Lab 06 – Buscador footprinting

Marzo 2014

Descripción

- Implementar una aplicación de escritorio que tenga configurado por default operadores avanzados para búsquedas de información en Google.

- El objetivo de la aplicación es encontrar información que permita generar un reporte (footprinting) de un sitio Web.

- Por default la aplicación ya debe tener búsquedas predefinidas que ayuden a encontrar información sensible (inurl:”Index of”, etc).

Descripción

- La aplicación desarrollada buscará sitios o páginas que pudieran ser vulnerables a SQL Inyection o ver listado de directorios.

- Eres libre de elegir el lenguaje de programación.

- Puedes elegir dos métodos para la implementación
  - Utilizando la API de Google para búsquedas
  - Utilizando un HTML Parser para la Web de Google.com

Método 1

- Crear un motor de búsqueda personalizada
  - https://www.google.com.mx/cse/
- Crear un proyecto en la consola de desarrollador de Google:
  - https://console.developers.google.com/
- Utilizar la API de Google para hacer búsquedas
  - https://developers.google.com/custom-search/json-api/v1/using_rest
- El buscador no permite el uso de operadores avanzados, por lo que tendrás que implementar un mecanismo que te permita filtrar la información obtenida
  - Es decir, utilizando tus propios operadores tipo Google Dorks:
    - site, inurl, typefile, etc.

Método 2

- Enviar peticiones GET/POST directamente al buscador de google: interpretar la información HTML regresada por el sitio

- Para la interpretación de los resultados obtenidos en HTML podrías usar bibliotecas como Jericho HTML Parser.

- Al no usar la API de Google no es necesario que implementes tu propio mecanismo para filtrar información, pues puedes incluir directamente los operadores avanzados de búsqueda.