



# Projet des 5 vulnérabilités

23.02.2021

MASTER SSI M1

**Lien du site web : <http://praise-gamemaster.ddnsking.com/>**

HAROUNI DJIHANE OUM KELTOUM

171731091986

ZIANI Mohamed Riad

171731074153

## Aperçu

Internet est né dans la fin des années 80 et le Web au début des années 90, offrant un mode de consultation passif des sites Web à l'utilisateur. Les années 2000 ont vu l'émergence du Web 2.0 rendant l'internaute actif et créateur de contenu et amenant les applications sur la toile.. Il n'est donc pas étonnant qu'elles soient devenues une cible privilégiée des pirates. En profitant des vulnérabilités mais celles-ci sont exposées à une plus grande population. Les problèmes peuvent aller jusqu'au vol d'informations confidentielles et à la corruption de l'application.

Mais d'abord c'est quoi une vulnérabilité ?

### Les vulnérabilités

Une vulnérabilité est une faille de sécurité. Elle provient dans la majorité des cas d'une faiblesse dans la conception d'un système d'information (SI), d'un composant matériel ou d'un logiciel.

Toutes les vulnérabilités ne mènent pas forcément à une cyberattaque. En effet, elles sont majoritairement rendues publiques et corrigées.

Pour ce projet nous allons développer, concevoir et réaliser un site web contenant cinq vulnérabilités exploitables, et leur exploitation doit permettre à l'attaquant de prendre le contrôle de la machine cible (notre machine virtuelle qui héberge le site web vulnérable ).

## L'Environnement de Travail :

Dans la réalisation de ce site web on a :

- Utiliser **Windows Server 2012 R2** comme Système d'exploitation.
- **WAMP** comme plateforme de développement web utilisant principalement *Apache* comme logiciel serveur chargé de servir les pages Web. Lorsque vous demandez qu'une page soit vue par vous, Apache accepte votre requête via HTTP et vous montre le site.  
*MySQL* est un système de gestion de bases de données relationnelles SQL open source développé et supporté par Oracle.  
*PHP* est un langage de scripts généraliste et Open Source, spécialement conçu pour le développement d'applications web. Il peut être intégré facilement au HTML/CSS.
- *No-IP* comme service DNS Dynamique.
- *Router Port Forwarding* pour configurer le Router a rediriger les requêtes de communication d'une adresse ip à une autre passant par le port choisi.

## Les Vulnérabilités qu'on a implémenter :

### I. SQL injection :

Criticité : haute.

Exploitation : moyenne.

Correction : moyenne.

Cette vulnérabilité permet à un attaquant d'avoir toutes les informations contenues dans la base de données, y compris les login et les mot de passe des utilisateurs et même l'administrateur .

#### Exploitation :

On injecte le code SQL suivant dans l'URL de la page **redact.php** (dans l'onglet qui affiche les informations sur les rédacteurs de l'article de Top News ) et exactement dans la variable **"id\_news"** :

