



Try
Hack
Me

RECHERCHE DE VULNERABILITE

Teste d'intrusions informatique

08 août 2022

Central-Toyama

1.Vulnérabilités 101

1.1 Introduction

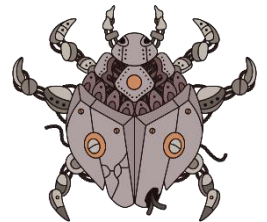
La cybersécurité est une grosse affaire dans le monde moderne. Les piratages dont nous entendons parler dans les journaux proviennent de l'exploitation de vulnérabilités. Dans cette salle, nous allons expliquer exactement ce qu'est une vulnérabilité, les types de vulnérabilités et comment nous pouvons les exploiter pour réussir notre pénétration tentatives de test.

Une grande partie des tests d'intrusion consiste à connaître le compétences et ressources quelle que soit la situation à laquelle vous faites face. Cette pièce va vous présenter quelques ressources indispensables à la recherche vulnérabilités, en particulier, vous allez être initié à :

- Quelles sont les vulnérabilités
- Pourquoi ils méritent d'être appris
- Comment les vulnérabilités sont-elles évaluées
- Bases de données pour la recherche de vulnérabilité
- Une vitrine de la façon dont la recherche sur les vulnérabilités est utilisée dans l'engagement d'ACKme

1.2 Introduction aux vulnérabilités

Une vulnérabilité en cybersécurité est définie comme une faiblesse ou défaut dans la conception, la mise en œuvre ou les comportements d'un système ou d'une application. Un l'attaquant peut exploiter ces faiblesses pour accéder à des informations non autorisées informations ou effectuer des actions non autorisées. Le terme « vulnérabilité » a de nombreuses définitions par les organismes de cybersécurité. Cependant, il y a une variation minime entre eux tous.



Par exemple, NIST définit une vulnérabilité comme « une faiblesse dans un système d'information, la sécurité du système procédures, contrôles internes ou mise en œuvre qui pourraient être exploités ou déclenché par une source de menace ». Les vulnérabilités peuvent provenir de nombreux facteurs, y compris un une mauvaise conception d'une application ou un oubli des actions prévues d'un utilisateur.

Nous reviendrons sur les différents types de vulnérabilités dans une pièce ultérieure. Cependant, pour l'instant, nous devrions savoir qu'il y a sont sans doute cinq grandes catégories de vulnérabilités :

Vulnérabilité	La description
Système opérateur	Ces types de vulnérabilités se trouvent dans les systèmes d'exploitation (OS) et entraînent souvent une élévation des privilèges.
(Mauvais) Basé sur la configuration	Ces types de vulnérabilité proviennent d'une application ou d'un service mal configuré. Par exemple, un site Web exposant les détails des clients.
Identifiants faibles ou par défaut	Les applications et les services qui ont un élément d'authentification seront livrés avec des informations d'identification par défaut lors de l'installation. Par exemple, un tableau de bord administrateur peut avoir le nom d'utilisateur et le mot de passe "admin". Ceux-ci sont faciles à deviner par un attaquant.
Logique d'application	Ces vulnérabilités sont le résultat d'applications mal conçues. Par exemple, des mécanismes d'authentification mal implémentés qui peuvent permettre à un attaquant de se faire passer pour un utilisateur.
Facteur humain	Les vulnérabilités du facteur humain sont des vulnérabilités qui tirent parti du comportement humain. Par exemple, les e-mails de phishing sont conçus pour faire croire aux humains qu'ils sont légitimes.

En tant que chercheur en cybersécurité, vous évalueriez les candidatures et systèmes - en utilisant les vulnérabilités contre ces cibles dans la vie de tous les jours, il est donc crucial de se familiariser avec cette découverte et cette exploitation traitée.

1.3 Évaluation des vulnérabilités (CVSS et VPR)

La gestion de la vulnérabilité est le processus d'évaluation, de catégorisation et finalement remédier aux menaces (vulnérabilités) auxquelles une organisation est confrontée.

Il est sans doute impossible de corriger et de remédier à chaque vulnérabilité d'un réseau ou d'un système informatique et parfois un gaspillage de ressources.

Après tout, seulement environ 2 % des vulnérabilités finissent par être exploitées ([Kenna security.. 2020](#)). Au lieu de cela, il s'agit de s'attaquer aux vulnérabilités les plus dangereuses et réduire la probabilité qu'un vecteur d'attaque soit utilisé pour exploiter un système.

