exploit-db : Une base de données d’exploit

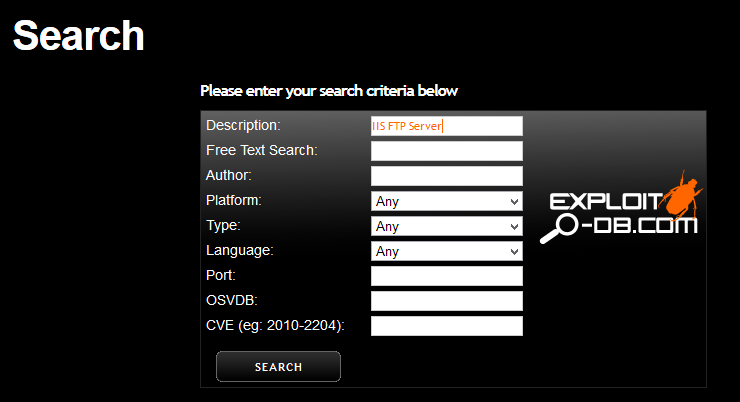
**Penchons-nous un peu sur le site web exploit-db, une plate-forme très connue des experts en sécurité informatique.**

**Exploit-db** n’est rien d’autre qu’une base de données d’exploits qui peuvent être récupérés et utilisés gratuitement. L’intérêt est multiple, à la fois pour les administrateurs systèmes, les pentesters et aussi … pour les pirates informatiques. Il est néanmoins important de souligner que le site web et la base de données associées ont été créés pour les chercheurs de vulnérabilités et les pentesters, comme revendiqué dans la page “*About*” du projet.

Une base de données d’exploit, pourquoi ?

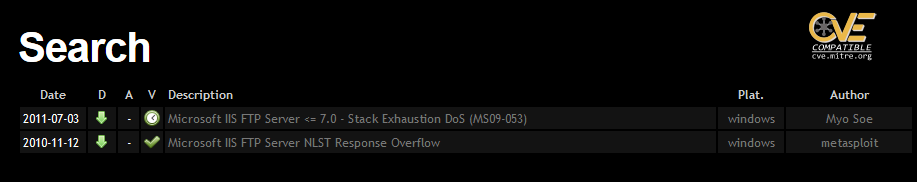
Lorsqu’un pentester découvre une vulnérabilité ou une faiblesse dans un réseau, un système ou une application, il peut écrire un code/script pour exploiter cette vulnérabilité : l’exploit. Cependant l’écriture d’un exploit fonctionnel requiert du temps et des compétences en développement, d’où l’intérêt à la fois de partager les exploits écrits, mais aussi de les centraliser dans une base de données en ligne. **Exploit-db va en effet permettre d’effectuer des recherches par services/produits visés et d’aller jusqu’à la précision de la version vulnérable.**

En tant qu’administrateur système ou que responsable de la sécurité d’un système d’information, exploit-db va permettre de suivre les exploits qui paraissent (bien qu’exploit-db ne soit pas forcément la source la plus réactive pour se tenir au courant des dernières vulnérabilités). On va en effet pouvoir suivre les outils qui peuvent être utilisés contre notre SI et ainsi anticiper les attaques et mieux comprendre les façons dont nous allons être attaqués. La base de données exploit-db va également permettre de savoir si une version d’un de nos services contient une vulnérabilité connue, à la manière des CVE. Par exemple si vous disposez d’un serveur FTP IIS dans votre SI, il vous suffit d’aller dans **“SEARCH”** puis de mettre le nom de votre service dans **“Description”** par exemple :

[[](http://www.information-security.fr/wp-content/uploads/2014/11/exploit-db-01.png)](http://www.information-security.fr/wp-content/uploads/2014/11/exploit-db-01.png)