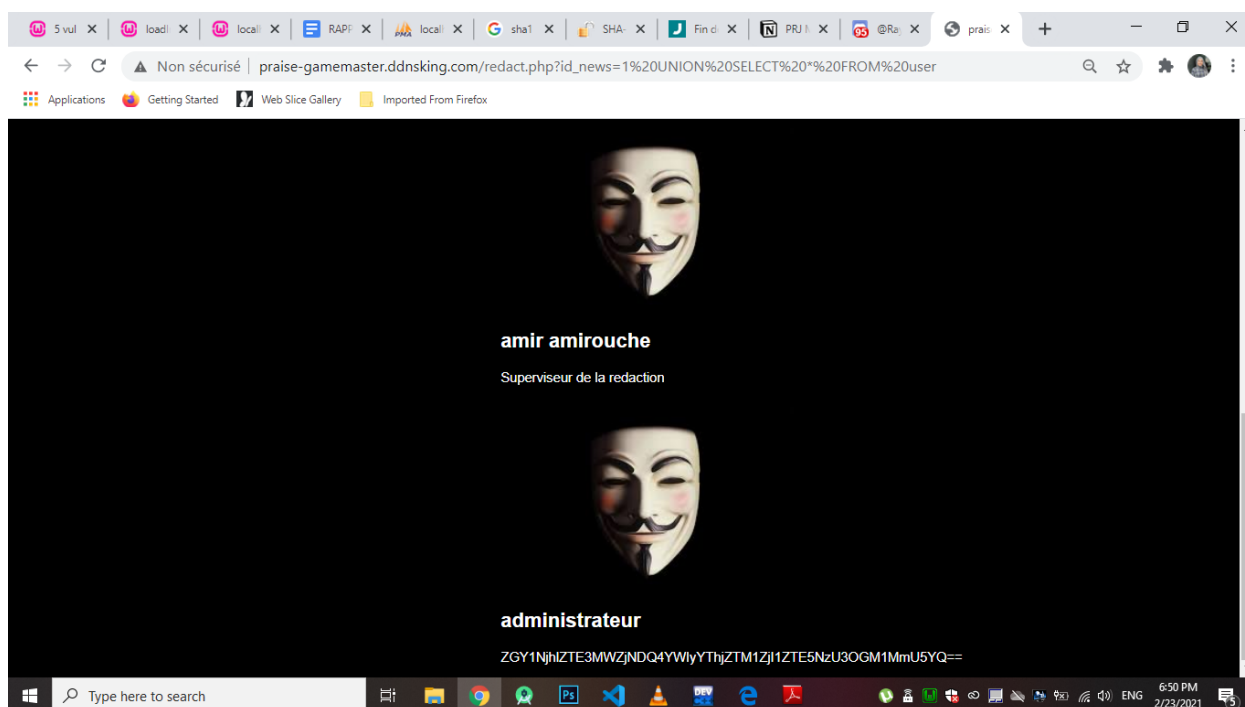
```
UNION SELECT * FROM user
```

Et là l'attaquant pourra récupérer les informations confidentielles (username + password) de l'admin à la place des informations des rédacteurs .

Mais après les mots de passe sont d'abord hashés à l'aide de l'algorithme SHA-1 (Secure Hash Algorithm) et coder en base64, un indice est caché dans une photo dans la page des news, l'attaquant devras récupérer le message secret grâce au site de stéganographie en ligne pour déduire le type de chiffrement utilisé (SHA1).

Afin de récupérer les mot de passe en clair l'attaquant est censé décoder le mdp enregistré dans la base de données en base64 et après chercher dans les base de données proposer en ligne pour le dehash.

1- il récupère d'abord les données de l'admin en utilisant SQL injection comme le montre la figure suivante :



2- il decode en base64 il retrouve la valeur hash du mot de passe

Df568ee171fc448ab2a8ce35f25e197578c52e9a

3- enfin il récupère le mot de passe grâce au base de données en ligne ou il retrouvera le hash SHA1(on a utiliser la stéganographie avec le site mentionné dans l'article de stéganographie pour donner un indice sur le type de hash) du mot de passe qui est : Jz3Xb@8g2U

### Recommandations :

- Il est recommandé de filtrer les données rentrées par les utilisateurs, pour qu'elles ne contiennent pas des caractères comme ",', #, etc. La fonction `mysql_real_escape_string()` offerte par le SGBD MySQL assure ce type de filtrage.
- Validation des données d'entrée : les données remises devraient toujours être en accord avec le type de données attendu. Si un **paramètre** numérique est requis, vous pouvez le vérifier avec un script PHP à l'aide de la fonction `is_numeric()`.
- Les requêtes paramétrées sont un moyen de pré-compiler une instruction SQL afin que vous puissiez ensuite fournir les paramètres afin que l'instruction soit exécutée. Cette méthode permet à la base de données de reconnaître le code et de le distinguer des données d'entrée.

## II. Arbitrary File Upload :

Criticité : moyenne.

