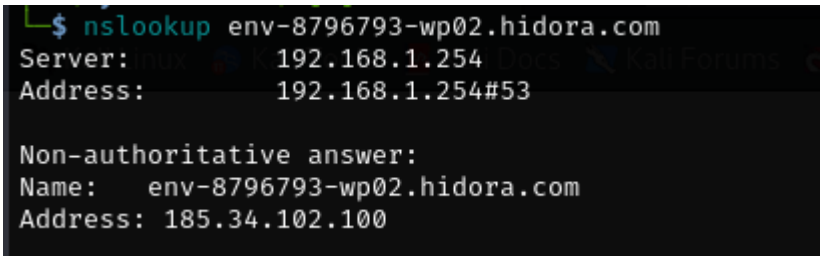
Analyse du site wordpress env-8796793-wp02.hidora.com

Test effectué sans accès SSH

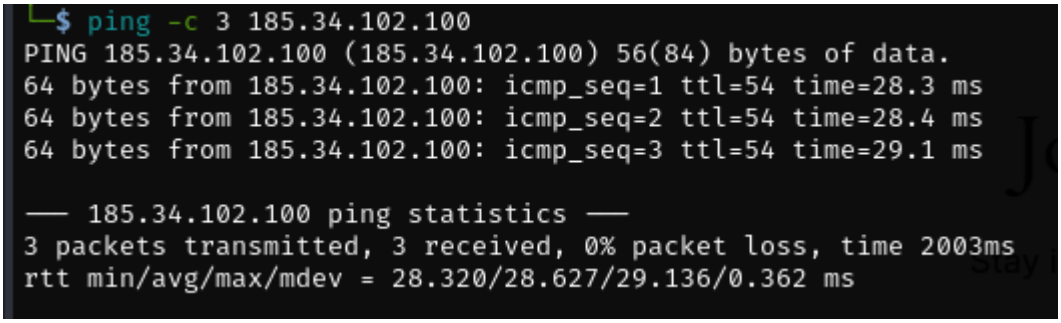
Identification de l'IP du site avec nslookup

Recherche DNS pour obtenir des informations sur un l'adresse IP.

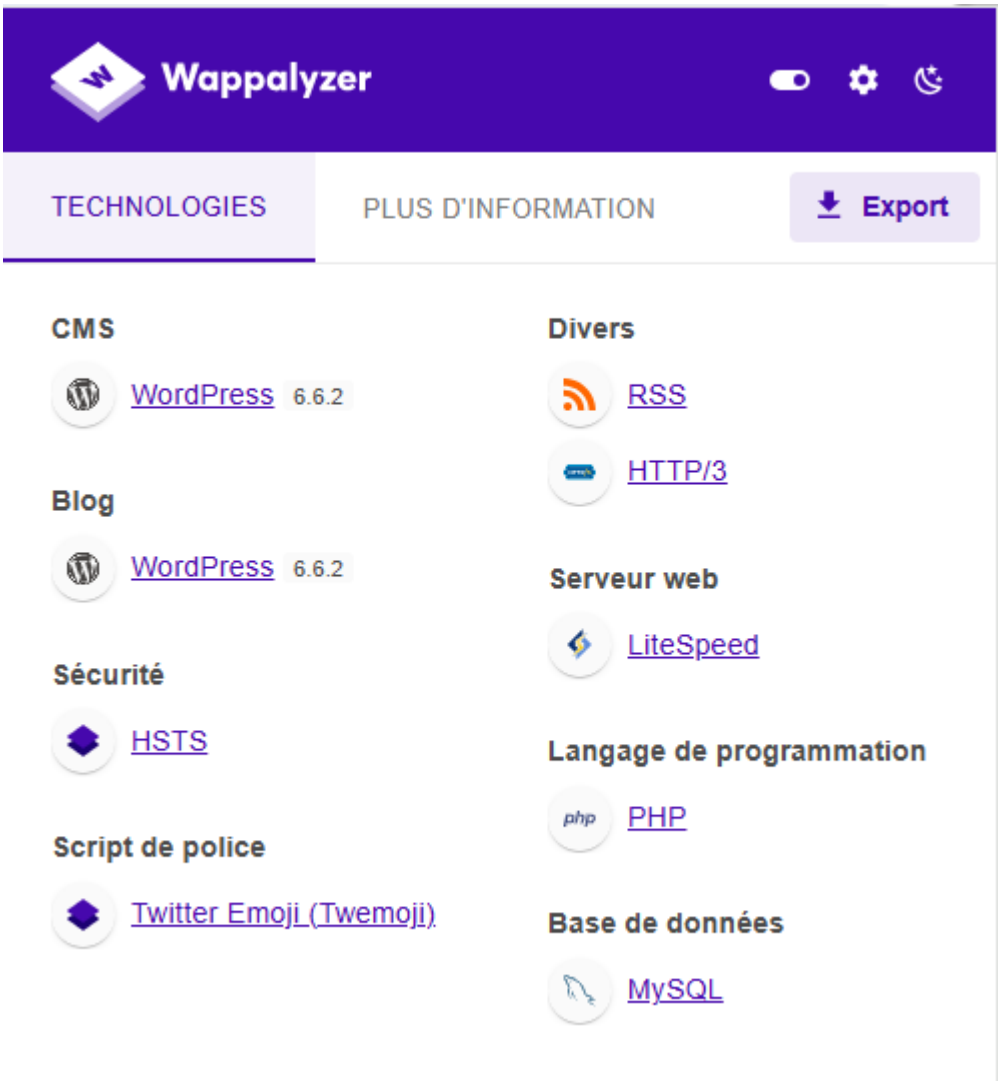
```
nslookup env-8796793-wp02.hidora.com
```



Test de la connectivité avec ping



1. Résumé des Technologies du Site:



- CMS : WordPress 6.6.2.
- Serveur Web : LiteSpeed.