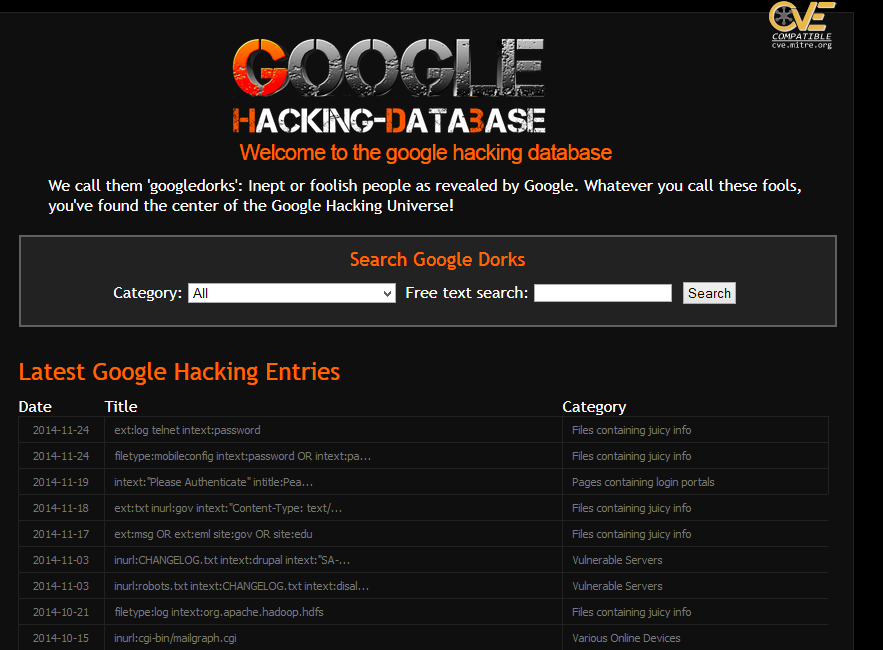
*Formulaire de recherche exploit-db*

Tous les exploits qui se rapportent à **“IIS FTP Server”** vont alors être affichés ainsi que leur date de soumission à la base de données exploit-db, leur état (validé ou en attente de validation), la plate-forme à laquelle ils s’affectent, etc. :

[[](http://www.information-security.fr/wp-content/uploads/2014/11/exploit-db-02.png)](http://www.information-security.fr/wp-content/uploads/2014/11/exploit-db-02.png)

*Résultat d’une recherche d’exploit sur exploi-db*

Outre des exploits écrits et partagés par la communauté, on peut également sur exploit-db trouver un espace dédié aux **Google Dorks**. Pour rappel, les Google Dorks sont des requêtes Google visant à faire ressortir des résultats contenant des informations sensibles. Il arrive très souvent par erreur ou par omission que des données sensibles comme des documents scannés ou des logs se retrouvent indexés par les robots de Google ou d’autres moteurs de recherche. Les Google Dorks vont alors être des requêtes spécialement conçues pour faire ressortir ce type d’information :

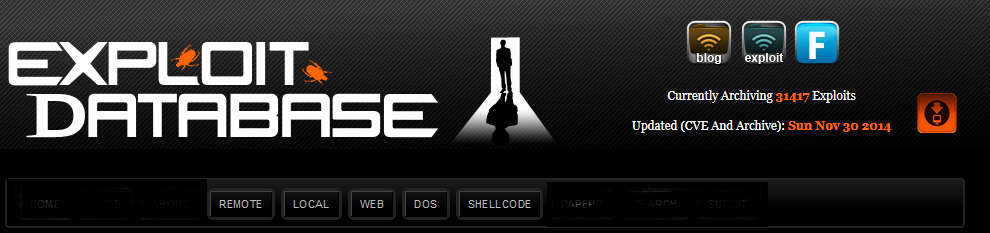
[[](http://www.information-security.fr/wp-content/uploads/2014/11/exploit-db-03.png)](http://www.information-security.fr/wp-content/uploads/2014/11/exploit-db-03.png)

*Google Dorks sur exploit-db*

Si vous retrouvez les données de votre entreprise en utilisant des Google dorks, **il y a de quoi s’inquiéter sérieusement**.

Le but d’exploit-db  est donc de servir une vaste collection d’exploits recueillis par différents moyens, le plus souvent par des soumissions faites par les utilisateurs, mais aussi les listes de diffusion, et d’autres sources publiques, et de les présenter dans une base de données librement accessible et facile à naviguer. La base de données est une base de données **Exploit CVE-Compatible**, c’est-à-dire que l’on peut effectuer une recherche à partir d’un CVE. Cela permet de croiser les sources, par exemple avec des sites comme [CVE-Details](http://www.cvedetails.com/).

La façon la plus courante d’utiliser la base de données exploit-db est tout simplement d’utiliser le module de recherche comme nous l’avons vu plus haut. En naviguant sur le site, on peut voir que les exploits sont découpés en 5 sections :

[[](http://www.information-security.fr/wp-content/uploads/2014/12/exploit-db-04.png)](http://www.information-security.fr/wp-content/uploads/2014/12/exploit-db-04.png)

*Différents types d’exploit sur exploit-db*

On retrouve donc les exploits qui peuvent être utilisés à distance (Remote), les exploits nécessitant d’avoir déjà un accès sur notre cible pour être utilisé en local, les exploits web, ceux visant à causer une attaque par déni de service et les shellcode (code binaire exécutable).

Outre les exploits, on trouvera également les **“Paper”** qui sont des exploits documentés au format PDF, on trouvera par exemple la documentation de PoC (**Proof of Concept**), des revues sur la sécurité ou encore des documents détaillant des vulnérabilités.

Le plus simple pour être le plus souvent à jour est tout simplement de s’abonner au flux RSS du site web.

Il y aurait beaucoup à dire sur cette base de données d’exploit ! Mais le plus simple reste encore de la visiter sur ce lien : [exploit-db](http://www.exploit-db.com/).