[Exploitation/Réseau] Exploit-DB & Searchsploit

Introduction

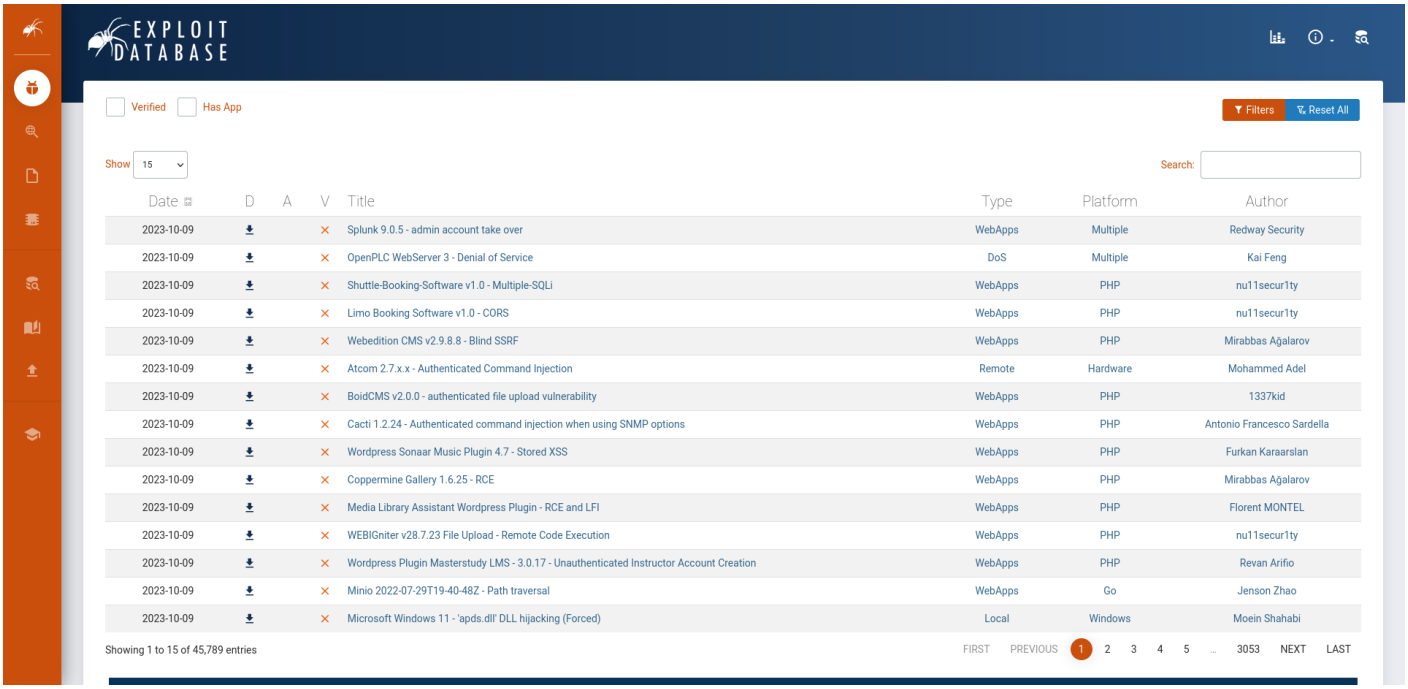
La base **Exploit-DB** recense l'ensemble des CVE connues et dont au moins un exploit est disponible.

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.

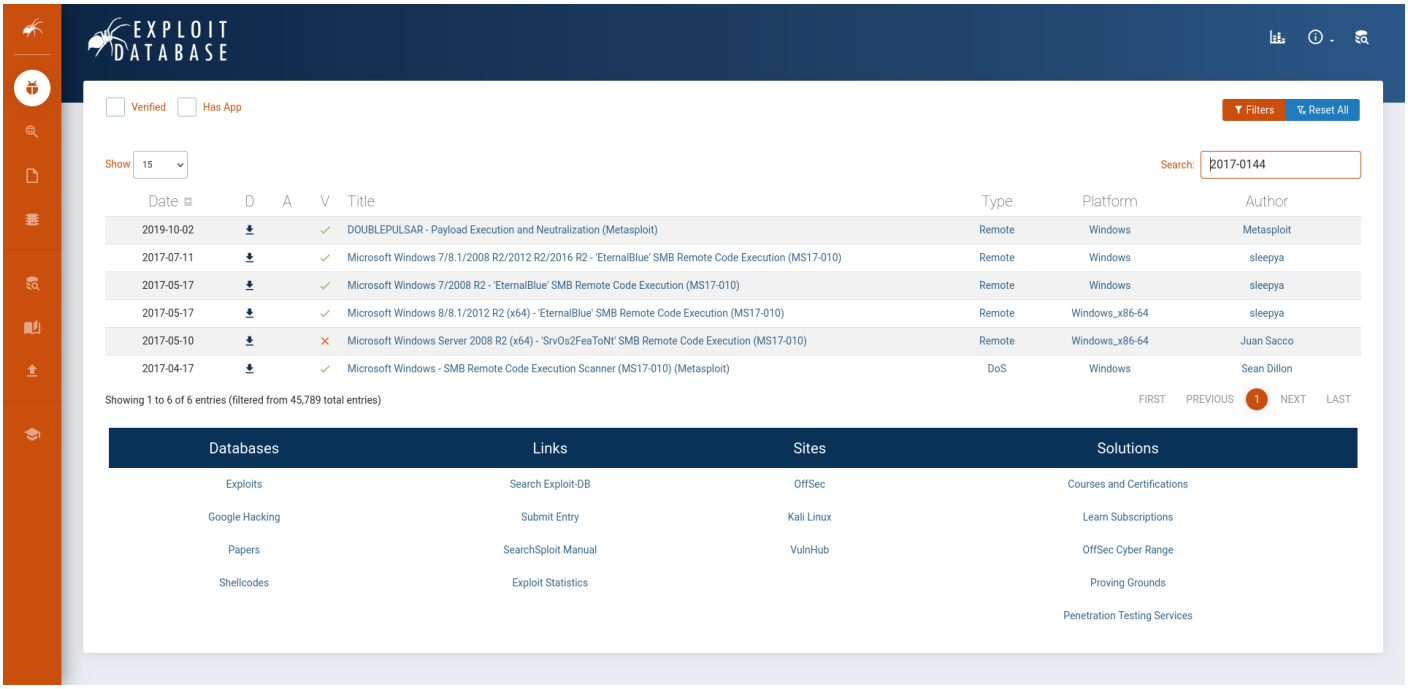


Exploit-DB

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



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 :



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 2023-10-20 15:25:03 UTC by Elieroc
Updated 2024-05-03 13:14:15 UTC by Elieroc