C'est là que le score de vulnérabilité entre en jeu. Vulnérabilité la notation joue un rôle essentiel dans la gestion des vulnérabilités et est utilisée pour déterminer le risque potentiel et l'impact qu'une vulnérabilité peut avoir sur un réseau ou un ordinateur système. Par exemple, le populaire Common Vulnerability Scoring System (CVSS) attribue des points à une vulnérabilité en fonction de ses fonctionnalités, de sa disponibilité et de sa reproductibilité.

Bien sûr, comme toujours dans le monde de l'informatique, il n'y a jamais qu'un cadre ou une idée proposée. Explorons deux des cadres les plus courants et analyser comment ils diffèrent.

Système commun de notation des vulnérabilités

Introduit pour la première fois en 2005, le Common Vulnerability Scoring System (ou CVSS) est un cadre très populaire pour la notation des vulnérabilités et comporte trois itérations principales. Dans l'état actuel des choses, la version actuelle est CVSSv3.1 (avec la version 4.0 actuellement en projet), un score est essentiellement déterminé par certains des facteurs suivants (mais bien d'autres) :

1. Est-il facile d'exploiter la vulnérabilité ?
2. Existe-t-il des exploits pour cela ?
3. Comment cette vulnérabilité interfère-t-elle avec la CIA triade

En fait, il y a tellement de variables que vous devez utiliser une [calculatrice](#) pour déterminer le score à l'aide de ce cadre. Une vulnérabilité est classée (sur cinq) en fonction du score qui lui a été attribué. J'ai mis l'échelle d'évaluation qualitative de la gravité et leurs plages de notes dans le tableau ci-dessous.

Évaluation	Score
Aucun	0
Bas	0.1 - 3.9
Moyen	4.0 - 6.9
Haute	7.0 - 8.9
Critique	9.0 - 10.0

Cependant, CVSS n'est pas une solution miracle. Analysons quelques-uns des avantages et des inconvénients de CVSS dans le tableau ci-dessous :

Avantages de CVSS	Inconvénients du CVSS
CVSS existe depuis longtemps.	CVSS n'a jamais été conçu pour aider à hiérarchiser les vulnérabilités, à la place, il suffit d'attribuer une valeur de gravité.
CVSS est populaire dans les organisations.	CVSS évalue fortement les vulnérabilités d'un exploit disponible. Cependant, seulement 20 % de toutes les vulnérabilités ont un exploit disponible (Tenable., 2020).
CVSS est un cadre libre à adopter et recommandé par des organisations telles que le NIST.	Les vulnérabilités changent rarement de notation après évaluation malgré le fait que de nouveaux développements tels que des exploits peuvent être trouvés.

Évaluation de la priorité des vulnérabilités (VPR)

Le VPR est un cadre beaucoup plus moderne de gestion des vulnérabilités - développé par Tenable, un fournisseur de solutions industrielles pour la gestion des vulnérabilités. Ce cadre est considéré comme axé sur les risques; ce qui signifie que les vulnérabilités reçoivent un score avec un accent particulier sur le risque qu'une vulnérabilité représente pour l'organisation elle-même, plutôt que sur des facteurs tels que l'impact (comme avec CVSS).

Contrairement à CVSS , la notation VPR prend en compte la pertinence d'une vulnérabilité. Par exemple, aucun risque n'est considéré concernant une vulnérabilité si cette vulnérabilité ne s'applique pas à l'organisation (c'est-à-dire qu'elle n'utilise pas le logiciel qui est vulnérable). VPR est également considérablement dynamique dans sa notation, où le risque qu'une vulnérabilité peut poser peut changer presque quotidiennement à mesure qu'elle vieillit.

VPR utilise une plage de notation similaire à CVSS, que j'ai également mise dans le tableau ci-dessous. Cependant, deux différences notables sont que VPR n'a pas de "Aucun/Informationnel" , et parce que VPR utilise une méthode de notation différente, la même vulnérabilité aura un score différent en utilisant VPR qu'en utilisant CVSS.

Évaluation	Score
Bas	0.0 - 3.9
Moyen	4.0 - 6.9
Haute	7.0 - 8.9
Critique	9.0 - 10.0

Récapitulons quelques-uns des avantages et des inconvénients de l'utilisation du VPR dans le tableau ci-dessous.