Exploitation : facile.

Correction : moyenne.

Cette vulnérabilité offre à un attaquant la possibilité d'uploader des fichiers sur le site web. Si les fichiers uploader sont des scripts ou des exécutables, ils représentent alors une grande menace s'ils sont exécutés.

### Exploitation :

Dans la page réservée à l'administrateur après s'être authentifié le bouton "contribuer" lui permet d'uploader un fichier .pdf ou .txt qui recevra un nom aléatoire, l'attaquant peut changer l'extension de son fichier malveillant et uploader un web shell-script .php ,asp etc pour passer le filtre et le lancer à l'aide d'une autre méthode d'exploitation comme l'OS command injection.

1- Après avoir connecté en tant qu'administrateur l'attaquant peut afficher une des actualités d'une catégorie en appuyant sur **Plus**, puis en appuyant sur **contribuer** un formulaire s'affiche pour remplir le titre de l'article et télécharger un fichier .pdf ou .txt qui contient le contenu de l'article et là réside cette vulnérabilité puisque on peut caster un fichier .php sous .php.pdf, et malgré qu'on génère un nom random du pdf téléchargé dans notre répertoire contrib, l'attaquant pourra comme même récupérer le nom de ce fichier grâce à une autre vulnérabilité par exemple OS command injection ou il pourra lister le répertoire et retrouver le chemin vers son fichier uploader.

Exemple ici on upload action.php.pdf

phares dans laquelle on se glissera da  
virus, le concours d'entrée se fera donc  
certains mystères dans un lieu aussi d

re bouleversé par le Covid. En raison du  
audio !) pour avancer et résoudre

**E-Mail**

djihane.harouni@gmail.com

**Titre de l'article**

Le Bayern Munich a mis un genou à terre la semaine dernière. Un coup de pompe qui

Choisir un fichier action.php.pdf

Contribuer

Cancel

**Attack on Titan ne finirait peut être pas d'adapter la série de la saison 4**

Attack on Titan a progressé avec une quatrième saison épique, mais n'a pas immunisé les fans contre la spéculation. Après tout, le spectacle est celui qui  
engendre des théories de fans, mais les fans sont plus préoccupés par le rythme de la saison quatre. On dit que la saison est la dernière de l'animé, mais il y a

2-On exécutant la commande dans la bar recherche: **Le manga Midnight Eye Gok||cd /contrib & dir >dircontrib.txt**

17 - Goc 17.pdf prai: x localhost sha1 - R SHA-1 C Fin de la PRJ MEI @Rayzi Arrêtez t - PHP, A PHP ne t +

Non sécurisé praise-gamemaster.ddnsking.com/details.php

Applications Getting Started Web Slice Gallery Imported From Firefox

All News Contribuer

Le manga Midnight Eye Gok||cd /contrib & dir >dircontrib.txt

Search

**Les Actualites**

Le manga Midnight Eye Gok||cd /contrib & dir >dircontrib.txt



```

Le volume dans le lecteur C n'a pas de nom.
Le num,ro de s,rie du volume est 2E91-6E0C

R,pertoire de C:\wamp64\www\contrib

23/02/2021  21:13    <DIR>          .
23/02/2021  21:13    <DIR>          ..
23/02/2021  19:26                947 603548cb226736.31460196.pdf
23/02/2021  21:13                0 dircontrib.txt
                2 fichier(s)                947 octets
                2 Rép(s) 95ÿ542ÿ968ÿ320 octets libres

```

Et là on retrouve le fichier créer pour lister le répertoire contrib et on remarque aussi le pdf uploader et son nom random.

### Recommandations :

Améliorer le filtre d'extension en utilisant des méthodes de vérification plus efficaces et utiliser des API qui détectent le type des fichiers ( comme le redimensionnement d'images ).

## III. OS command injection (Exécution de commandes arbitraires) :

Criticité : haute.

Exploitation : moyenne.

Correction : moyenne.