LiteSpeed est un serveur web performant connu pour sa rapidité, sa gestion efficace des connexions simultanées, et ses optimisations pour les sites WordPress.

- Base de données : MySQL.
- Langage de programmation : PHP.

Sécurité et Performances

- Sécurité : Le site utilise HTTP Strict Transport Security (HSTS).

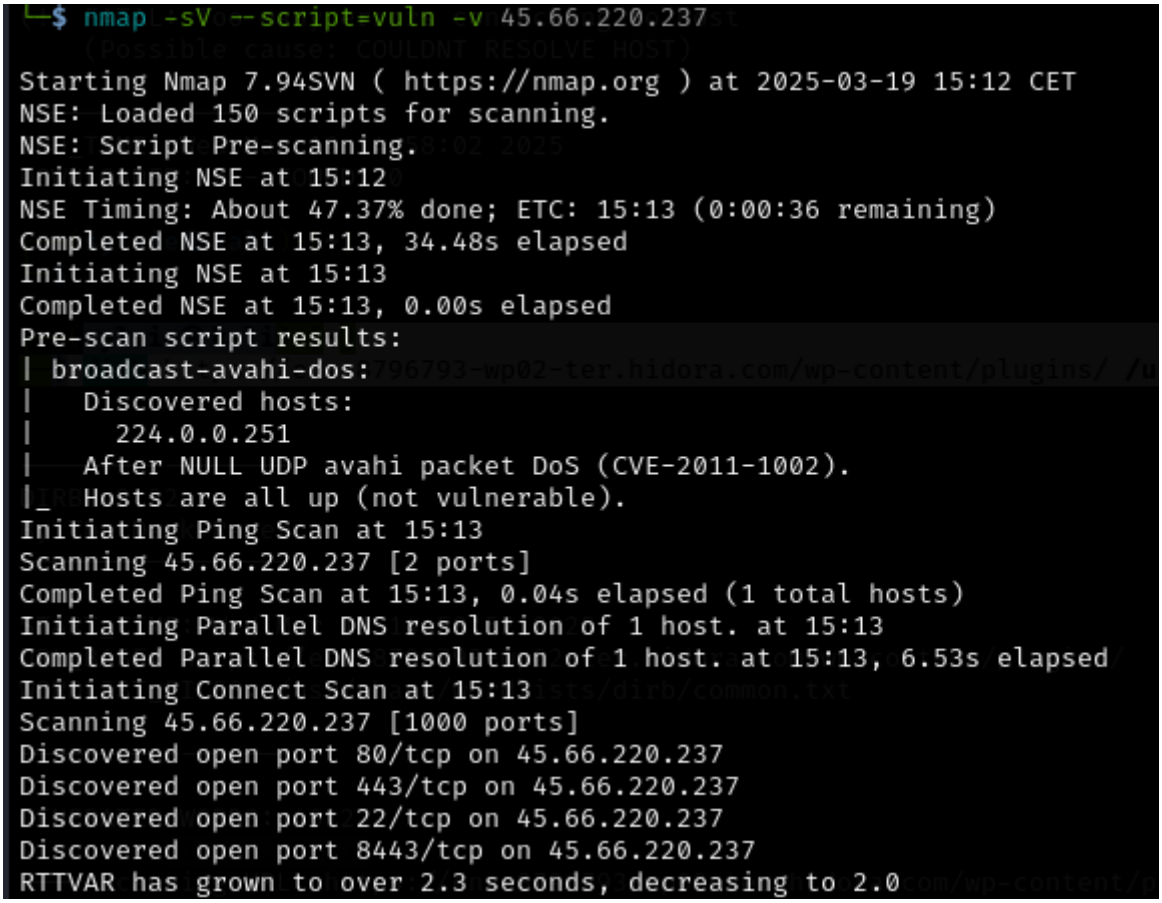
Les navigateurs qui accèdent à ce site seront contraints d'utiliser des connexions HTTPS sécurisées, empêchant ainsi toute connexion non sécurisée (HTTP).

- Réseau : HTTP/3 est activé, ce qui améliore la performance de la connexion.

Le site utilise également des emojis Twitter via l'intégration de Temodji.

Analyse de la Sécurité Réseau et des Services du Serveur

```
nmap -sV --script=vuln -v 45.66.220.237
```



1. Ports et Services Découverts

- Port 443/tcp (SSL/HTTPS)

Le serveur utilise HTTPS sur le port 443 avec LiteSpeed comme serveur web.

Recommandation: Vérifier la configuration SSL/TLS pour s'assurer que seules les versions modernes et sécurisées (TLS 1.2 ou 1.3) sont activées. Désactiver les versions obsolètes .

- Port 80/tcp (HTTP)

Le port 80 est ouvert, permettant des connexions HTTP non sécurisées. Cependant, le site utilise HTTP Strict Transport Security (HSTS), ce qui force les navigateurs à établir des connexions uniquement via HTTPS sécurisées, empêchant ainsi toute communication non sécurisée.

- Port 22/tcp (SSH)

Le port 22 est ouvert et utilisé pour le service OpenSSH.

Tester les Services d'Authentification SSH à Distance :

```
nmap --script ssh-auth-methods -p 22 45.66.220.237
```

```
└─$ nmap --script ssh-auth-methods -p 22 45.66.220.237
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 17:13 CET
Nmap scan report for 45.66.220.237
Host is up (0.028s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|     gssapi-keyex
|_    gssapi-with-mic

Nmap done: 1 IP address (1 host up) scanned in 7.40 seconds
```

l'accès SSH ne peut pas être effectué par mot de passe, mais uniquement par clé publique ou authentification GSSAPI.

