

# [Exploitation/Réseau]

# Exploit-DB & Searchsploit

## Introduction

La base **Exploit-DB** recense l'ensemble des CVE connues et dont au moins un exploit est disponible.

L'outil **searchsploit** quant à lui s'utilise en ligne de commande et permet de trouver les vulnérabilités disponibles pour une application donnée et pour une version donnée de cette application si elle est composée.



## Exploit-DB

Une barre de recherche est disponible pour taper le numéro de la **CVE** que vous souhaitez rechercher :

EXPLOIT  
DATABASE

☐ Verified ☐ Has App

Show 15

Search:

| Date       | D | A | V | Title   | Type    | Platform | Author                     |
|------------|---|---|---|---|---------|----------|----------------------------|
| 2023-10-09 |   |   |   | Splunk 9.0.5 - admin account take over  | WebApps | Multiple | Redway Security            |
| 2023-10-09 |   |   |   | OpenPLC WebServer 3 - Denial of Service   | DoS     | Multiple | Kai Feng                   |
| 2023-10-09 |   |   |   | Shuttle-Booking-Software v1.0 - Multiple-SQLi   | WebApps | PHP      | nu11secur1ty               |
| 2023-10-09 |   |   |   | Limo Booking Software v1.0 - CORS   | WebApps | PHP      | nu11secur1ty               |
| 2023-10-09 |   |   |   | Webedition CMS v2.9.8.8 - Blind SSRF  | WebApps | PHP      | Mirabbas Agalarov          |
| 2023-10-09 |   |   |   | Atcom 2.7.x.x - Authenticated Command Injection   | Remote  | Hardware | Mohammed Adel              |
| 2023-10-09 |   |   |   | BoldCMS v2.0.0 - authenticated file upload vulnerability                                | WebApps | PHP      | 1337kid                    |
| 2023-10-09 |   |   |   | Cacti 1.2.24 - Authenticated command injection when using SNMP options                  | WebApps | PHP      | Antonio Francesco Sardella |
| 2023-10-09 |   |   |   | Wordpress Sonaar Music Plugin 4.7 - Stored XSS  | WebApps | PHP      | Furkan Karaarslan          |
| 2023-10-09 |   |   |   | Coppermine Gallery 1.6.25 - RCE   | WebApps | PHP      | Mirabbas Agalarov          |
| 2023-10-09 |   |   |   | Media Library Assistant Wordpress Plugin - RCE and LFI                                  | WebApps | PHP      | Florent MONTEL             |
| 2023-10-09 |   |   |   | WEBIGniter v28.7.23 File Upload - Remote Code Execution                                 | WebApps | PHP      | nu11secur1ty               |
| 2023-10-09 |   |   |   | Wordpress Plugin Masterstudy LMS - 3.0.17 - Unauthenticated Instructor Account Creation | WebApps | PHP      | Revan Arifio               |
| 2023-10-09 |   |   |   | Minio 2022-07-29T19-40-48Z - Path traversal   | WebApps | Go       | Jenson Zhao                |
| 2023-10-09 |   |   |   | Microsoft Windows 11 - 'apds.dll' DLL hijacking (Forced)                                | Local   | Windows  | Moein Shahabi              |

Showing 1 to 15 of 45,789 entries

FIRST PREVIOUS 1 2 3 4 5 ... 3053 NEXT LAST

Si on prend l'exemple de la vulnérabilité **Eternal Blue** sortie en 2017, ayant pour nom **CVE-2017-0144**, on peut chercher 2017-0144 dans la barre de recherche pour trouver les exploits disponibles :

EXPLOIT  
DATABASE

☐ Verified ☐ Has App

Show 15

Search: 2017-0144

| Date       | D | A | V | Title  | Type   | Platform       | Author      |
|------------|---|---|---|--|--------|----------------|-------------|
| 2019-10-02 |   |   |   | DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit)                                     | Remote | Windows        | Metasploit  |
| 2017-07-11 |   |   |   | Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010) | Remote | Windows        | sleepya     |
| 2017-05-17 |   |   |   | Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)                     | Remote | Windows        | sleepya     |
| 2017-05-17 |   |   |   | Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010)           | Remote | Windows_x86-64 | sleepya     |
| 2017-05-10 |   |   |   | Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToN' SMB Remote Code Execution (MS17-010)         | Remote | Windows_x86-64 | Juan Sacco  |
| 2017-04-17 |   |   |   | Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)                        | DoS    | Windows        | Sean Dillon |

Showing 1 to 6 of 6 entries (filtered from 45,789 total entries)

FIRST PREVIOUS 1 NEXT LAST

Databases

Links

Sites

Solutions

Exploits

Search Exploit-DB

OffSec

Courses and Certifications

Google Hacking

Submit Entry

Kali Linux

Learn Subscriptions

Papers

SearchSploit Manual

VulnHub

OffSec Cyber Range

Shellcodes

Exploit Statistics

Proving Grounds

Penetration Testing Services

# Searchsploit

Pour chercher les vulnérabilités disponibles pour une application on peut utiliser cette commande :

```
searchsploit <APP> [VERSION]
```

Pour afficher le descriptif d'un exploit :

```
searchsploit -m <EXPLOIT_PATH>
```

---

Revision #3

Created 20 October 2023 15:25:03 by Elieroc

Updated 3 May 2024 13:14:15 by Elieroc