Avantages du VPR	Inconvénients du VPR
VPR est un cadre moderne qui est du monde réel.	VPR n'est pas open-source comme certains autres frameworks de gestion des vulnérabilités.
VPR prend en compte plus de 150 facteurs lors du calcul du risque.	VPR ne peut être adopté qu'en dehors d'une plateforme commerciale.
VPR est axé sur les risques et utilisé par les organisations pour hiérarchiser les vulnérabilités de correction.	VPR ne considère pas la triade de la CIA dans la mesure où CVSS le fait ; ce qui signifie que le risque pour la confidentialité, l'intégrité et la disponibilité des données ne joue pas un rôle important dans la notation des vulnérabilités lors de l'utilisation de VPR.
Les notations ne sont pas définitives et sont très dynamiques, ce qui signifie que la priorité à accorder à une vulnérabilité peut changer à mesure que la vulnérabilité vieillit.	<i>Intentionnellement laissé en blanc.</i>

1.4 Données de vulnérabilité

Tout au long de votre parcours dans la cybersécurité, vous aurez souvent rencontrer une multitude d'applications et de services différents. Par exemple, un CMS alors qu'ils ont tous le même but, ont souvent conceptions et comportements très différents (et, à leur tour, potentiellement différents vulnérabilités).

Heureusement pour nous, il existe des ressources sur Internet qui suivre les vulnérabilités de toutes sortes de logiciels, systèmes d'exploitation et Suite! Cette salle présentera deux bases de données que nous pouvons utiliser pour rechercher des les vulnérabilités des applications découvertes lors de notre parcours infosec, notamment les sites suivants :

1. [NVD \(Base de données nationale sur les vulnérabilités\)](#)
2. [Exploit-DB](#)

Avant de plonger dans ces deux ressources, assurons-nous que notre compréhension de certains termes clés fondamentaux se trouve sur la même page :

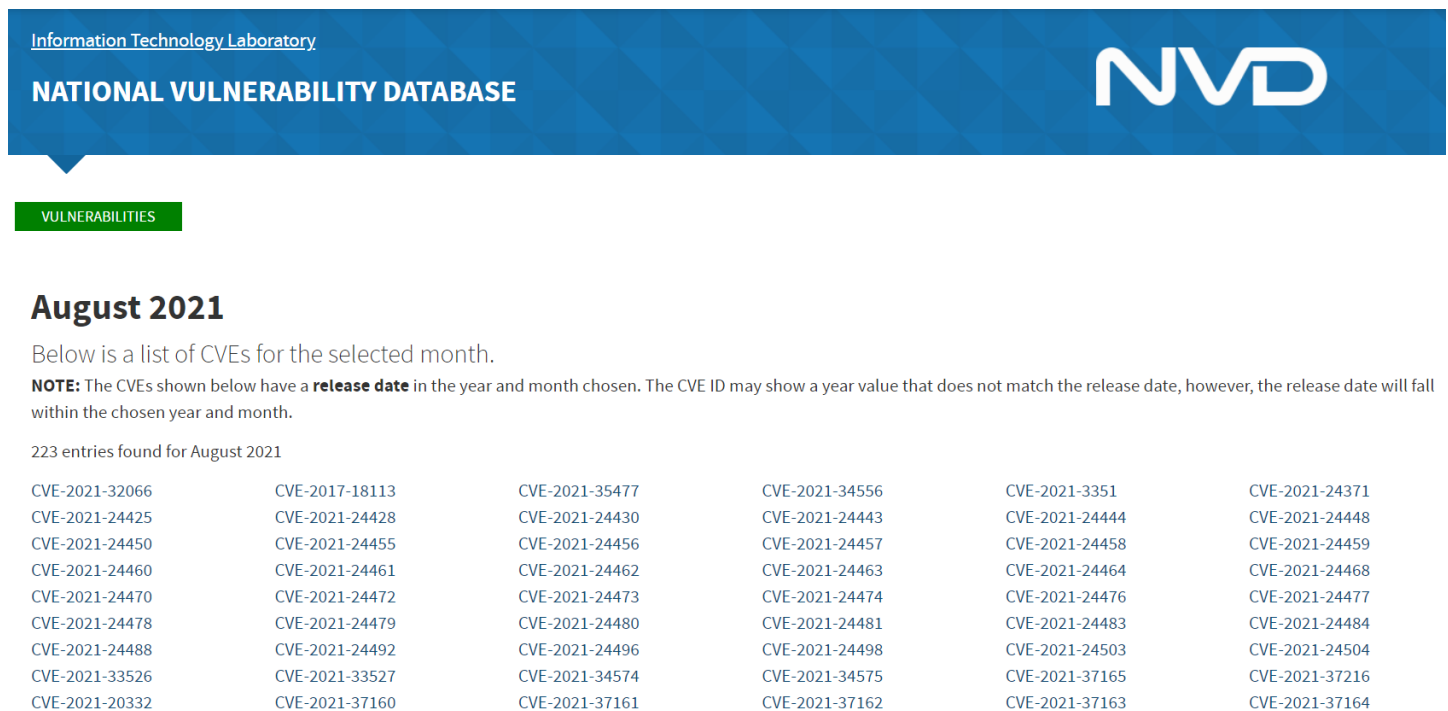
Terme	Définition
Vulnérabilité	Une vulnérabilité est définie comme une faiblesse ou un défaut dans la conception, la mise en œuvre ou les comportements d'un système ou d'une application.
Exploiter	Un exploit est quelque chose comme une action ou un comportement qui utilise une vulnérabilité sur un système ou une application.
Preuve de concept (PoC)	Un PoC est une technique ou un outil qui démontre souvent l'exploitation d'une vulnérabilité.