L'injection de commande du système d'exploitation (également appelée injection shell) est une vulnérabilité de sécurité Web qui permet à un attaquant d'exécuter des commandes arbitraires du système d'exploitation (OS) sur le serveur qui exécute une application, et de compromettre généralement complètement l'application et toutes ses données. Très souvent,

un attaquant peut exploiter une vulnérabilité d'injection de commande du système d'exploitation pour compromettre d'autres parties de l'infrastructure d'hébergement, exploitant les relations de confiance pour faire pivoter l'attaque vers d'autres systèmes au sein de l'organisation.

### Blind OS command injection :

De nombreuses instances d'injection de commandes OS sont des vulnérabilités aveugles. Cela signifie que l'application ne renvoie pas la sortie de la commande dans sa réponse HTTP. Les vulnérabilités aveugles peuvent encore être exploitées, mais différentes techniques sont nécessaires.

#### Exploitation :

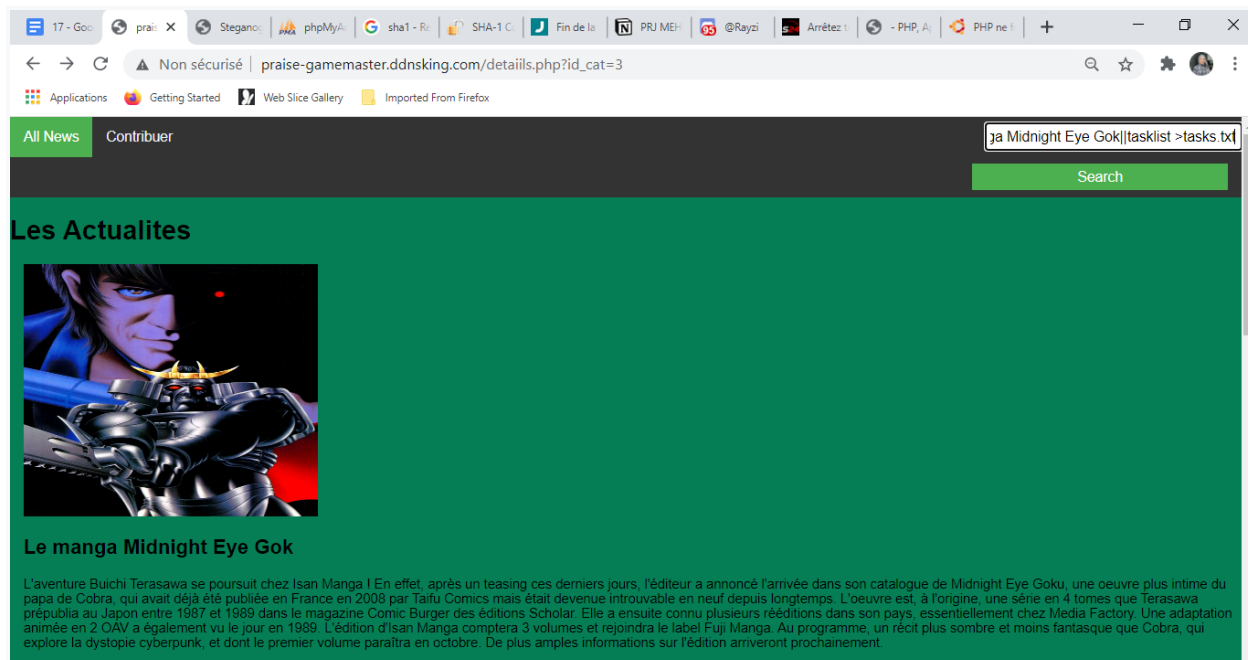
Pour notre cas la vulnérabilité réside dans le champ de recherche dans la page de détails de n'importe quelle catégorie de News lors de la recherche l'attaquant peut exécuter une commande sur le cmd du serveur .

