Google Dorks Report

Name: Richu Joseph

Aim:

To explore and understand the use of Google Dorks for information gathering by identifying publicly exposed directories, login portals, and sensitive files on the internet using advanced Google search operators, while ensuring ethical and legal compliance.

Dork 1:

site:tatamotors.com filetype:pdf

Result:

https://www.tatamotors.com/wp-content/uploads/2023/11/Tata-Motors-Corporate-Presentation-2023.pdf

https://smalltrucks.tatamotors.com/assets/smalltrucks/files/2025-01/Ace%20EV-Brochure.pdf

Dork 2:

site:tatamotors.com intitle:"index of" passwords

Result:

No results found. The domain does not have any publicly indexed directories titled “index of” containing the keyword “passwords”, indicating proper indexing control and better security posture.

Dork 3:

site:tatamotors.com filetype:xls inurl:"email"

Result:

No results found**. The** domain does not have any publicly indexed `.xls` files containing "email" in the URL. This indicates effective data exposure prevention and well-configured access restrictions.

Conclusion:

The exploration of Google Dorks demonstrated how advanced search operators can be leveraged for open-source intelligence (OSINT) gathering. By applying various dorks on both intentionally vulnerable sites and real-world domains such as *tatamotors.com*, it was evident that while some sites may unintentionally expose sensitive information, well-secured domains show no results. Reflecting strong cybersecurity practices.

No sensitive data or vulnerabilities were accessed or exploited during this activity. This task helped reinforce the importance of search engine indexing hygiene, proper server configurations, and awareness of how publicly available information can pose security risks. Overall, this exercise enhanced my understanding of reconnaissance techniques used during the initial stages of ethical hacking and vulnerability assessments