NVD - Base de données nationale sur les vulnérabilités

La base de données nationale sur les vulnérabilités est un site Web qui répertorie toutes les vulnérabilités classées publiquement. En cybersécurité, les vulnérabilités sont classées sous « **vulnérabilités** expositions **V** et **courantes** » (ou CVE en abrégé).

Ces CVE ont le format de CVE-YEAR-IDNUMBER. Pour exemple, la vulnérabilité utilisée par le célèbre malware WannaCry était CVE-2017-0144.

NVD vous permet de voir tous les CVE qui ont été confirmés, en utilisant des filtres par catégorie et mois de soumission. Par exemple, c'est trois jours en août ; il y a déjà eu 223 nouvelles CVE soumises à ce base de données.



The screenshot shows the NVD website interface. At the top, it says 'Information Technology Laboratory' and 'NATIONAL VULNERABILITY DATABASE' with a large 'NVD' logo. Below this is a green button labeled 'VULNERABILITIES'. The main heading is 'August 2021'. Below the heading, it states 'Below is a list of CVEs for the selected month.' and includes a 'NOTE' about release dates. It then reports '223 entries found for August 2021' and displays a grid of CVE IDs.

CVE-2021-32066	CVE-2017-18113	CVE-2021-35477	CVE-2021-34556	CVE-2021-3351	CVE-2021-24371
CVE-2021-24425	CVE-2021-24428	CVE-2021-24430	CVE-2021-24443	CVE-2021-24444	CVE-2021-24448
CVE-2021-24450	CVE-2021-24455	CVE-2021-24456	CVE-2021-24457	CVE-2021-24458	CVE-2021-24459
CVE-2021-24460	CVE-2021-24461	CVE-2021-24462	CVE-2021-24463	CVE-2021-24464	CVE-2021-24468
CVE-2021-24470	CVE-2021-24472	CVE-2021-24473	CVE-2021-24474	CVE-2021-24476	CVE-2021-24477
CVE-2021-24478	CVE-2021-24479	CVE-2021-24480	CVE-2021-24481	CVE-2021-24483	CVE-2021-24484
CVE-2021-24488	CVE-2021-24492	CVE-2021-24496	CVE-2021-24498	CVE-2021-24503	CVE-2021-24504
CVE-2021-33526	CVE-2021-33527	CVE-2021-34574	CVE-2021-34575	CVE-2021-37165	CVE-2021-37216
CVE-2021-20332	CVE-2021-37160	CVE-2021-37161	CVE-2021-37162	CVE-2021-37163	CVE-2021-37164

Bien que ce site Web aide à suivre les nouvelles vulnérabilités, ce n'est pas génial lors de la recherche de vulnérabilités pour une application spécifique ou scénario.

Exploit-DB

[Exploit-DB](#) est une ressource que nous, en tant que pirates, trouverons beaucoup plus utile lors d'une évaluation. Exploit-DB conserve les exploits pour les logiciels et applications stockées sous le nom, l'auteur et la version du logiciel ou application.

Nous pouvons utiliser Exploit-DB pour rechercher des extraits de code (connu sous le nom de Proof of Concepts) utilisé pour exploiter une vulnérabilité spécifique.

☐ Verified ☐ Has App

Filters Reset All

Show 15

Search:

Date	D	A	V	Title	Type	Platform	Author
2021-08-03			×	Hotel Management System 1.0 - Cross-Site Scripting (XSS) Arbitrary File Upload Remote Code Execution (RCE)	WebApps	PHP	Merbin Russel
2021-08-02			×	Panasonic Sanyo CCTV Network Camera 2.03-0x - 'Disable Authentication / Change Password' CSRF	WebApps	Hardware	LiquidWorm
2021-08-02			×	Online Hotel Reservation System 1.0 - 'Multiple' Cross-site scripting (XSS)	WebApps	PHP	Mohammad Koochaki
2021-08-02			×	Neo4j 3.4.18 - RMI based Remote Code Execution (RCE)	Remote	Java	Christopher Ellis
2021-08-02			×	Men Salon Management System 1.0 - SQL Injection Authentication Bypass	WebApps	PHP	Akshay Khanna
2021-07-29			×	Oracle Fatwire 6.3 - Multiple Vulnerabilities	WebApps	Multiple	J. Francisco Bolivar
2021-07-29			×	CloverDX 5.9.0 - Cross-Site Request Forgery (CSRF) to Remote Code Execution (RCE)	WebApps	Java	niebardzo
2021-07-29			×	Care2x Integrated Hospital Info System 2.7 - 'Multiple' SQL Injection	WebApps	PHP	securityforeveryone.com
2021-07-29			×	IntelliChoice eFORCE Software Suite 2.5.9 - Username Enumeration	WebApps	ASPX	LiquidWorm
2021-07-29			×	Longjing Technology BEMS API 1.21 - Remote Arbitrary File Download	WebApps	Hardware	LiquidWorm
2021-07-29			×	Denver IP Camera SHO-110 - Unauthenticated Snapshot	WebApps	Hardware	Ivan Nikolsky

