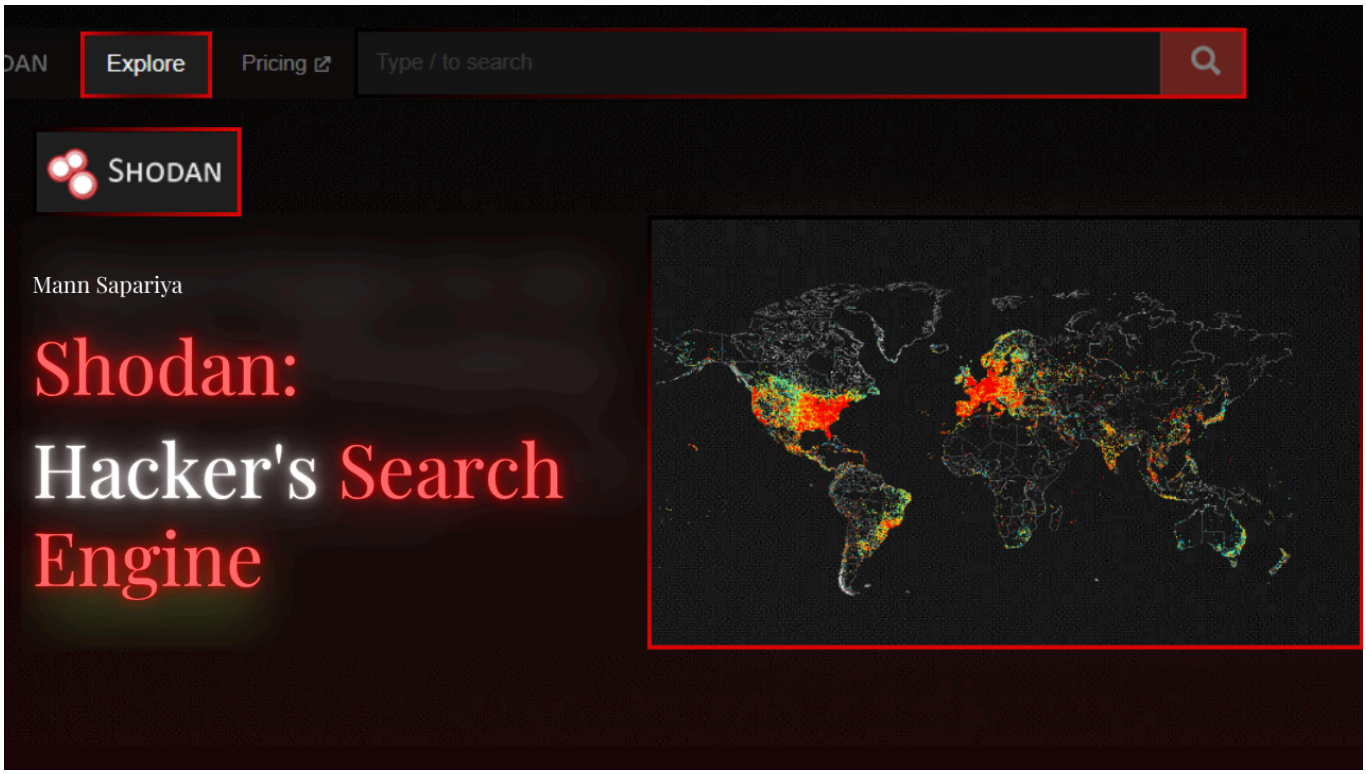
Mastering Shodan Dorking: Finding Gold on the Open Internet

Mann Sapariya 2 Months Ago



Hello, security enthusiasts!

My name is **Mann Sapariya**, and I'm thrilled to welcome you to my new blog dedicated to **bug bounty hunting, advanced reconnaissance, and practical hacking techniques**. Whether you're a beginner or a seasoned researcher, this blog is crafted to help you uncover hidden assets, automate your recon, and maximize your impact in bug bounty programs.

Key Features of This Blog

- **Original, Actionable Content:** Every guide and dork is written from scratch, focusing on real-world use cases and avoiding copyright issues.
- **Step-by-Step Reconnaissance:** Learn how to escalate your searches from basic to advanced, with practical examples and explanations.
- **Advanced Google & Shodan Dorks:** Find hidden endpoints, sensitive files, and vulnerable systems with the latest and most effective search queries.

- **Efficiency Boosters:** Discover automation tips, tool integrations, and unique dork combinations to save time and increase your bug bounty rewards.
- **Ethical Hacking Focus:** All techniques respect legal boundaries and program scopes, empowering you to hack responsibly.