Cette faille est dû à l'utilisation de la fonction **shell\_exec** dans PHP qui permet d'exécuter un programme externe via le shell, puis renvoie le résultat sous forme d'une chaîne, mais pour notre cas il doit redirectionner le résultat pour pouvoir le consulter.

L'attaquant peut par exemple afficher les informations concernant PHP en utilisant la commande **"php -i"**, ou peut être afficher le contenu du répertoire désiré. Ou bien l'utiliser pour localiser un fichier uploadé par la vulnérabilité précédente et l'exécuter ou bien même ouvrir un shell sur le serveur pour initier une escalation de privilège.

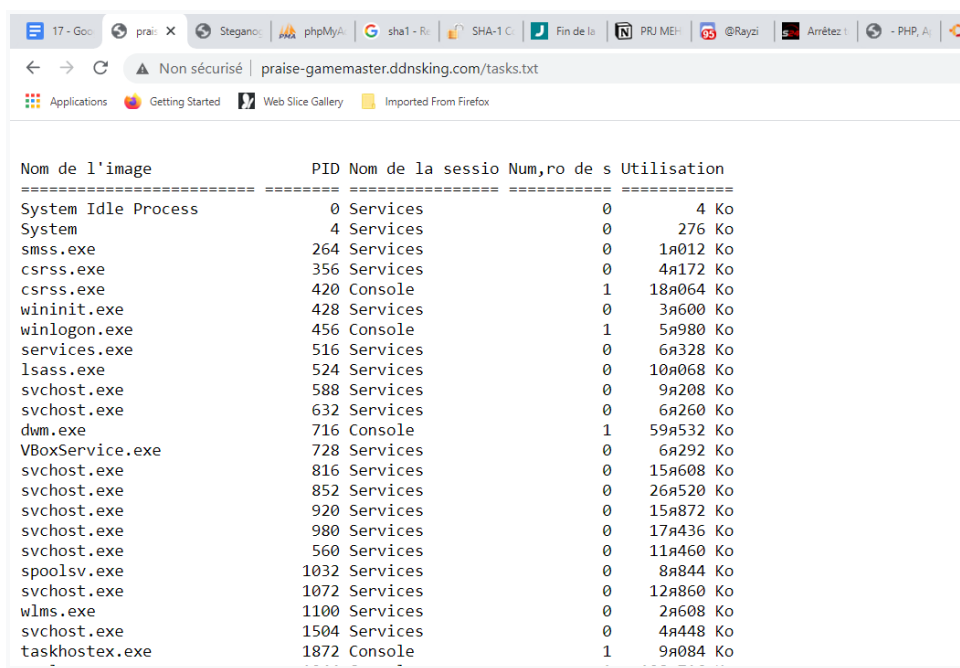
## 1- Le manga Midnight Eye Gok||tasklist >tasks.txt

la ca vas me retourner le résultat du titre chercher et aussi va exécuter la commande tasklist ou on redirectionne le résultat dans tasks.txt



