30 Advanced Google Dork Queries for Uncovering Hidden Data and OSINT Insights

Arno Sontheim
.
Follow
Published in
OSINT Team
5 min read
.
Sep 27, 2024
Listen
Share
More

This list is about powerful search techniques for discovering exposed emails, passwords, confidential files, and sensitive information using advanced Google search operators. Ideal for cybersecurity experts and OSINT analysts, this guide enhances your ability to identify vulnerabilities and extract critical intelligence from public sources.

1. Identifying Usernames in Online Forums or Comment Sections

Query:

intext:”username123" intitle:”forum” OR intitle:”comment” OR intitle:”discussion” OR inurl:”/profile/” OR inurl:”/user/” -intitle:”documentation” -filetype:pdf -filetype:docx

Explanation:

Looks for specific usernames in online forums or comment sections, useful for tracking user activity.

2. Finding Leaked Password Lists

Query:

intitle:”index of” (“passwords.txt” OR “leaked-passwords.csv” OR “passwords.bak” OR “secrets.txt”) -git -github -gitlab -bitbucket -intitle:”documentation”

Explanation:

This query helps locate directories containing password lists or leaks.

3. Discovering Sensitive Config Files on Public Servers

Query:

intitle:”index of” (“config.php” OR “wp-config.php” OR “database-config.php” OR “settings.conf” OR “appsettings.json”) AND (“database” OR “credentials”) -intitle:”documentation” -filetype:pdf

Explanation:

Searches for publicly exposed configuration files, often containing database credentials or other sensitive information.

4. Uncovering Exposed Camera Feeds

Query:

intitle:”webcamXP 5" OR intitle:”axis camera” OR intitle:”network camera” OR intitle:”IP camera” OR intitle:”live feed” inurl:”/view/” OR inurl:”/stream/” -intitle:”documentation” -filetype:pdf

Explanation:

This query identifies unsecured IP camera feeds that are publicly accessible.

5. Searching for Publicly Available SSH Keys

Query:

intitle:”index of” (“id_rsa.pub” OR “id_dsa.pub” OR “authorized_keys” OR “ssh_public_key” OR “ssh_keys”) AND (“key” OR “pub”) -intitle:”documentation” -filetype:pdf

Explanation:

Finds publicly exposed SSH key files on servers, which can be crucial in securing systems.

6. Finding Misconfigured Amazon S3 Buckets

Query:

site:s3.amazonaws.com intitle:”index of” (“bucket” OR “files” OR “public” OR “documents” OR “images”) AND (“access” OR “public”) -intitle:”documentation” -filetype:pdf

Explanation:

Targets open Amazon S3 buckets that may contain sensitive information or files.

7. Locating Vulnerable Login Pages

Query:

inurl:”/login.php” OR inurl:”/admin.php” OR inurl:”/signin.php” OR inurl:”/user/login” intitle:”login” OR intitle:”admin” OR intitle:”portal” OR intext:”username” AND intext:”password” -intitle:”documentation”

Explanation:

Identifies public login portals that might be vulnerable to brute force attacks or SQL injections.

8. Discovering Public Network Device Configurations

Query:

intitle:”index of” (“router.conf” OR “switch.conf” OR “firewall.conf” OR “network_settings” OR “device-config”) AND (“network” OR “configuration”) -intitle:”documentation” -filetype:pdf

Explanation:

Searches for exposed network device configuration files, which could reveal network setup or credentials.

9. Tracking Leaked Email Passwords on Pastebin

Query:

site:pastebin.com intext:”email” AND intext:”password” OR intext:”credentials” OR intext:”login” OR intext:”user:pass” -api -key -intitle:”documentation”

Explanation:

Locates email and password combinations that have been leaked and shared on Pastebin.

10. Uncovering Sensitive Government Documents

Query:

site:.gov filetype:pdf OR filetype:xls OR filetype:doc intitle:”confidential” OR intitle:”sensitive” OR intitle:”restricted” OR intitle:”classified” -intitle:”documentation” -filetype:docx

Explanation:

Focuses on publicly accessible government files labeled as confidential or sensitive.

11. Identifying Social Media Profiles via Public Posts

Query:

site:facebook.com OR site:twitter.com OR site:instagram.com OR site:linkedin.com intext:”username” OR intext:”email@example.com” OR intext:”profile” OR intext:”contact”

Explanation:

Searches for specific usernames or emails within social media platforms to track public activity.

12. Discovering Personal Data in Academic Papers

Query:

site:*.edu intext:”personal information” OR intext:”sensitive data” OR intext:”private details” OR intext:”confidential” filetype:pdf OR filetype:docx OR filetype:doc -intitle:”documentation”

Explanation:

Identifies academic papers that may accidentally include personal data.

13. Finding Exposed Database Backups

Query:

intitle:”index of” (“backup.sql” OR “dump.sql” OR “database_backup.sql” OR “data_dump.sql” OR “db_backup.zip”) AND (“database” OR “backup”) -intitle:”documentation” -filetype:pdf

Explanation:

Locates publicly available SQL database backup files, often stored without protection.

14. Exposing Employee Credentials in Internal Reports

Query:

intext:”employee credentials” OR intext:”staff passwords” OR intext:”HR records” OR intext:”login details” filetype:pdf OR filetype:doc OR filetype:xls OR filetype:docx -intitle:”documentation”

Explanation:

Searches for documents containing employee credentials that are unintentionally made public.

15. Tracking Down Exposed Personal Identification Numbers

Query:

intext:”SSN” OR intext:”Social Security Number” OR intext:”personal ID” OR intext:”national ID” OR intext:”identification number” filetype:pdf OR filetype:xls OR filetype:docx -intitle:”documentation”

Explanation:

Looks for files containing sensitive personal identification numbers, such as Social Security numbers in the U.S.