1.5 Exemple de recherche d'une vulnérabilité

Dans cette tâche, je vais démontrer le processus de recherche d'une vulnérabilité mineure, couplé à des recherches dans les bases de données de vulnérabilités menant à une vulnérabilité et à un exploit beaucoup plus précieux en fin de compte.

Tout au long d'une évaluation, vous combinerez souvent plusieurs vulnérabilités pour obtenir des résultats. Par exemple, dans cette tâche, nous allons exploiter la **Version Disclosure** » vulnérabilité. Avec cette version, nous pouvons ensuite utiliser [Exploit-DB](#) pour rechercher tous les exploits qui fonctionnent avec cette version spécifique.

Les applications et les logiciels ont généralement un numéro de version. Cette information est généralement laissée avec de bonnes intentions ; par exemple, l'auteur peut prendre en charge plusieurs versions du logiciel et autres. Ou parfois, laissé involontairement.

Par exemple, dans la capture d'écran ci-dessous, nous pouvons voir que le nom et le numéro de version de cette application est " **Apache Tomcat 9.0.17** "

Apache Tomcat/9.0.17

If you're seeing this, you've successfully installed Tomcat. Congratulations!

**Recommended Reading:**[Security Considerations How-To](#)[Manager Application How-To](#)[Clustering/Session Replication How-To](#)[Server Status](#)[Manager App](#)[Host Manager](#)**Developer Quick Start**[Tomcat Setup](#)[First Web Application](#)[Realms & AAA](#)[JDBC DataSources](#)[Examples](#)[Servlet Specifications](#)[Tomcat Versions](#)**Managing Tomcat**

For security, access to the [manager webapp](#) is restricted. Users are defined in:

```
$CATALINA_HOME/conf/tomcat-users.xml
```

In Tomcat 9.0 access to the manager application is split between different users.
[Read more...](#)

[Release Notes](#)[Changelog](#)[Migration Guide](#)[Security Notices](#)**Documentation**[Tomcat 9.0 Documentation](#)[Tomcat 9.0 Configuration](#)[Tomcat Wiki](#)

Find additional important configuration information in:

```
$CATALINA_HOME/RUNNING.txt
```

Developers may be interested in:

[Tomcat 9.0 Bug Database](#)[Tomcat 9.0 JavaDocs](#)[Tomcat 9.0 SVN Repository](#)**Getting Help**[FAQ and Mailing Lists](#)

The following mailing lists are available:

[tomcat-announce](#)
 Important announcements, releases, security vulnerability notifications. (Low volume).

[tomcat-users](#)

User support and discussion


[taglibs-user](#)

User support and discussion for [Apache Taglibs](#)

[tomcat-dev](#)

Development mailing list, including commit messages

Avec ces informations en main, utilisons le filtre de recherche sur Exploit-DB pour rechercher tous les exploits pouvant s'appliquer à « **Apache Tomcat 9.0.17** ».



[List](#) [Info](#) [Search](#)

☐ Verified ☐ Has App

[Filters](#) [Reset All](#)

Show 15

Search: Tomcat 9.0

Date	D	A	V	Title	Type	Platform	Author
2021-07-13			×	Apache Tomcat 9.0.0.M1 - Cross-Site Scripting (XSS)	WebApps	Multiple	Central InfoSec
2021-07-13			×	Apache Tomcat 9.0.0.M1 - Open Redirect	WebApps	Multiple	Central InfoSec
2020-01-08			×	Tomcat proprietaryEvaluate 9.0.0.M1 - Sandbox Escape	WebApps	Java	hantwister
2017-10-09			✓	Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)	WebApps	JSP	intx0x80
2017-09-20			×	Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1)	WebApps	Windows	xxlegend

Showing 1 to 5 of 5 entries (filtered from 44,305 total entries)

[FIRST](#) [PREVIOUS](#) 1 [NEXT](#) [LAST](#)

Super ! Après avoir recherché Exploit-DB, il y a un total de cinq exploits qui peuvent nous être utiles pour cette version spécifique de l'application.