**Le manga Midnight Eye Gok**

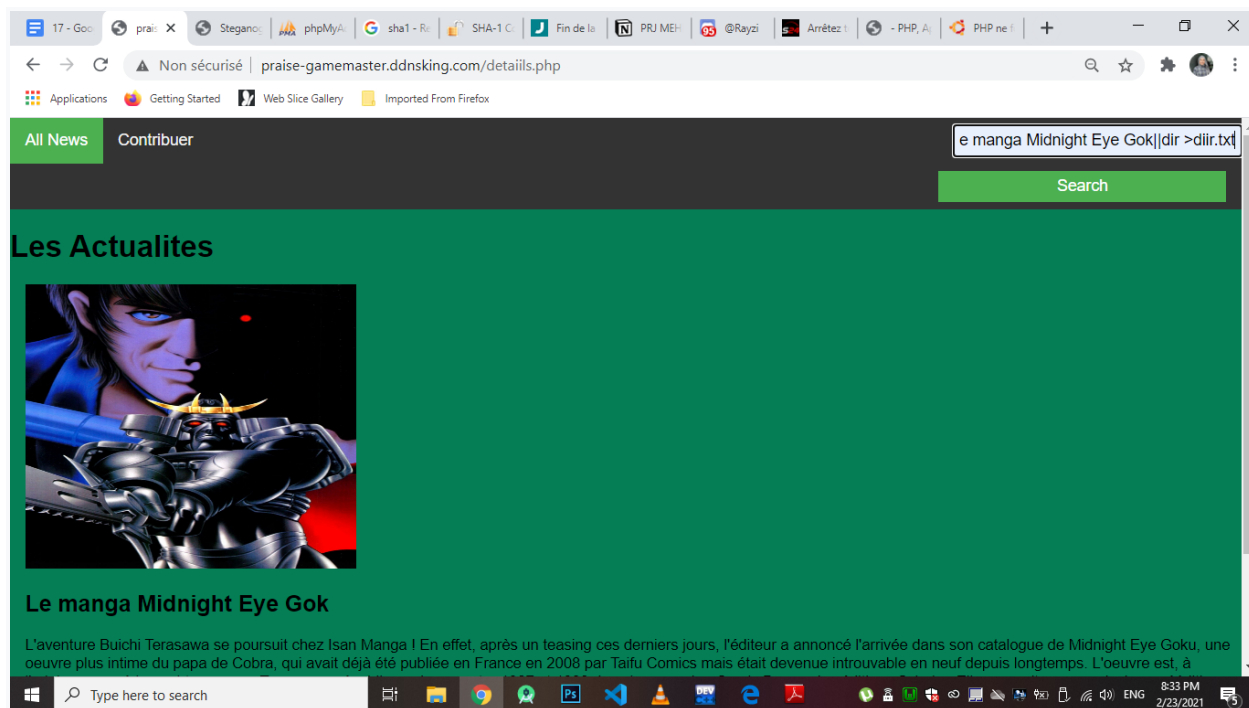
L'aventure Buichi Terasawa se poursuit chez Isan Manga ! En effet, après un teasing ces derniers jours, l'éditeur a annoncé l'arrivée dans son catalogue de Midnight Eye Goku, une oeuvre plus intime du papa de Cobra, qui avait déjà été publiée en France en 2008 par Taifu Comics mais était devenue introuvable en neuf depuis longtemps. L'oeuvre est, à l'origine, une série en 4 tomes que Terasawa prépublia au Japon entre 1987 et 1989 dans le magazine Comic Burger des éditions Scholier. Elle a ensuite connu plusieurs rééditions dans son pays, essentiellement chez Media Factory. Une adaptation animée en 2 OAV a également vu le jour en 1989. L'édition d'Isan Manga comptera 3 volumes et rejoindra le label Fuji Manga. Au programme, un récit plus sombre et moins fantasque que Cobra, qui explore la dystopie cyberpunk, et dont le premier volume paraîtra en octobre. De plus amples informations sur l'édition arriveront prochainement.



Nom de l'image	PID	Nom de la session	Num, ro de s	Utilisation
System Idle Process	0	Services	0	4 Ko
System	4	Services	0	276 Ko
smss.exe	264	Services	0	11012 Ko
csrss.exe	356	Services	0	41172 Ko
csrss.exe	420	Console	1	181064 Ko
wininit.exe	428	Services	0	31600 Ko
winlogon.exe	456	Console	1	51980 Ko
services.exe	516	Services	0	61328 Ko
lsass.exe	524	Services	0	101068 Ko
svchost.exe	588	Services	0	91208 Ko
svchost.exe	632	Services	0	61260 Ko
dwm.exe	716	Console	1	591532 Ko
VBoxService.exe	728	Services	0	61292 Ko
svchost.exe	816	Services	0	151608 Ko
svchost.exe	852	Services	0	261520 Ko
svchost.exe	920	Services	0	151872 Ko
svchost.exe	980	Services	0	171436 Ko
svchost.exe	560	Services	0	111460 Ko
spoolsv.exe	1032	Services	0	81844 Ko
svchost.exe	1072	Services	0	121860 Ko
wlms.exe	1100	Services	0	21608 Ko
svchost.exe	1504	Services	0	41448 Ko
taskhost.exe	1872	Console	1	91084 Ko

Et voilà le résultat de tous les processus en cours avec leur PID.