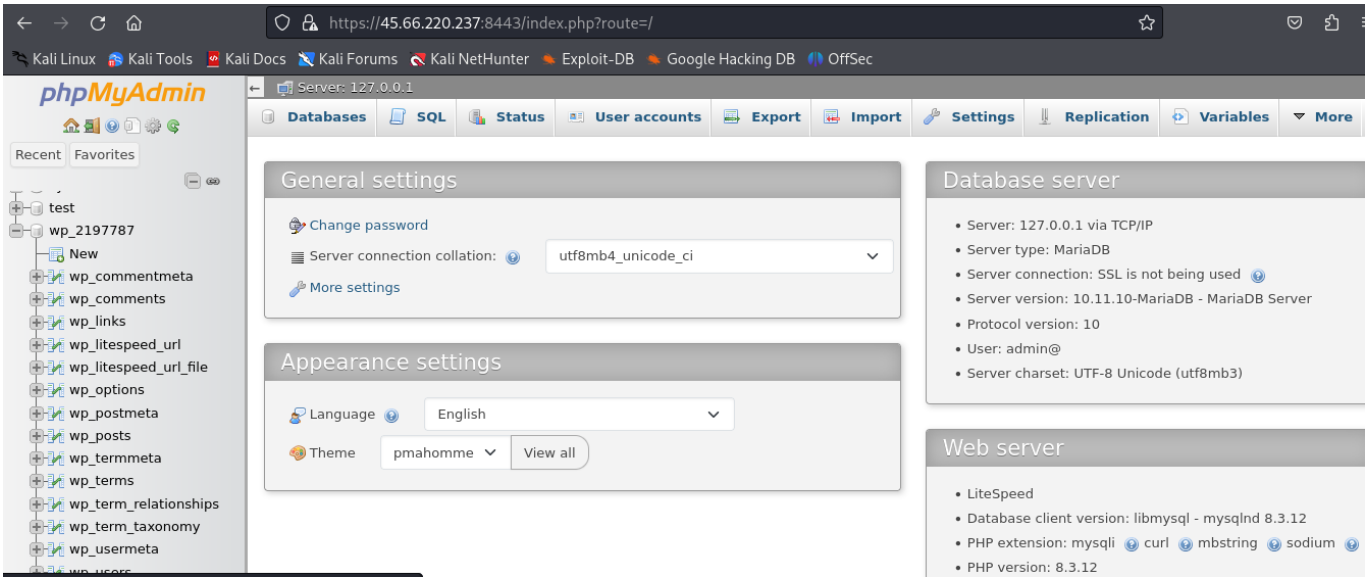
- Port 8443/tcp (HTTPS alternatif)

Le port 8443 est ouvert, généralement utilisé pour des interfaces d'administration ou des outils de gestion.

- tentative de connexion:

```
https://45.66.220.237:8443
```

identifiant: admin mot de passe: admin



Modification des identifiants par défaut

Problème identifié: L'interface d'administration est accessible avec un identifiant et un mot de passe par défaut ("admin/admin").

Recommandation: Modifier les identifiants par défaut. Utiliser des noms d’utilisateur uniques et des mots de passe forts. Les mots de passe doivent comporter au moins 12 caractères, inclure des lettres majuscules, des lettres minuscules, des chiffres et des symboles spéciaux.

Désactivation de l'accès public à l'interface d'administration

- Problème identifié: L’interface d’administration est accessible publiquement via le port 8443.

- Recommandation: Restreindre l’accès à cette interface. Utiliser un VPN ou un pare-feu pour limiter l’accès aux adresses IP internes ou de confiance. **Bloquer l'accès public pour le port 8443**

```
https://45.66.220.237:8443
```

Création de la chaîne input dans la table ip

```
sudo nft add chain ip filter input { type filter hook input priority 0 \; }
```

Ajout de la règle pour bloquer le port 8443

```
sudo nft add rule ip filter input tcp dport 8443 drop
```

Activation de l’authentification à double facteurs (2FA)

L'interface d'administration ne utilise pas l'authentification à double facteurs (2FA). Il est recommandé d'activer le 2FA pour toutes les connexions administratives, ajoutant une couche de sécurité supplémentaire avec une validation secondaire (code SMS, application d'authentification, etc.). Cela protège contre les attaques par force brute, même en cas de mot de passe compromis

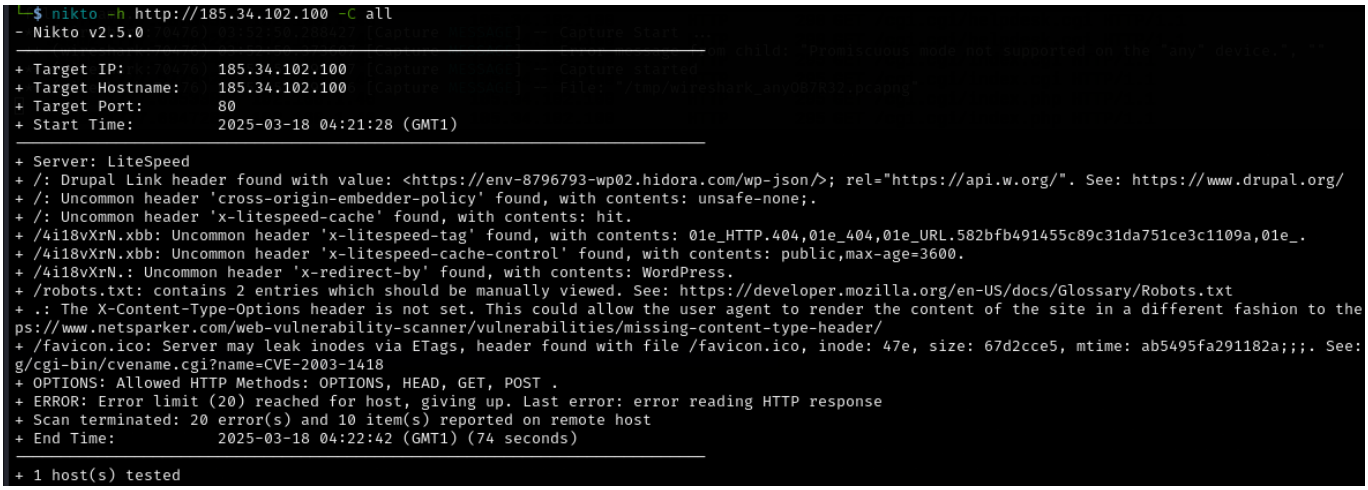
- Port 21/tcp (FTP)

Le port FTP (21) est fermé, ce qui est positif si aucun service FTP n'est nécessaire.