2. Exploiter les vulnérabilités

1.1 Automatisé Vs. Recherche manuelle de vulnérabilité

Il existe une myriade d'outils et de services disponibles en cybersécurité pour l'analyse des vulnérabilités. Qu'ils soient commerciaux (et payant une lourde facture) ou open-source et gratuits, les scanners de vulnérabilité sont des moyens pratiques de rechercher rapidement les défauts d'une application.



Par exemple, le scanner de vulnérabilité [Nessus](#) a à la fois une édition gratuite (communautaire) et commerciale. La version commerciale qui coûte des milliers de livres pour une licence d'un an sera probablement utilisée dans les organisations fournissant des services de test d'intrusion ou des audits. Si vous souhaitez en savoir plus sur Nessus, consultez la [salle](#) dédiée.

J'ai détaillé certains des avantages et des inconvénients de l'utilisation d'un scanner de vulnérabilité dans le tableau ci-dessous :

Avantage	Désavantage
Les analyses automatisées sont faciles à répéter et les résultats peuvent être facilement partagés au sein d'une équipe.	Les gens peuvent souvent devenir dépendants de ces outils.
Ces scanners sont rapides et peuvent tester efficacement de nombreuses applications.	Ils sont extrêmement "bruyants" et produisent beaucoup de trafic et de journalisation. Ce n'est pas bon si vous essayez de contourner les pare-feu et autres.
Des solutions open source existent.	Les solutions open source sont souvent basiques et nécessitent des licences coûteuses pour disposer de fonctionnalités utiles.
Les scanners automatisés couvrent un large éventail de vulnérabilités différentes qui peuvent être difficiles à rechercher manuellement.	Souvent, ils ne trouvent pas toutes les vulnérabilités d'une application.

Les frameworks tels que Metasploit ont souvent des scanners de vulnérabilité pour certains modules ; c'est quelque chose que vous découvrirez dans un autre module de ce parcours.

L'analyse manuelle des vulnérabilités est souvent l'arme de choix d'un testeur d'intrusion lors du test d'applications ou de programmes individuels. En fait, l'analyse manuelle implique la recherche des mêmes vulnérabilités et utilise des techniques similaires à l'analyse automatisée.

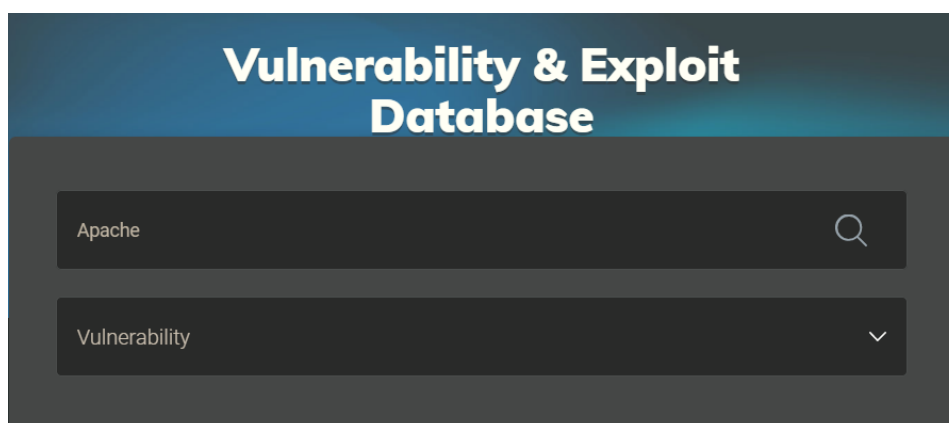
En fin de compte, les deux techniques impliquent de tester une application ou un programme pour détecter les vulnérabilités. Ces vulnérabilités incluent :

Vulnérabilité	La description
Mauvaises configurations de sécurité	Les erreurs de configuration de sécurité impliquent des vulnérabilités dues à la surveillance des développeurs. Par exemple, exposer les informations du serveur dans les messages entre l'application et un attaquant.
Contrôle d'accès cassé	Cette vulnérabilité se produit lorsqu'un attaquant est capable d'accéder à des parties d'une application qu'il n'est pas censé pouvoir accéder autrement.
Désérialisation non sécurisée	Il s'agit du traitement non sécurisé des données envoyées via une application. Un attaquant peut être en mesure de transmettre un code malveillant à l'application, où il sera ensuite exécuté.
Injection	Une vulnérabilité d'injection existe lorsqu'un attaquant est capable d'entrer des données malveillantes dans une application. Cela est dû à l'échec de ne pas s'assurer (connu sous le nom de désinfection) que l'entrée n'est pas nocive.

