Google Dorking Reconnaissance Report - CUSAT

1.0 Introduction & Objective

This document details the findings of a security reconnaissance exercise conducted on the domain cusat.ac.in and its subdomains. The primary objective of this assessment was to utilize Google Dorking techniques to identify any potentially sensitive, non-public information or misconfigurations that may have been inadvertently exposed to the public via Google's search index.

The assessment aimed to simulate the initial information-gathering phase an external attacker might perform to discover potential vectors for an attack. The focus was on discovering documents, server directories, and other information not intended for public consumption.

2.0 Methodology

The assessment was performed using Google's advanced search operators, a practice commonly known as "Google Dorking." This passive reconnaissance technique uses Google's own indexing power to find specific strings of text, file types, and directory listings that may be of interest. This method does not involve any direct interaction with the target's servers, such as network scanning or intrusion attempts.

The key search operators used in this assessment included:

- site: (To confine the search to the cusat.ac.in domain.)
- filetype: (To search for specific file extensions like pdf, xlsx, etc.)
- intitle:"index of" (To locate server-generated directory listings.)

3.0 Assessment Findings

The reconnaissance process successfully identified several publicly indexed resources. The two most significant categories of findings were analyzed and are detailed below.

Finding 1: Discovery of Public Software Mirror

Dork Used: site:cusat.ac.in intitle:"index of"

Result: An open directory was found at https://foss.cusat.ac.in/mirror/.

Analysis: Investigation of the URL revealed that the subdomain foss.cusat.ac.in hosts a "Free and Open-Source Software" mirror. Universities commonly host mirrors for projects like Debian, Ubuntu, etc., as a public service to the developer community. This provides faster local downloads and supports the open-source ecosystem. The directory and its contents are, therefore, intentionally public. This finding does not represent an accidental data leak or a security vulnerability.

Finding 2: Discovery of Public Accreditation Documents

Dork Used: site:cusat.ac.in filetype:pdf "naac"

Result: Multiple PDF documents were located, for example: https://cusat.ac.in/naac/criteria1/1.4.1/dom/sample.pdf.

Analysis: The files were located within a directory named /naac/. NAAC (National Assessment and Accreditation Council) is the official body for accrediting higher education institutions in India. As part of the accreditation process, universities are often required to make their reports and supporting documents public to ensure transparency. These documents, while containing institutional data, are intentionally published and do not constitute a sensitive data exposure.