

Forum:[Hack Forums](#)

Thread: [\[MEGA-GUIDE\] The Ultimate Google Dorks Collection for Ethical Hacking & Bug Bounty](#)

kushzh4x - February 23, 2026, 11:03 am

Hi everyone,

Google Dorking (Google Hacking) remains one of the most powerful tools in a researcher's arsenal for the reconnaissance phase. Today, I'm sharing a comprehensive and curated list of dorks to help you identify security flaws and sensitive data exposure.

? ETHICAL NOTICE: This list is for authorized security auditing and educational purposes only. Unauthorized access to data is illegal. Respect the laws and the targets.

Post compiled and shared by: kushzh4x

? 1. Sensitive Files & Information Disclosure

Dorks to find files that should be under lock and key.

Exposed Environment Files: Code filetype:env "DB_PASSWORD" | "SECRET_KEY"

Backup Databases: Code intitle:"index of" "backup.sql" | "dump.sql" | "db_backup.gz"

SSH Private Keys: Code filetype:pem "BEGIN RSA PRIVATE KEY"

Configuration Files: Code extension:config "connectionString="

VS Code Settings (FTP/SSH): Code inurl:".vscode" "sftp.json" | "settings.json"

Git Repositories: Code intitle:"index of" ".git/config"

? 2. Credentials & API Keys

Searching for credential leaks directly within the code.

WordPress Configs: Code filetype:php "DB_PASSWORD" "wp-config.php"

AWS Credentials: Code filetype:txt "aws_access_key_id" | "aws_secret_access_key"

Log Files with Passwords: Code filetype:log "login" | "password" | "user_id"

Firebase Databases: Code inurl:firebaseio.com ".json"

? 3. Login Panels & Admin Portals

To map the attack surface of a target organization.

General Admin Panels: Code intitle:"Login" "admin" inurl:admin

Dashboard Discovery: Code inurl:/dashboard/home.php | inurl:/admin/index.php

Exposed Control Panels: Code intitle:"cPanel" "2082" | intitle:"Plesk" "8443"

Unprotected PHPMyAdmin: Code intitle:"phpMyAdmin" "Running on" inurl:"phpmyadmin"

? 4. Vulnerability Hunting (Potential SQLi/XSS/LFI)

Parameters that are usually "juicy" for finding flaws.

Potential SQL Injection: Code inurl:".php?id=" | inurl:".php?cat=" | inurl:".php?item="

Local File Inclusion (LFI): Code inurl:"include.php?file=" | inurl:"page.php?p="

Open Redirects: Code inurl:"redirect.php?url=" | inurl:"return="

Directory Listing: Code intitle:"index of" "parent directory"

? 5. IoT, Hardware & Industrial Systems

Connected devices that often have weak configurations.

Webcams (Generic): Code intitle:"Live View / - AXIS"

Printers: Code intitle:"Network Print Server" inurl:top.html
Industrial Systems (SCADA): Code intitle:"SCADA Login" | inurl:/Scada/
UPS / Power Systems: Code intitle:"APC Management Card" | inurl:ups_stats.html
? BONUS: Exotic Dorks (2026 Selection) — The kushzh4x Special
These are less common but extremely effective in modern infrastructures:

Jupyter Notebooks: Code intitle:"Jupyter Notebook" inurl:tree
Docker Registry API: Code inurl:/v2/_catalog
Kibana Dashboards: Code intitle:"Kibana" inurl:5601
Exposed Grafana Panels: Code intitle:"Grafana" inurl:3000
ElasticSearch Nodes: Code inurl:9200 "/_cat/indices"
Jenkins Build Servers: Code intitle:"Dashboard [Jenkins]"
Government Documents: Code site:*.gov filetype:pdf "confidential" | "internal use only"
Email Servers (Exposed Logs): Code filetype:log inurl:mail "authentication failed"
? Pro Tips by kushzh4x

Scope your search: Always use Code site:target.com to avoid getting lost in the noise.

Filter by Date: Add Code after:2025 to find recent leaks that haven't been patched yet.

Avoid CAPTCHAs: If Google blocks you, rotate your VPN or use automation tools like Dork-eye.

What's the most interesting thing you've found using these commands? Leave a comment and let's keep this thread updated!

EGY.voldemort - February 28, 2026, 9:13 pm

Awesome