Advanced Google Dorking for Bug Bounty Efficiency

Google Dorking is a powerful OSINT technique for discovering hidden assets, misconfigurations, and vulnerabilities. Here's your ultimate guide to using Google dorks—moving from basic to advanced—so you can supercharge your bug bounty recon.

---

1. Basic Recon Dorks

Exposed Admin Panels

> textintitle:"admin login" site:example.com

Finds possible admin login pages on your target domain.

Public GitHub Secrets

> textfiletype:env site:github.com "API_KEY"

Searches for exposed environment files containing sensitive API keys on GitHub.

Backup Files

> textext:bak inurl:"wp-content" site:example.com

Locates unprotected backup files in WordPress installations.

---

2. Intermediate Asset Discovery

Hidden API Endpoints

> textinurl:/api/v1/ ext:json | xml -site:docs.example.com

Uncovers undocumented API endpoints returning JSON/XML data.

Debug Interfaces

> textintitle:"Debug Console" intext:"Django" OR "Flask"

Finds web applications with active debug consoles.

Subdomain Takeovers

> textsite:*.example.com "404 Not Found" "CNAME"

Identifies subdomains with dangling DNS records, a common target for takeovers.

---

3. Vulnerability-Specific Dorks

Plaintext Credentials

> textallintext:"password=" ext:txt | log | cfg -git

Searches for plaintext passwords in configuration or log files.

Exposed .git Directories

> textintitle:"Index of /.git" "parent directory"

Finds public .git repositories that may leak source code.

AWS Keys in Public Files

> text"AWS_ACCESS_KEY_ID" ext:env | yml | yaml

Targets AWS credentials in environment or YAML files.

SQL Injection Points

> textinurl:index.php?id= intext:"warning" + "mysql"

Looks for URLs with potential SQL injection vulnerabilities.

SSRF/LFI Test Points

> textinurl:"url=http://internal" OR "file=../../etc/passwd"

Finds parameters that may be vulnerable to SSRF or Local File Inclusion.

Open Redirects

> textinurl:"redirect=https://evil.com" site:example.com

Detects open redirect vulnerabilities on your target domain.

---

4. Advanced Dork Combinations

Time-Based Recon

> textafter:2024-01-01 before:2024-06-30 inurl:/wp-admin site:gov

Finds recently updated WordPress admin panels on government sites.

Multi-Operator Precision

> textintitle:"index of" intext:"database" filetype:sql -forum

Targets exposed SQL databases, filtering out forum results.

Third-Party Service Leaks

> text"firebasestorage.googleapis.com" ext:txt "apiKey"

Finds Firebase misconfigurations exposing API keys.

---

5. New & Unique Advanced Dorks (For 2025+)

Exposed Internal Docs

> textsite:example.com inurl:confluence OR inurl:wiki intext:"internal only"

Finds internal documentation mistakenly exposed to the public.

Leaked JWT Tokens

> textintext:"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9" ext:log | txt

Searches for leaked JWT tokens in logs and text files.

Unlisted Dev Environments

> textsite:dev.example.com -www -staging intitle:"Welcome"

Discovers development environments that are not indexed on the main site.

Exposed Cloud Storage Buckets

> textsite:storage.googleapis.com inurl:example-bucket

Finds public Google Cloud Storage buckets related to your target.

CI/CD Pipeline Leaks

> textinurl:".github/workflows" ext:yml intext:"secrets"

Targets GitHub Actions workflow files that may leak secrets.

Optimization & Automation Tips

- **Automate Dorking:** Use tools like GooDork to automate and scale your searches.
- **Combine with Subdomain Enumeration:** Pair Google dorks with tools like Sublist3r or Amass for comprehensive asset discovery.
- **Stay Ethical:** Always operate within bug bounty program scopes and respect `robots.txt` exclusions.

Conclusion

By mastering Google dorking from basic to advanced, you can dramatically improve your bug bounty reconnaissance and vulnerability discovery. This blog will continue to deliver fresh techniques, unique dorks, and actionable insights to help you stay ahead in the security game.

Thank you for joining me on this journey. Happy hacking!

All content is original and designed to help you learn, grow, and succeed in bug bounty and security research. Stay tuned for regular updates and deep dives!

BUGBOUNTY

YOU MAY LIKE THESE POSTS

Mass Subdomain Takeover on NASA.gov – Bug Bounty Write-Up

June 20, 2025

Deep Dive Into HTTP Request Smuggling – A High-Impact Bug for Bounty Hunters

June 14, 2025

🚨 Jenkins Security Guide: Common Bugs & Real-World Exploitation (Beginner to Advanced)

May 28, 2025

0 Comments

To leave a comment, click the button below to sign in with Blogger.

SIGN IN WITH BLOGGER