16. Locating Internal Network Diagrams

Query:

intext:”network diagram” OR intext:”network topology” OR intext:”infrastructure map” OR intext:”system architecture” filetype:pdf OR filetype:png OR filetype:jpg OR filetype:svg

Explanation:

Finds network diagrams and topologies that may reveal internal infrastructure layouts.

17. Uncovering Publicly Shared Financial Spreadsheets

Query:

intext:”balance sheet” OR intext:”financial statement” OR intext:”budget report” OR intext:”profit and loss” filetype:xls OR filetype:csv OR filetype:xlsx -intitle:”documentation”

Explanation:

Searches for exposed financial documents like balance sheets or income statements.

18. Tracking Source Code Leaks

Query:

intitle:”index of” (“source code” OR “src.zip” OR “codebase” OR “repository.zip” OR “source_files”) AND (“code” OR

“repository”) -intitle:”documentation” -filetype:pdf

Explanation:

Looks for directories containing publicly exposed source code repositories or files.

19. Finding Exposed API Keys in GitHub Repositories

Query:

site:github.com intext:”API_KEY” OR intext:”SECRET_KEY” OR intext:”access_token” OR intext:”client_secret” OR intext:”auth_token” -README -intitle:”documentation”

Explanation:

Targets exposed API keys that are inadvertently included in public GitHub repositories.

20. Locating Cloud Storage Links

Query:

intext:”drive.google.com” OR intext:”dropbox.com” OR intext:”onedrive.com” OR intext:”icloud.com” OR intext:”mega.nz” filetype:pdf OR filetype:txt OR filetype:doc OR filetype:xlsx -intitle:”documentation”

Explanation:

Searches for exposed links to cloud storage services such as Google Drive or Dropbox.

21. Finding Personal Data in Public Legal Filings

Query:

site:courtlistener.com OR site:justia.com OR site:pacermonitor.com intext:”personal information” OR intext:”confidential” OR intext:”private data” OR intext:”sensitive information” -intitle:”documentation”

Explanation:

Identifies personal information that may be exposed in publicly available legal documents.

22. Discovering Vulnerable IoT Devices

Query:

inurl:”/device.rsp” OR inurl:”/config.xml” OR inurl:”/status.xml” OR inurl:”/device_config” OR inurl:”/admin/config” intitle:”IoT” OR intitle:”device” OR intitle:”configuration” -intitle:”documentation”

Explanation:

Locates configuration or status pages of Internet of Things devices that might be misconfigured or insecure.

23. Uncovering HR Files or Recruitment Documents

Query:

intitle:”HR” OR intitle:”recruitment” OR intitle:”staff” OR intitle:”talent acquisition” OR intitle:”job applications” intext:”resume” OR intext:”CV” filetype:pdf OR filetype:docx -intitle:”documentation”

Explanation:

Finds recruitment documents or HR files containing resumes and other sensitive information.

24. Searching for Public Data Breach Reports

Query:

intitle:”data breach” OR intitle:”security incident” OR intitle:”breach report” OR intitle:”compromise report” filetype:pdf OR filetype:doc OR filetype:xls OR filetype:txt -intitle:”documentation”

Explanation:

Targets reports and documents related to data breaches, often detailing compromised data and vulnerabilities.

25. Identifying Exposed SSL/TLS Certificates

Query:

intitle:”index of” (“ssl.crt” OR “ssl.key” OR “certificate.pem” OR “private.key” OR “tls_certificate” OR “certificates”) -intitle:”documentation” -filetype:pdf

Explanation:

Finds directories containing SSL/TLS certificates, which may be exposed without proper security.

26. Finding Employee Handbooks or Policy Documents

Query:

intext:”employee handbook” OR intext:”HR policies” OR intitle:”company policies” OR intitle:”employee guide” OR intext:”staff manual” filetype:pdf OR filetype:docx -intitle:”documentation”

Explanation:

Locates public employee handbooks or HR policy documents, useful for OSINT on company procedures.

27. Tracking Personal Contact Information in Online Directories

Query:

site:linkedin.com OR site:facebook.com OR site:twitter.com intext:”contact” AND intext:”email@example.com” OR intext:”phone number” OR intext:”address” OR intext:”contact details"

Explanation:

Focuses on personal contact information that may be shared in online profiles or directories.

28. Discovering Publicly Accessible Bug Reports or Vulnerability Logs

Query:

intext:”bug report” OR intext:”vulnerability log” OR intext:”issue tracker” OR intext:”security report” OR intext:”error log” filetype:txt OR filetype:log -intitle:”documentation"

Explanation:

Searches for bug reports or vulnerability logs, which might contain sensitive technical information.

29. Finding Publicly Exposed Corporate Email Lists

Query:

intext:”corporate email list” OR intext:”employee email list” OR intext:”staff email addresses” OR intext:”business email list” filetype:csv OR filetype:txt OR filetype:xlsx -intitle:”documentation"

Explanation:

Identifies publicly shared corporate email lists, useful for OSINT targeting specific organizations.

30. Discovering Exposed Medical Records or Health Data

Query:

intext:”medical record” OR intext:”patient information” OR intext:”health data” OR intext:”clinical data” OR intext:”

Explanation:

Locates publicly accessible medical records or health data files, often unintentionally exposed.

Please keep in mind that the utilization of Google Dorks should always be carried out responsibly and ethically. It is crucial to have authorization when assessing vulnerabilities. Unauthorized entry, into systems or data can be deemed illegal. It is important to adhere to privacy and security regulations while conducting any form of testing or research.