Recherche des vunérabilités

- Détecter des vulnérabilités courantes avec Nikto

```
nikto -h http://45.66.221.1 -C all
```



Drupal Link Header Le scan a détecté un en-tête Drupal dans la réponse HTTP alors que le site semble être un site WordPress. Cela peut être dû à des traces laissées par un autre CMS (Drupal) ou à des fichiers associés qui devraient être supprimés pour éviter toute fuite d'information.

En-têtes HTTP peu communs

- cross-origin-embedder-policy: Si mal configuré, cela peut permettre des attaques CORS. Il est recommandé de restreindre cette politique.

- x-litespeed-cache, x-litespeed-tag et x-litespeed-cache-control: Ces en-têtes sont associés au cache LiteSpeed. Une mauvaise configuration peut entraîner des fuites d'information ou des problèmes de mise en cache.

-x-redirect-by: Indique l'utilisation de WordPress pour la redirection.

Fichier robots.txt Le fichier robots.txt peut contenir des informations sensibles ou des ressources inutiles accessibles aux moteurs de recherche.

Manque d'en-tête X-Content-Type-Options L'absence de cet en-tête expose le site à des attaques MIME Sniffing. Il est recommandé de l'ajouter avec la valeur nosniff pour renforcer la sécurité.

Fichier favicon.ico et problème d'inodes Les ETags exposent potentiellement des informations sensibles, comme les inodes des fichiers. Cela doit être configuré pour éviter des fuites d'informations.

Méthodes HTTP autorisées La méthode OPTIONS est autorisée, ce qui permet de découvrir les capacités du serveur. Il est recommandé de limiter les méthodes HTTP au strict nécessaire.

Erreur de lecture HTTP Des erreurs HTTP ont été rencontrées lors du scan, probablement dues à une configuration du serveur ou des protections en place.

Vérifier les en-têtes HTTP renvoyés par le serveur

Obtenir des informations sur le serveur sans télécharger le contenu.

```
wget --server-response --spider http://185.34.102.100
```

```
└─$ wget --server-response --spider http://185.34.102.100
Spider mode enabled. Check if remote file exists.
--2025-03-18 04:27:43--  http://185.34.102.100/
Connecting to 185.34.102.100:80 ... connected.
HTTP request sent, awaiting response ...
  HTTP/1.1 200 OK
  Connection: Keep-Alive
  Keep-Alive: timeout=5, max=100
  content-type: text/html; charset=UTF-8
  link: <https://env-8796793-wp02.hidora.com/wp-json/>; rel="https://api.w.org/"
  etag: "7-1742297182;;;"
  x-litespeed-cache: hit
  date: Tue, 18 Mar 2025 11:32:37 GMT
  server: LiteSpeed
  cross-origin-embedder-policy: unsafe-none;
  cross-origin-opener-policy: same-origin-allow-popups;
  cross-origin-resource-policy: same-origin;
  permissions-policy: geolocation=(self), payment=(self)
  referrer-policy: strict-origin-when-cross-origin
  x-content-type-options: nosniff
  x-frame-options: SAMEORIGIN
  x-permitted-cross-domain-policies: none;
  x-xss-protection: 1; mode=block;
  strict-transport-security: max-age=5; includeSubDomains
Length: unspecified [text/html]
Remote file exists and could contain further links,
but recursion is disabled -- not retrieving.
```

Réponse HTTP valide (200 OK): Le serveur répond correctement à la requête, confirmant que le site est accessible.

En-têtes de sécurité présents:

- X-Frame-Options : Protège contre les attaques de type clickjacking avec la valeur SAMEORIGIN.
- X-Content-Type-Options : Empêche le navigateur de deviner des types MIME incorrects.
- Strict-Transport-Security (HSTS) : Bien qu'il soit activé, l'en-tête a une durée courte (max-age=5), ce qui peut permettre des connexions HTTP non sécurisées.

Exposition de l'API REST de WordPress:

Un lien vers l'API wp-json est exposé, ce qui peut constituer une vulnérabilité si l'API n'est pas sécurisée.

Vulnérabilités et recommandations:

- Améliorer la configuration de HSTS: Actuellement, max-age=5 est trop court. Il est recommandé de définir max-age=1 an et d'ajouter includeSubDomains pour couvrir tous les sous-domaines.
- Sécurisation de l'API WordPress: L'API wp-json doit être protégée via des mécanismes comme OAuth ou des clés API pour restreindre l'accès aux utilisateurs non autorisés.
- Gestion du cache: S'assurer que aucune donnée sensible n'est stockée dans le cache public afin de prévenir des fuites d'informations sensibles.