## 2- Le manga Midnight Eye Gok||dir >diir.txt



On affiche le fichier ou on a redirectionné le résultat :



L'attaquant pourra ensuite consulter le fichier contrib et retrouver le nom de son fichier déjà uploadé qui peut aussi être utilisé comme backdoor.

### Recommandations :

Pour se protéger contre les injections de commande et de code il faut, encore une fois, vérifier toutes les saisies de l'utilisateur afin qu'il ne puisse pas saisir de commande ou de code, d'une autre façon tous les arguments de commande doivent être échappés à l'aide de **escapeshellarg ()** ou **escapeshellcmd ()**. Cela rend les arguments non exécutables. Pour chaque paramètre, la valeur d'entrée doit également être validée.

## IV. Local File Inclusion :

Criticité : haute.

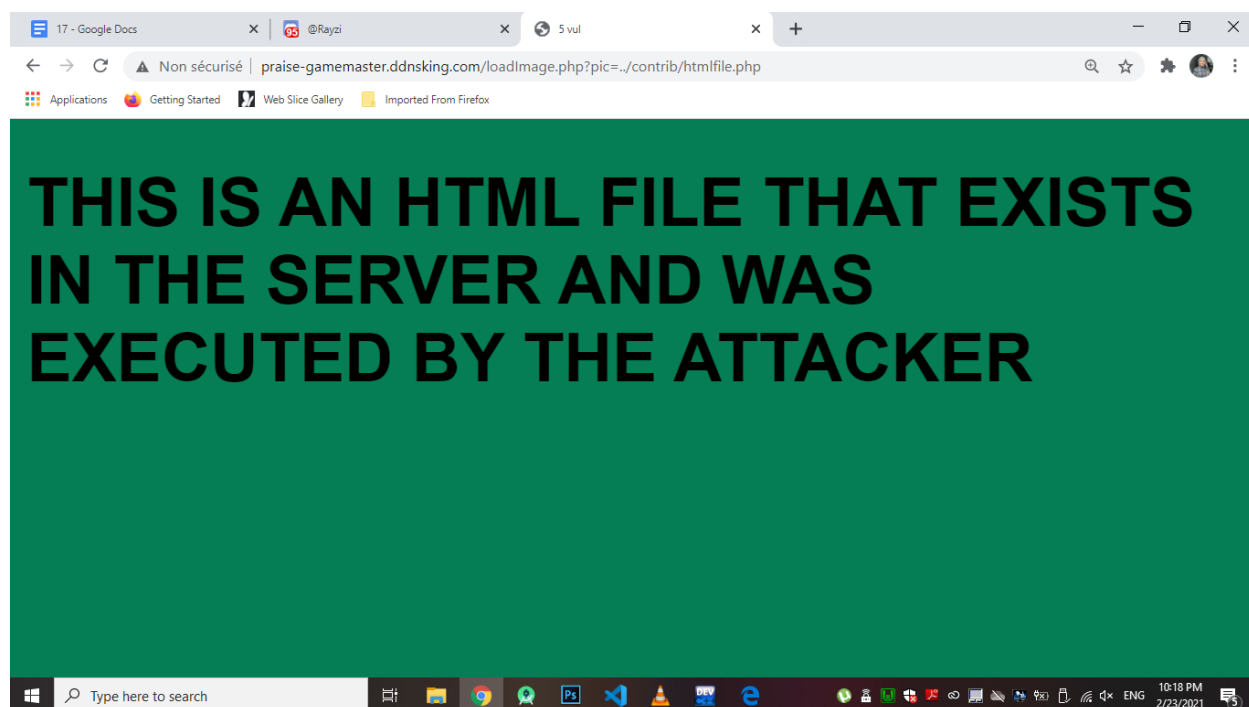
Exploitation : moyenne.