1.2 Recherche d'exploits manuels

Rapid7

Tout comme d'autres services tels que Exploit DB et NVE, Rapid7 est une base de données de recherche de vulnérabilités. La seule différence étant que cette base de données agit également comme une base de données d'exploits. Grâce à ce service, vous pouvez filtrer par type de vulnérabilité (c'est-à-dire application et système d'exploitation).



De plus, la base de données contient des instructions pour exploiter des applications à l'aide de l'outil populaire Metasploit (vous en apprendrez plus sur cet outil plus tard dans le parcours d'apprentissage). Par exemple, cette entrée sur [Rapid7](#) est pour " [Wordpress Plugin SP Project & Document](#) ", où nous pouvons voir des instructions sur la façon d'utiliser un module d'exploit pour abuser de cette

```
1 msf > use exploit/multi/http/wp_plugin_sp_project_document_rce
2 msf exploit(wp_plugin_sp_project_document_rce) > show targets
3 ...targets...
4 msf exploit(wp_plugin_sp_project_document_rce) > set TARGET < target-id >
5 msf exploit(wp_plugin_sp_project_document_rce) > show options
6 ...show and set options...
7 msf exploit(wp_plugin_sp_project_document_rce) > exploit
```

vulnérabilité.

GitHub

[GitHub](#) est un service Web populaire conçu pour les développeurs de logiciels. Le site est utilisé pour héberger et partager le code source des applications afin de permettre un effort collaboratif. Cependant, les chercheurs en sécurité se sont également tournés vers cette plate-forme pour les raisons susmentionnées. Les chercheurs en sécurité stockent et partagent les PoC (preuves de concept) sur GitHub, les transformant en une base de données d'exploits dans ce contexte.

GitHub est extrêmement utile pour trouver des exploits rares ou frais, car n'importe qui peut créer un compte et télécharger - il n'y a pas de processus de vérification formel comme c'est le cas avec les bases de données d'exploits alternatives. Cela dit, il y a aussi un inconvénient dans le fait que les PoC peuvent ne pas fonctionner là où peu ou pas de support sera fourni.

Repositories 9K

Code 11M

Commits 7M

Issues 5M

Discussions 228

Packages 12

Marketplace 4

Topics 569

Wikis 3K

Users 2K

Languages

Python 2,763

C 740

Shell 646

JavaScript 477

Java 408

HTML 407

9,682 repository results

Sort: Best match

zhzyker/exphub

Exphub(漏洞利用脚本库) 包括Weblogic、Struts2、Tomcat、Nexus、Solr、Jboss、Drupal的漏洞利用脚本，最新添加CVE-2020-14882、CVE-2020-11444、CVE-2020-1...

poc exploit drupal nexus tomcat vulnerability webshell exp weblogic getshell

cve-2020-1938 cve-2020-2551 cve-2020-2555 cve-2020-10199 cve-2020-10204 cve-2020-2883

cve-2020-11444 cve-2020-5902 cve-2020-14882

☆ 2.9k ● Python Updated on 4 Apr

0xn0ne/weblogicScanner

weblogic 漏洞扫描工具。目前包含对以下漏洞的检测能力：CVE-2014-4210、CVE-2016-0638、CVE-2016-3510、CVE-2017-3248、CVE-2017-3506、CVE-2017-10271、CVE...

cve-2019-2725 cve-2020-2551 cve-2020-2555 cve-2018-2894 cve-2019-2729 cve-2014-4210

cve-2017-10271 cve-2020-2883 cve-2019-2888 cve-2019-2890 cve-2019-2618 cve-2018-3252

cve-2018-3245 cve-2018-3191 cve-2018-2893 cve-2017-3248 cve-2016-3510 cve-2016-0638

cve-2020-14882 cve-2020-14883

☆ 1.2k ● Python Updated on 27 Nov 2020

nongiaich/CVE

☆ 191 ● C Updated on 25 Oct 2017

GitHub utilise un système de marquage et de mots-clés, ce qui signifie que nous pouvons rechercher GitHub par des mots-clés tels que "PoC", "vulnérabilité", et bien d'autres. Au moment de la rédaction, il existe 9 682 référentiels avec le mot-clé "cve". Nous sommes également en mesure de filtrer les résultats par langage de programmation.

Recherche

Searchsploit est un outil disponible sur les distributions de pentesting populaires telles que Kali Linux. Il est également disponible sur la TryHackMe AttackBox. Cet outil est une copie hors ligne d'Exploit-DB, contenant des copies d'exploits sur votre système.