Audit de Sécurité avec WPScan

- Installer WPScan

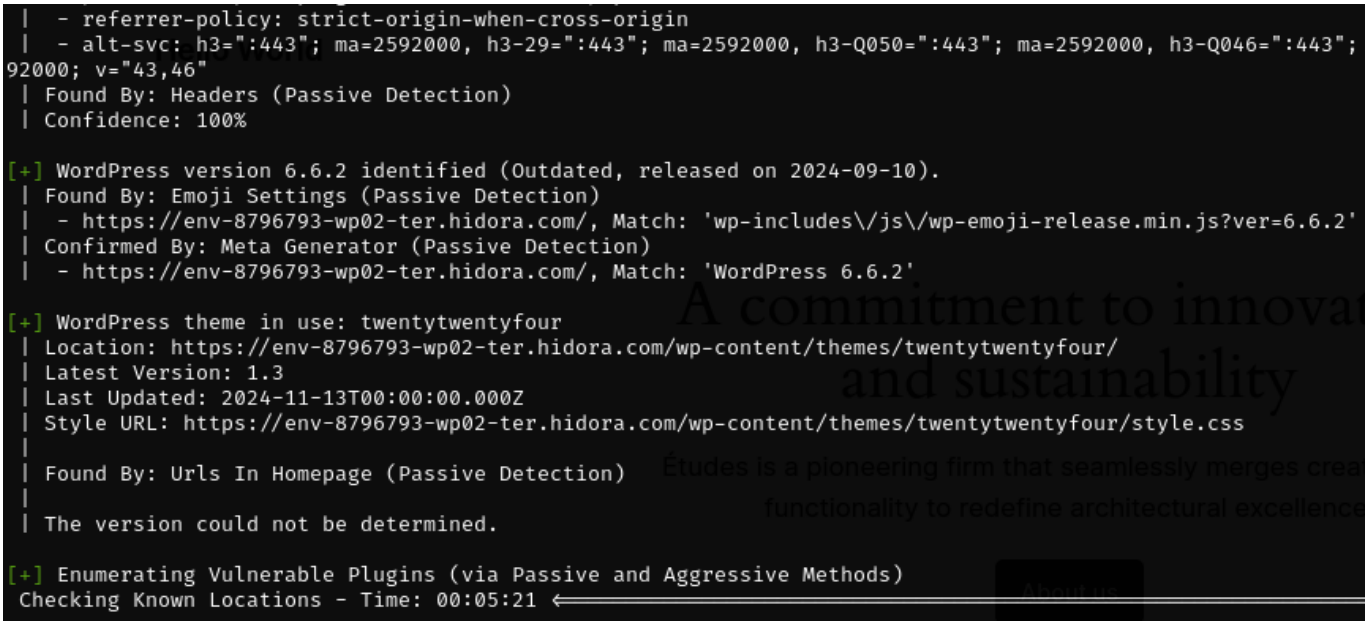
```
sudo apt update
sudo apt install wpscan
```

Lancer un scan basique

```
wpscan --url https://env-9206928-wp02-nosecure.hidora.com/
```

Scan de sécurité sur un site WordPress pour identifiant les plugins installés et vérifier leur sécurité.

```
wpscan --url https://env-8796793-wp02-ter.hidora.com/ -e vp --plugins-detection
mixed --api-token ta_token
```



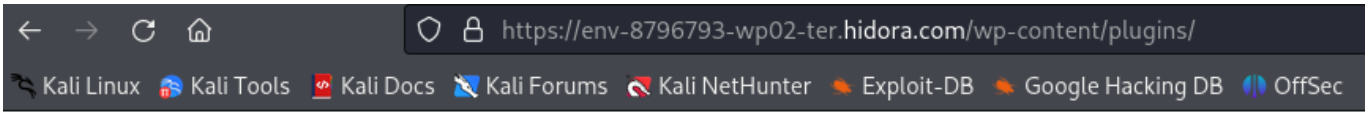
Version de WordPress détectée: 6.6.2 **Problème:** Cette version est obsolète. Il est fortement recommandé de mettre à jour WordPress vers la version la plus récente pour bénéficier des derniers correctifs de sécurité.

Thème utilisé: twentytwentyfour Vérifier si le thème est à jour

** Problèmes de sécurité détectés:** Aucun plugin vulnérable n'a été détecté lors de l'audit, ce qui est un bon signe en termes de sécurité.

Recommandations

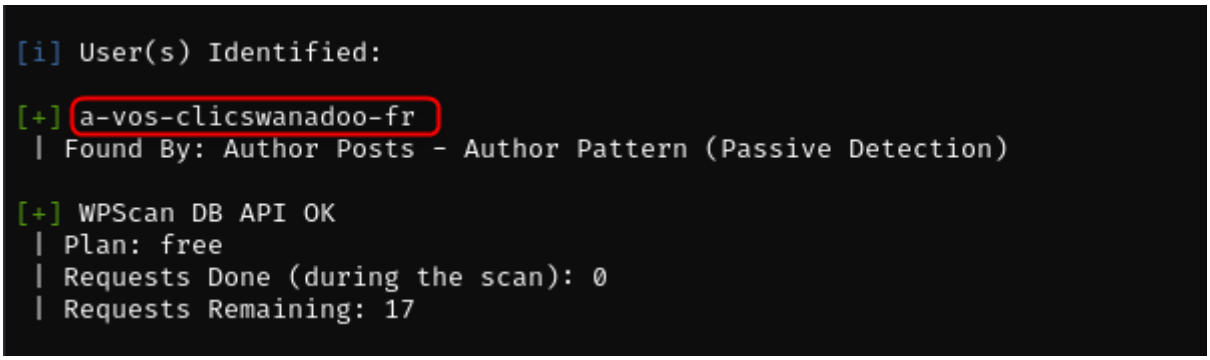
- Mettre à jour WordPress : La version 6.6.2 de WordPress est obsolète et doit être mise à jour pour profiter des derniers patchs de sécurité.
- Vérifier le thème WordPress : Bien que le thème twentytwentyfour semble être à jour avec la version 1.3, il est important de vérifier si la version installée est bien la dernière et si elle ne présente pas de vulnérabilités.



