**Google Exploit Database (Exploit-DB)** — one of the most important resources for ethical hackers, bug bounty hunters, and cybersecurity learners.

**💥 Google Exploit Database (Exploit-DB)**

**Level:** Beginner-Friendly

**Category:** Exploits / Vulnerability Research / Offensive Security

**🧠 What Is Exploit-DB?**

**Exploit-DB** is a **public archive** of known software vulnerabilities and their **exploits**, managed by the **Offensive Security** team (the creators of Kali Linux).

* Website: 🌐 [https://www.exploit-db.com](https://www.exploit-db.com/)
* You can search for **real-world exploits**, proof-of-concept code, and technical writeups.

**🎯 Why Use Exploit-DB?**

| **Reason** | **Purpose** |
| --- | --- |
| 🎓 Learn how real-world exploits work | Reverse engineer or study code |
| 🔍 Find vulnerabilities in software | Especially in older or misconfigured systems |
| 🧪 Use in labs or CTFs | Practice privilege escalation or remote code execution |
| 🔧 Improve defense | Blue teams learn how exploits work so they can defend better |
| 💣 Penetration Testing | Use verified exploits in your test environment or Red Team ops |

**🛠️ How to Use Exploit-DB**

**🔹 1. Browse/Search on the Website**

Go to:  
👉 [https://www.exploit-db.com](https://www.exploit-db.com/)

Use the search bar to look for:

* Software name (WordPress, Apache, OpenSSH, etc.)
* Vulnerability type (LFI, SQLi, RCE)
* CVE number (CVE-2023-12345)
* Platform (Linux, Windows)

**🔹 2. Understand Exploit Details**

Each exploit entry includes:

| **Field** | **Description** |
| --- | --- |
| **EDB-ID** | Unique ID in Exploit-DB |
| **CVE** | CVE ID of the vulnerability (if available) |
| **Date** | When it was published |
| **Author** | Who created the exploit |
| **Type** | Local / Remote / WebApp / Shellcode |
| **Platform** | OS or tech affected |
| **Exploit Code** | Usually in Python, C, Bash, etc. |
| **Download Link** | For the proof-of-concept script |

**🔹 3. Download the Exploit (Example)**

Suppose you're testing a system with **PHP 8.1.0-dev** installed.

Search:

php 8.1.0-dev

Result:  
**EDB-ID 50978** - PHP 8.1.0-dev - Backdoor RCE

Click, download the script, read the code, and test it **only in a lab**.

**📂 BONUS: Use Exploit-DB on Kali Linux (Offline)**

Exploit-DB comes preinstalled in Kali Linux.  
Use the searchsploit command to search offline!

**🔍 Example:**

searchsploit apache struts

**📄 View Full Exploit Code:**

searchsploit -x exploits/linux/remote/48143.sh

**🔁 Update the local database:**

searchsploit -u

**💡 Real-World Use Examples**

| **Scenario** | **Use Exploit-DB to…** |
| --- | --- |
| You found a vulnerable web app | Search for known web app exploits |
| You found a specific software version | Find an exact matching exploit |
| You’re writing a penetration test report | Link CVEs and known exploits |
| You're doing privilege escalation in a CTF | Look up kernel exploits |
| You're building a defense strategy | Learn attacker behavior by studying exploit code |

**⚠️ Legal & Ethical Reminder**

❗ **Exploit-DB is for educational and authorized testing only**  
Using real-world exploits on live/unauthorized systems is **illegal and unethical**.

Always use:

* Virtual labs (TryHackMe, HackTheBox, custom VMs)
* Authorized pentesting environments

**✅ Summary**

| **Feature** | **Description** |
| --- | --- |
| Search Exploits | By software, CVE, or vulnerability type |
| Learn From Code | Study how real exploits work |
| Use in Labs | Great for Red Team, Bug Bounty, CTFs |
| Comes with Kali | Use searchsploit offline |
| Helps Defense | Blue Teams can learn to patch or block attacks |