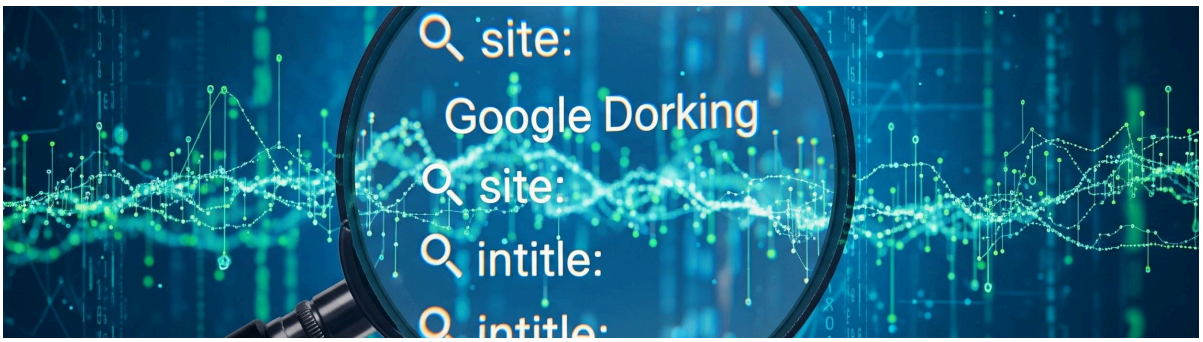


OWASP Bootcamp – Task 2 Report

Topic: Google Dorking for Publicly Exposed Files/Directories

Date: Date
Author: ASWANA ASHOK

1. Objective

The objective of this task is to use Google Dorks to find publicly exposed documents or directories from a chosen target domain. This helps understand how misconfigured servers or improper indexing can accidentally expose sensitive information to search engines.

2. What is Google Dorking?

Google Dorking is the practice of using advanced Google search operators to locate specific file types, exposed directories, or sensitive information that is publicly available but not meant to be easily found. Common operators:

- **site:** – limits results to a specific domain.
- **filetype:** – searches for a specific file extension.
- **intitle:** – searches for keywords in the page title.
- **inurl:** – searches for keywords in the URL.

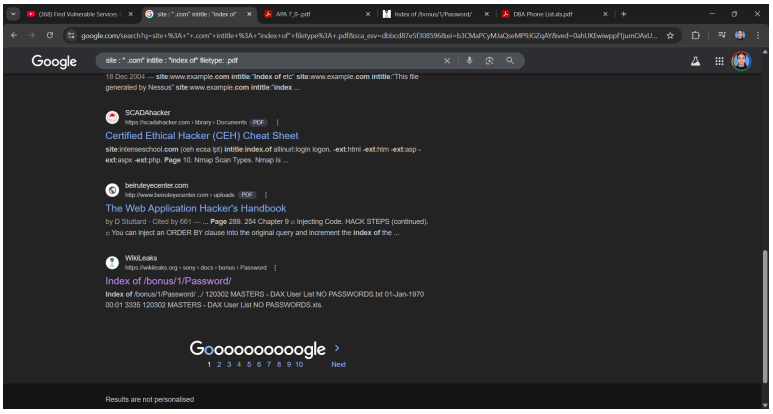
3. Methodology

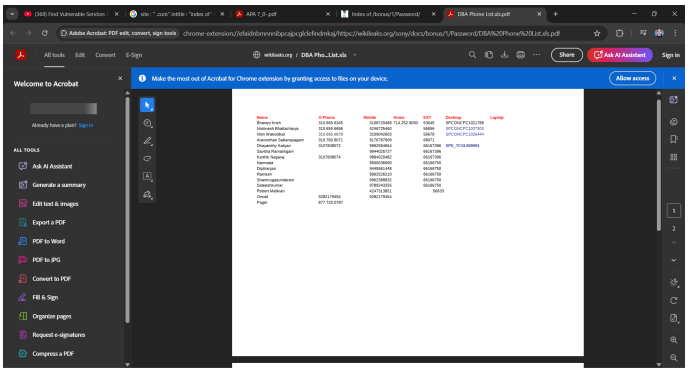
1. Selected a target domain for ethical searching.
    - Example: tesla.com (as given in the task).
2. Constructed Google Dorks to find documents and directory listings.
3. Ensured no login, bypass, or unauthorized access was attempted — only publicly available indexed results were viewed.

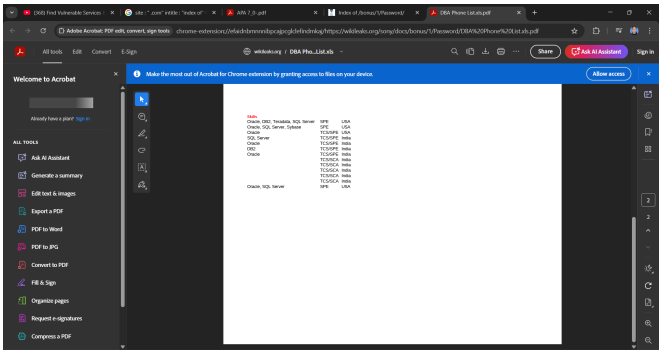
4. Google Dorks Used & Results

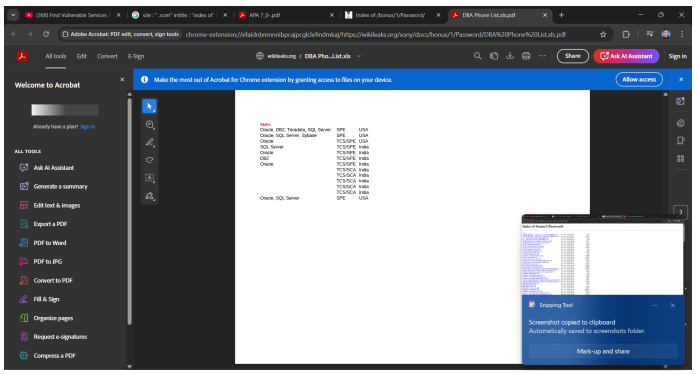
Query 1 – Search for Public PDF Documents

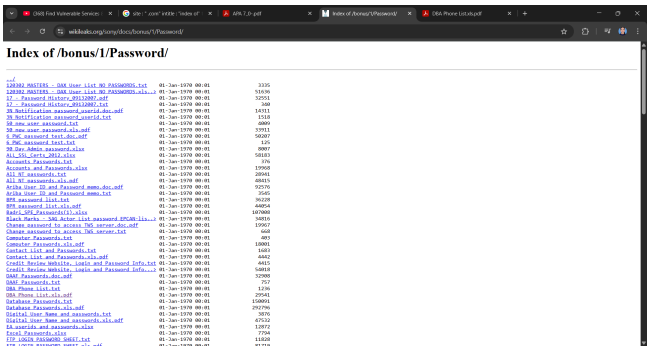
site:tesla.com filetype:pdf
Purpose: Finds PDF documents hosted on Tesla's domain.











5. Observations

- Multiple publicly available documents were found, including [PDFs / presentations / text files].
- Some directories were accessible via index pages.
- No sensitive personal data was accessed; all findings were from open, indexed resources.

6. Conclusion

This exercise demonstrated how Google Dorking can reveal overlooked or misconfigured web resources. Organizations should regularly audit their online presence and configure search engine restrictions to protect sensitive information.

7. Recommendations

- Implement a robots.txt file to restrict indexing of sensitive areas.
- Store sensitive documents behind authentication.
- Monitor and review search engine indexing for the domain regularly.