

Oct 8 2012

**Pengenalan Google Hacking**

**Definisi**

Google Hacking adalah istilah yang digunakan bagi sebuah seni atau teknik membuat query-query kompleks pada *search engine* dengan tujuan memfilter hasil pencarian untuk mendapatkan informasi-informasi yang berhubungan dengan keamanan komputer.

Google Hacking dapat dimanfaatkan untuk mendeteksi website-website yang memiliki lubang keamanan dan juga mendapatkan informasi-informasi yang bersifat sensitif dan pribadi seperti nomor kartu kredit, dan bahkan password.

Google hacking melibatkan pemakaian operator-operator google untuk mendapatkan informasi yang diinginkan.

Diantara informasi yang bisa didapatkan menggunakan Google Hacking antara lain :

* Lubang keamanan server.
* Pesan error yang menyimpan terlalu banyak informasi.
* File-file yang menyimpan pasword.
* Direktori-direktori sensitip.
* Halaman web yang berisi login portal.
* Halaman web yang berisi data network atau lubang keamanan seperti log firewall.

**Dasar – dasar Google Hacking**

**Memanfaatkan google untuk mengakses situs yang di blok**

Google dapat bekerja sebagai server proxy yang mengharuskan google melakukan translasi sebuah URL dan memberikan feedback web modifikasi hasil translasi. Dengan metode ini kita bisa mengakses beberapa situs yang di block oleh “cumi” tanpa harus membuat proxy illegal. Layanan google transation dapat di akses di lokasi [**http://translate.google.com**](http://translate.google.com/).

Jika sebuah URL situs yang di blok kita masukkan sebagai input dalam field yang akan ditranslasi, google akan melakukan penerjemahan dan menampilkan halaman web hasil translasi.

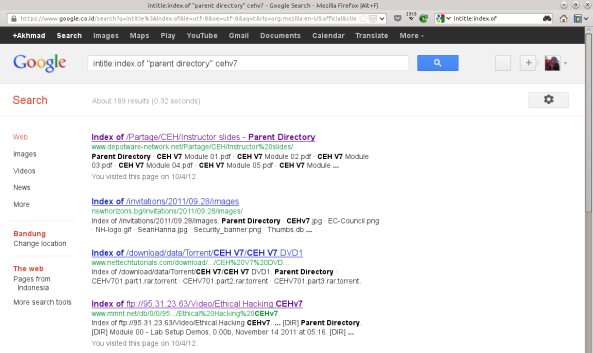
**Directory Listing**

*Directory Listing* adalah tipe halaman web yang menampilkan semua file dan folder yang ada dalam sebuah web server. Directory listing biasanya memiliki *title* yang mendeskripsikan direktori dan juga menampilkan link dari file-file dan folder yang bisa di klik. Lubang keamanan yang bisa kita temukan pada directory listing antara lain :

* Pada umumnya user bebas mendownload file-file dan melakukan navigasi pada folder-folder yang ada.
* Beberapa informasi tentang web server yang dapat membantu penyerangan dapat ditemukan disini.
* Tidak membedakan file-file yang seharusnya publik ataupun privat.
* Pada umumnya directory listing ditampilkan secara tidak sengaja, karena kebanyakan web server menampilkan directory listing jika tidak ditemukan file index pada sebuah direktori.

[](https://akhmadkun.files.wordpress.com/2012/10/googlehack00.png)  
Karena directory listing dapat menampilkan link-link top folder dan memungkinkan user untuk melakukan navigasi ke semua file dan sub-folder yang ada, *attacker* dapat menemukan data-data sensitip hanya dengan mencari directory listing sebuah web server kemudian melakukan navigasi di dalamnya.

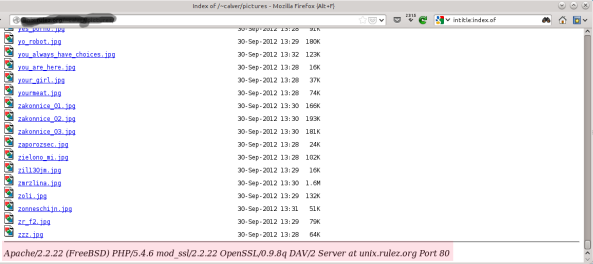
Mencari letak directory listing dengan google cukup dengan menggunakan kata kunci “index of” yang pada umumnya ada di bagian title halaman directory listing. Cara lebih spesifik adalah dengan kata kunci *intitle:index.of* yang dapat menemukan kata “index of” pada bagian title sebuah dokumen web. Kita juga dapat menggunakan kombinasi seperti *intitle:index.of “parent directory”* untuk memastikan google menampilkan hasil pencarian berupa directory listing karena karena keyword *parent directory* juga biasa di temukan pada halaman directory listing.

[](https://akhmadkun.files.wordpress.com/2012/10/googlehack01.png)

**Server Versioning**

Informasi yang dapat digunakan oleh *hacker* untuk menentukan metode yang tepat sebagai penyerangan web server adalah versi software yang digunakan. Hacker dapat mengambil informasi ini dengan melakukan koneksi secara langsung ke port web server dan melakukan request HTTP headers.

Pada umumnya *directory listing* juga menampilkan nama software dan juga versi yang digunakan pada bagian bawah. Bahkan selain informasi versi web server yang digunakan, terkadang operating sistem dan beberapa modul yang terinstall juga dapat kita lihat.

[](https://akhmadkun.files.wordpress.com/2012/10/googlehack02.png)

Masih banyak metode google hacking yang lain yang bisa kita manfaatkan. Selamat belajar 🙂