Google Dork Report

Dork 1

Query Used:

intext:"SECRET_KEY" ext|py inurl:mysite -site:stackoverflow.com -site:github.com

Results:

https://dashboard.tabtechinc.com/dashboard/mysite/settings.py

Explanation:

This result exposes a settings.py file that contains the SECRET_KEY used in a Django application. Exposure of this key can allow attackers to forge session cookies and potentially gain unauthorized access to the application.

Dork 2

Query Used:

intitle:"index of" /"privatekey.txt" OR "private key.txt"

Results:

https://2021.icaccpa.in/auto-birthday-message/resources/CSE_Alumni.json

Explanation:

These directories contain files or data that expose personal details of students, such as their personal email addresses, dates of birth, and educational background. This is a serious privacy concern and could lead to identity theft or targeted phishing attacks.

Dork 3

Query Used:

intitle:"index of" "credentials.json"

Results:

https://danielatik.com/api/credentials.json

Explanation:

The credentials.json file found here contains a Google API key. If not properly restricted, this API key can be misused by attackers to access APIs, incur costs, or even gain unauthorized access to services.

Submitted By:
Edwin C George