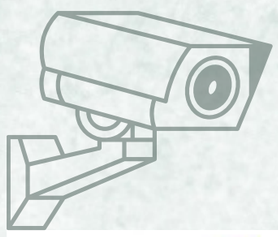
Footprinting with advanced Google Hacking Techniques

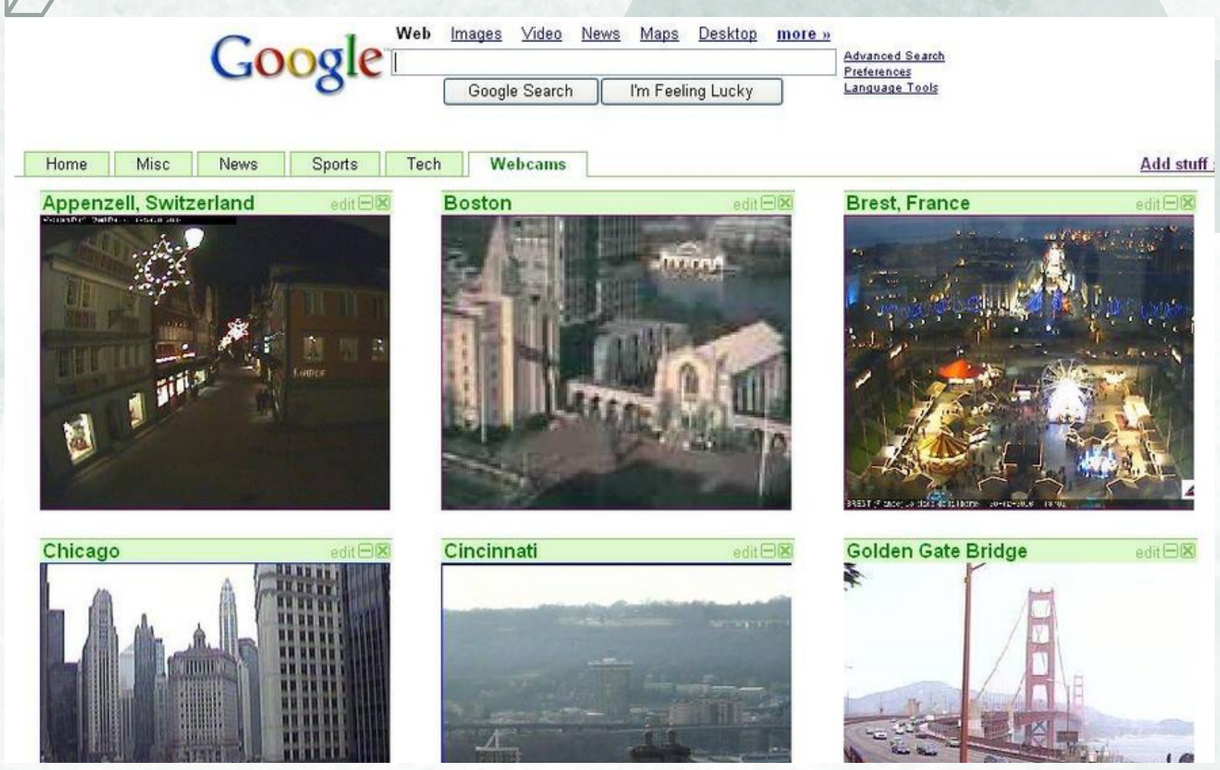
"Gathers information by **locating strings of text** within search results. When a query without advanced search operators is specified, Google **traces** for the search terms in any part of the webpage that includes the title, text, URL and so on." **[1]**

- Use the ***Google Advanced Search option*** to find sites that may link back to the target company's website.
- This may ***extract information*** such as partners, vendors, clients, and other affiliations for target website.
- With Google Advanced Search option, you can ***search web*** more precisely and accurately

"inurl:."domain"/"dorks" "



Explore Live Cameras
inurl:"lvappl.htm" **[2]**



Google has incredible web-crawling skills, it can index practically anything on your website, including sensitive data, even though you can't directly hack websites using it.

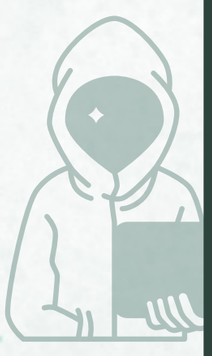
Google Hacking Databases

Google Hacking Database (GHDB): *http://www.hackersforcharity*.org
Google Dorks: *http://www.exploit-db.com*

Google "**Dorking**" is the practice of using Google to find vulnerable web applications and servers by using native Google search engine capabilities.

One of the best ways to prevent Google dorks is by using a **robots.txt** file.

User-agent: *
Disallow: /admin/
Disallow: /privatearea/file.htm



Real Life Attacks

Targeted Phishing Attack: 2016 Gmail Phishing attack exploiting 2FA system

SQL Injection Attack: 'Dark Overload' hacker group gained access to medical records (2018)

Information Disclosure: Security researcher found an unsecure DB containing over 700 million email ID's. (2019)

References

[1] *https://www.stationx.net/how-to-google-dork-a-specific-website/*
[2] *https://medium.com/infosec/exploring-google-hacking-techniques-using-google-dork-6df5d79796cf*

Paarth Kapur - 38
Alekhya Gorugantu - 41
Saloni Saraf - 65
Prof. Ashwini Dalvi
VAPT Dept. Elective -II
Grp ID -

Somaiya TRUST
SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College of Engineering