Scanner les utilisateurs:

```
wpscan --url https://ton-site.com --enumerate u
```

```
wpscan --url https://env-8796793-wp02-ter.hidora.com/ --enumerate u --api-token
your_api_token
```



Utilisateur identifié:** a-vos-clicswanadoo-fr

test de brute force sur un site WordPress.

```
wpscan --url https://env-8796793-wp02-ter.hidora.com/ --passwords
/usr/share/wordlists/rockyou.txt --usernames a-vos-clicswanadoo-fr
```

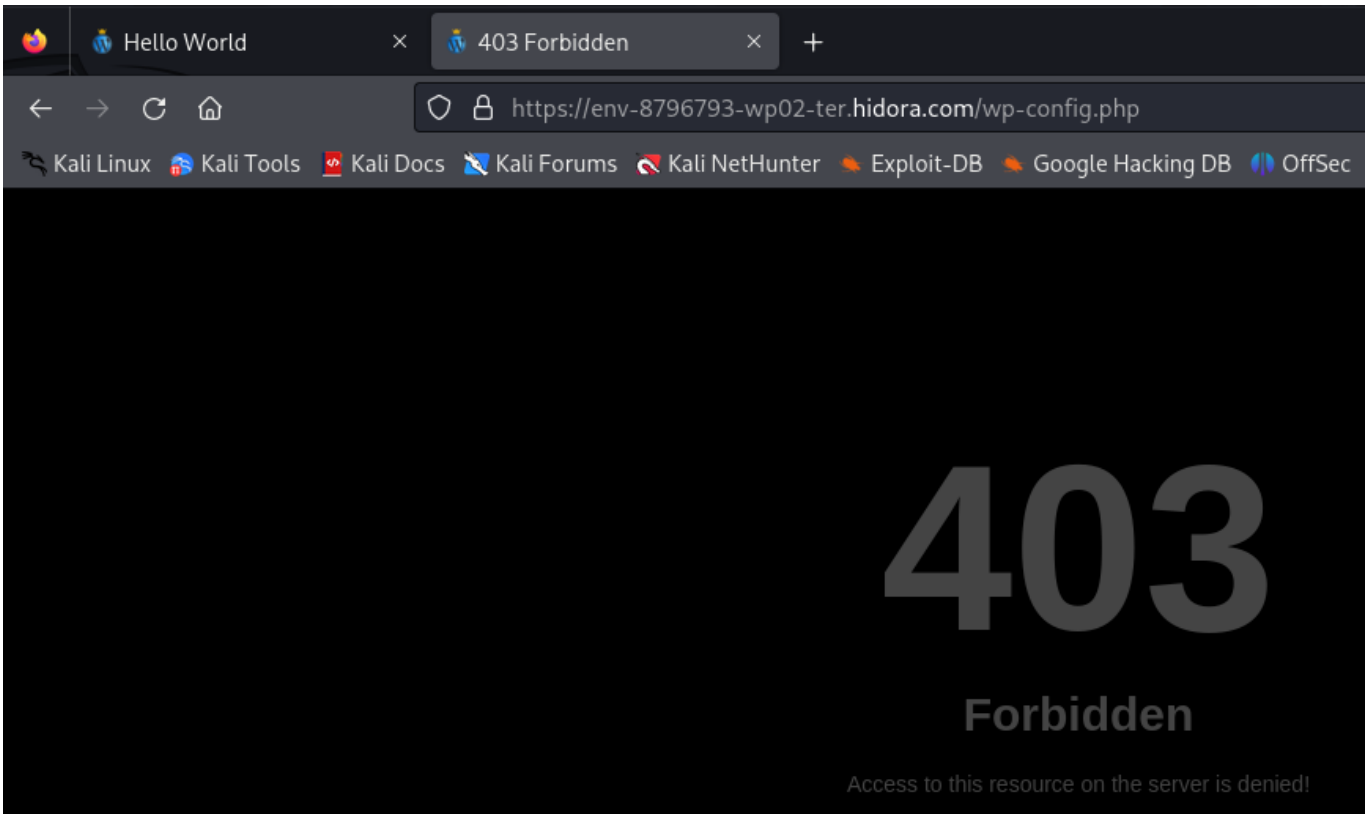
Aucun mot de passe valide n'a été trouvé pour l'utilisateur a-vos-clicswanadoo-fr parmi les mots de passe populaires de la liste rockyou.txt.