Correction : moyenne.

La vulnérabilité est le fait qu'une personne malveillante peut inclure le contenu d'un fichier local (qui se trouve dans le serveur hébergeant le site) dans une page du site. Elle permet d'afficher le contenu de certains fichiers critiques.

### Exploitation :

Dans la page **"NasaSsiiNews.php" (special admin)** en ouvrant l'image de n'importe quelle catégorie de News dans un nouvel onglet, et en remplaçant la valeur du champ **"pic"** par **le chemin du fichier** qu'on veut inclure. Dans cet exemple, il incite l'application à exécuter un script PHP **"htmlfile.php"** tel qu'un web shell que l'attaquant a réussi à télécharger sur le serveur Web.



### Recommandations :

Pour y remédier on peut : sauvegarder les chemins de fichiers dans une base de données et les indexer avec un ID unique, mettre les chemins fichiers qu'on veut afficher dans une liste blanche et ignorer tout chemin anormal.

## V. Directory Traversal :

Criticité : moyenne.

Exploitation : moyenne.

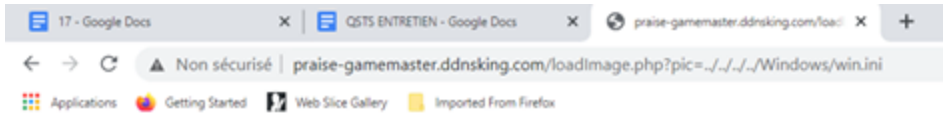
Correction : moyenne.

Combiné au LFI, cette vulnérabilité permet à un attaquant d'accéder à des fichiers qui se trouvent en dehors du fichier racine (www) du site web.

### Exploitation

L'exploitation de cette vulnérabilité a été vue dans des exploitations précédentes. Par exemple, lors de l'exploitation de la vulnérabilité Local File Inclusion, le fichier inclut été le **"C:\Windows\win.ini"** qui ne se trouve pas à l'intérieur de la racine du site web.

1- La on est simplement en train d'afficher l'image d'une catégorie mais si on change le paramètre pic( cela veut dire change le chemin vers **../..../Windows/win.ini**) on pourra afficher le fichier win.ini par exemple comme illustre la 2eme figure :



## Recommendations :

Il est recommandé de configurer apache pour qu'il n'accède pas au-delà du répertoire racine `www`. Ceci peut être fait en ajoutant un fichier **.htaccess** à la racine du répertoire et de le configurer.



## Conclusion :

Pour finir , les étapes à suivre et l'enchaînement des vulnérabilités se présente ainsi : - l'utilisateur accédera en premier à la page d'accueil ou il devras repérer le bouton login invisible ( grâce à l'outil d'inspection d'élément ), une fenêtre d'authentification demandera un mot de passe , pour récupérer ce mot de passe l'attaquant devra aller à la page "Réalisée par" pour exploiter la vulnérabilité de type SQL Injection contenu dans l'URL , le mot de passe chiffré sera déchiffrer en recueillant le type de chiffrement caché à l'aide d'un outil de stéganographie en ligne dans l'image correspondante à l'article stéganographie, après s'avoir authentifier une nouvelle page administrateur offre plus de fonctionnalités or plus de vulnérabilités, l'une d'elles est l'upload de fichiers arbitraires ( en cliquant sur Contribuer qui est une fonctionnalité permettant l'admin d'ajouter d'autre articles ) et puis combiner la précédente pour localiser et exécuter ce fichier grâce à l'OS command injection qui se cache dans un Textfield "Search" lui donnant un contrôle totale envers la machine. Les autres vulnérabilités LFI et Directory Traversal se trouvent si l'attaquant ouvre l'une des images dans un nouvel onglet et modifie le chemin d'accès de l'image situé dans l'url pour afficher d'autre fichier en dehors du dossier racine du site web.