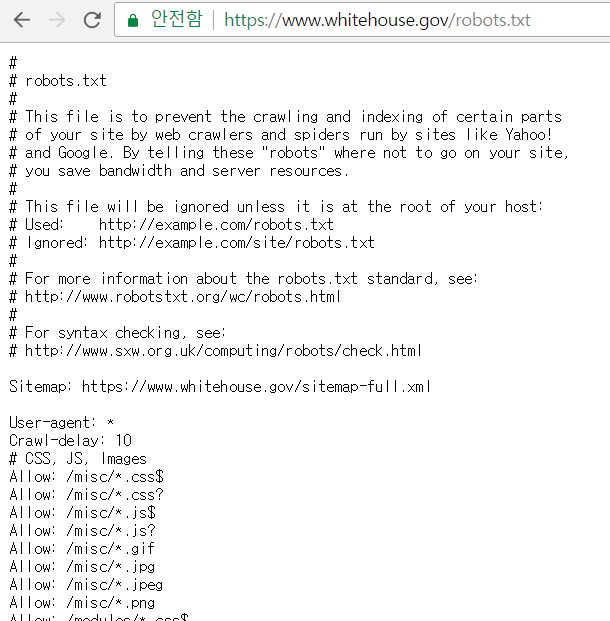
siteDigger을 이용.

* 1. 구글해킹 키워드 검색 툴 제작

파이썬으로 개발.

1. 대책

인터넷 검색엔진 배제 표준

* 검색엔진에 중요정보가 노출되는 것을 방지하기 위한 것이며 로봇 제한 기준 파일인 robots.txt를 통해 검색엔진을 제한할 수 있다.
* Rebots.txt.파일은 웹 컨텐츠 최상위 디렉터리에 생성하여 사용하게 된다.
  + Ex) <http://www.whitehouse.gov/robots.txt>
  + 
  + 검색엔진 접속을 차단하기 위해 등록된 파일이지만 사용자가 직접 해당 컨텐츠 내용을 확인 할 수 있다.
  + 즉 중요한 디렉토리등이 무엇인지를 파악할 수 있는 정보로 악용 될 여지가 있다.
  + 모든 검색엔진의 검색 금지
  + 
  + 
  + 자세한 내용은 http://www.robotstxt.org/