1. Vérification des fichiers sensibles

Vérification manuelle

Accès au fichier wp-config.php

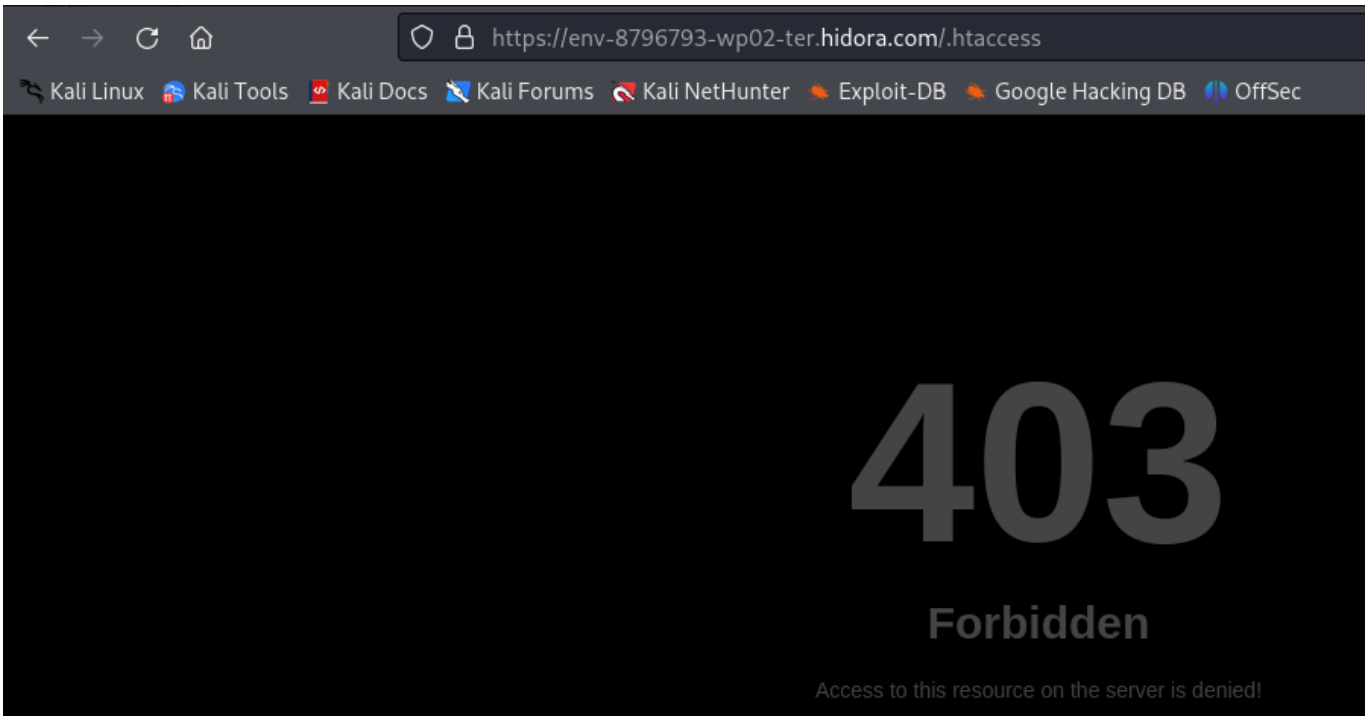
```
https://env-8796793-wp02-ter.hidora.com/wp-config.php
```



1. Le fichier wp-config.php est protégé L'accès au fichier wp-config.php est correctement protégé contre les accès non autorisés, Cela permet de réduire les risques d'exposition de données sensibles, comme les identifiants de la base de données et les clés secrètes.

Accès au fichier .htaccess

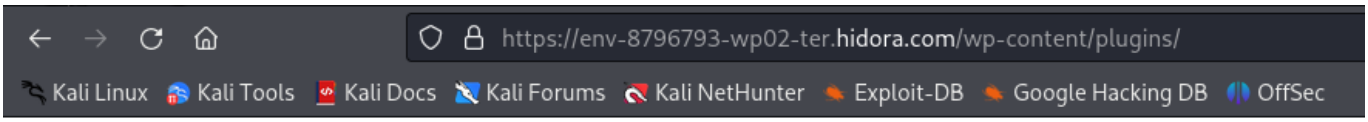
```
https://env-8796793-wp02-ter.hidora.com/.htaccess
```



L'accès au fichier .htaccess est correctement restreint contre les accès non autorisés, Cela réduit le risque d'attaques visant à modifier les paramètres de configuration du serveur et de compromission de la sécurité globale du site.

Accès au répertoire wp-content/plugins/

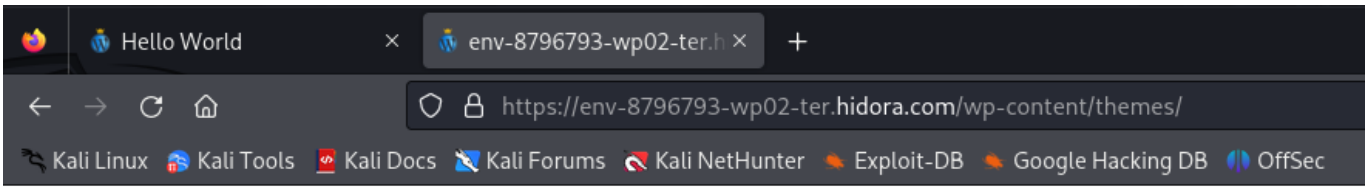
```
https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/
```



L'accès au répertoire wp-content/plugins/ est correctement protégé contre l'accès public, Cela réduit les risques liés à l'énumération des plugins et protège le site contre les attaques qui pourraient exploiter des plugins vulnérables.

Accès au répertoire /wp-content/themes/

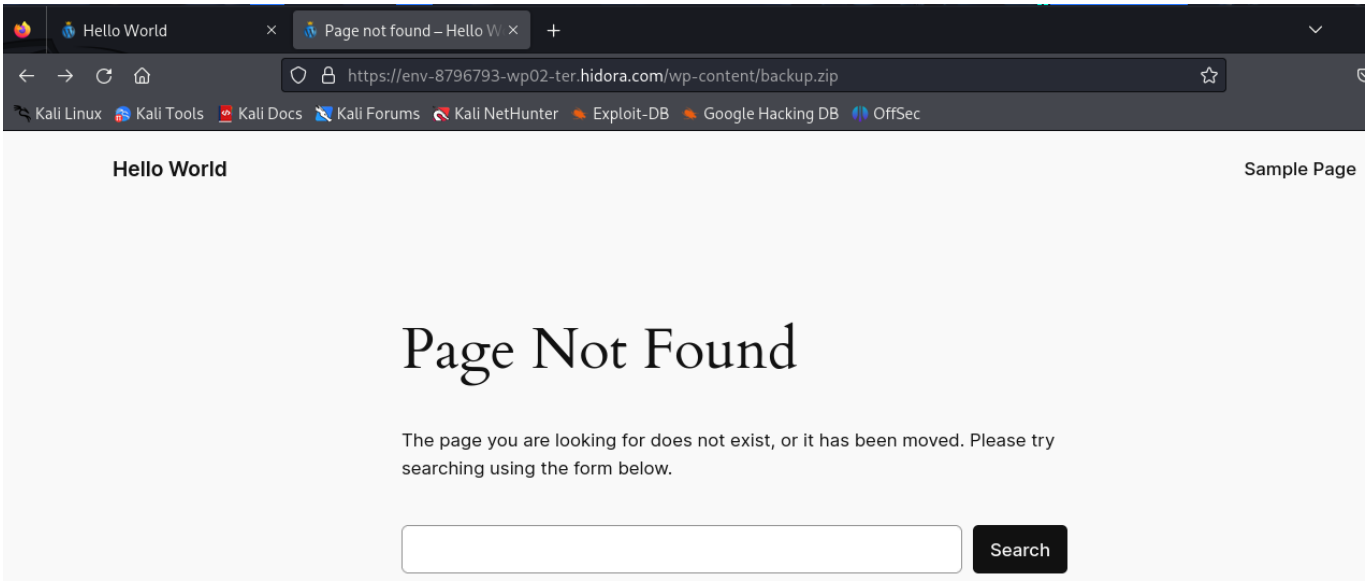
```
https://env-8796793-wp02-ter.hidora.com/wp-content/themes/
```