Vous pouvez rechercher searchsploit par nom d'application et/ou type de vulnérabilité. Par exemple, dans l'extrait ci-dessous, nous recherchons sur searchsploit des exploits liés à Wordpress que nous pouvons utiliser - aucun téléchargement nécessaire !

Utilisation de Searchsploit pour rechercher des exploits liés à "Wordpress"

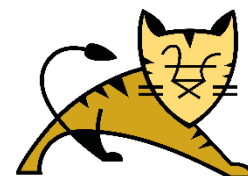
```
searchsploit wordpress
```

```
WordPress Theme Think Responsive 1.0 - Arbitr | php/webapps/29332.txt
WordPress Theme This Way - 'upload_settings_i | php/webapps/38820.php
WordPress Theme Toolbox - 'mls' SQL Injection | php/webapps/38077.txt
WordPress Theme Trending 0.1 - 'cpage' Cross- | php/webapps/36195.txt
WordPress Theme Uncode 1.3.1 - Arbitrary File | php/webapps/39895.php
WordPress Theme Urban City - 'download.php' A | php/webapps/39296.txt
WordPress Theme Web Minimalist 1.1 - 'index.p | php/webapps/36184.txt
WordPress Theme White-Label Framework 2.0.6 - | php/webapps/38105.txt
WordPress Theme Wp-ImageZoom - 'id' SQL Injec | php/webapps/38063.txt
WordPress Theme Zoner Real Estate - 4.1.1 Per | php/webapps/47436.txt
```

1.3 Exemple d'exploitation manuelle

Nous pouvons utiliser les informations recueillies à partir de la tâche 2 dans cette salle pour exploiter le service vulnérable. En fin de compte, l'une des vulnérabilités les plus efficaces que nous pouvons exploiter est la possibilité d'exécuter des commandes sur la cible qui exécute l'application ou le service vulnérable.

Par exemple, être capable d'exécuter des commandes sur la cible qui exécute l'application ou le service vulnérable nous permettra de lire des fichiers ou d'exécuter des commandes que nous ne pouvions pas exécuter auparavant en utilisant l'application ou le service seul. De plus, nous pouvons en abuser pour gagner ce que l'on appelle une prise de pied sur la machine. Un pied est un accès à la console de la machine vulnérable, où nous pouvons alors commencer à exploiter d'autres applications ou machines sur le réseau.



Apache Tomcat

Nous allons utiliser un exploit pour exécuter du code à distance sur l'application de la tâche 2 afin de pouvoir exécuter à distance des commandes sur la machine vulnérable.

Avant de commencer, il est important de noter que les exploits sortent rarement de la boîte et sont prêts à être utilisés. Ils nécessitent souvent une certaine configuration avant de fonctionner pour notre environnement ou notre cible. Le niveau de configuration varie selon l'exploit, vous

Vous trouverez donc souvent plusieurs exploits pour la même vulnérabilité sur une application. C'est à vous de déterminer quel exploit est le plus approprié ou le plus utile pour vous.

Par exemple, dans l'extrait ci-dessous, nous pouvons voir que quelques options ont été modifiées pour refléter l'adresse IP de la machine à partir de laquelle nous attaquons.

Modifier un Exploit (Avant)

```
nano exploit.py
mymachine="192.168.1.10"
port="1337"
```

Modification d'un exploit (après)

```
nano exploit.py
mymachine="10.13.37.10"
port="1337"
```

Une fois que nous avons correctement configuré l'exploit, lisons plus en détail cet exploit pour comprendre comment l'utiliser. Dans l'extrait ci-dessous, nous pouvons voir que nous devons fournir deux arguments lors de l'exécution de l'exploit :

Lister les arguments d'un exploit

```
exploit.py --help
To use this exploit, provide the following arguments:
-u The URL of the application
-c the command that you wish to execute
```

Avec ces informations à l'esprit, nous sommes maintenant prêts à utiliser cet exploit sur la machine vulnérable. Nous allons faire ce qui suit :

1. Utilisez l'exploit pour télécharger un fichier malveillant dans l'application vulnérable contenant la commande que nous souhaitons exécuter, où le serveur Web exécutera ce fichier malveillant pour exécuter le code.
2. Le fichier contiendra d'abord une commande de base que nous utiliserons pour vérifier que l'exploit a fonctionné.
3. Ensuite, nous allons lire le contenu d'un fichier situé sur la machine vulnérable.

Exécution de l'exploit pour afficher le nom de l'utilisateur sous lequel l'application s'exécute

```
exploit.py -u http://10.10.10.10 -c "whoami"
www-data
```

Exécution de l'exploit pour afficher le contenu d'un fichier sur la machine cible

```
exploit.py -u http://10.10.10.10 -c "cat flag.txt"
```