L'accès au répertoire wp-content/themes/ est bien protégé. Cela protège le site contre les attaques qui pourraient cibler des thèmes vulnérables et garantit que les informations sur les thèmes installés ne sont pas facilement accessibles aux attaquants.

Vérification des fichiers de sauvegarde (backup.zip)

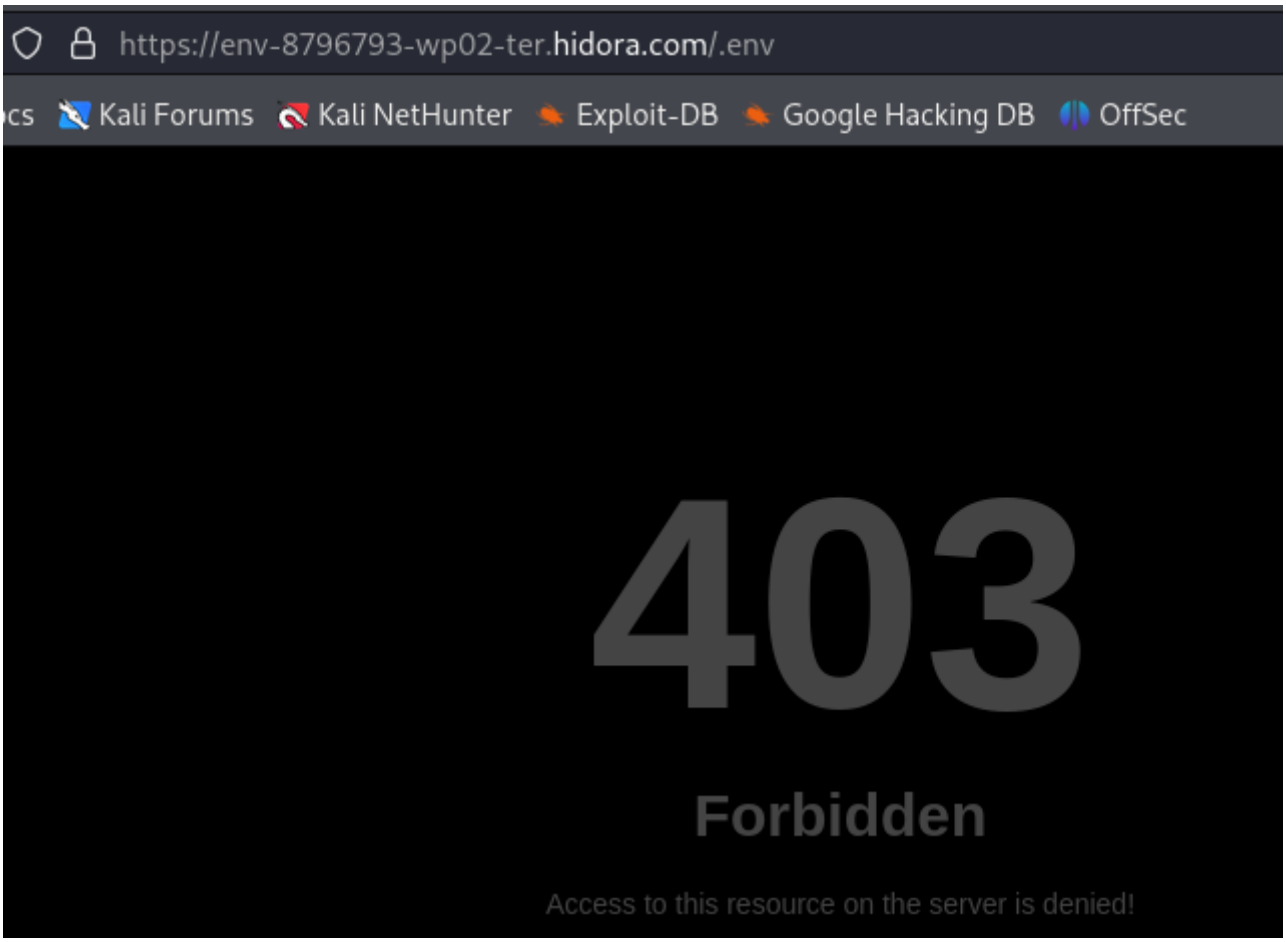
```
https://env-8796793-wp02-ter.hidora.com/wp-content/backup.zip
```



Le site applique une bonne pratique de sécurité en empêchant l'accès direct à des fichiers de sauvegarde tels que backup.zip. Cela réduit les risques d'attaques exploitant des fichiers de sauvegarde mal protégés.

.env

```
https://env-8796793-wp02-ter.hidora.com/.env
```

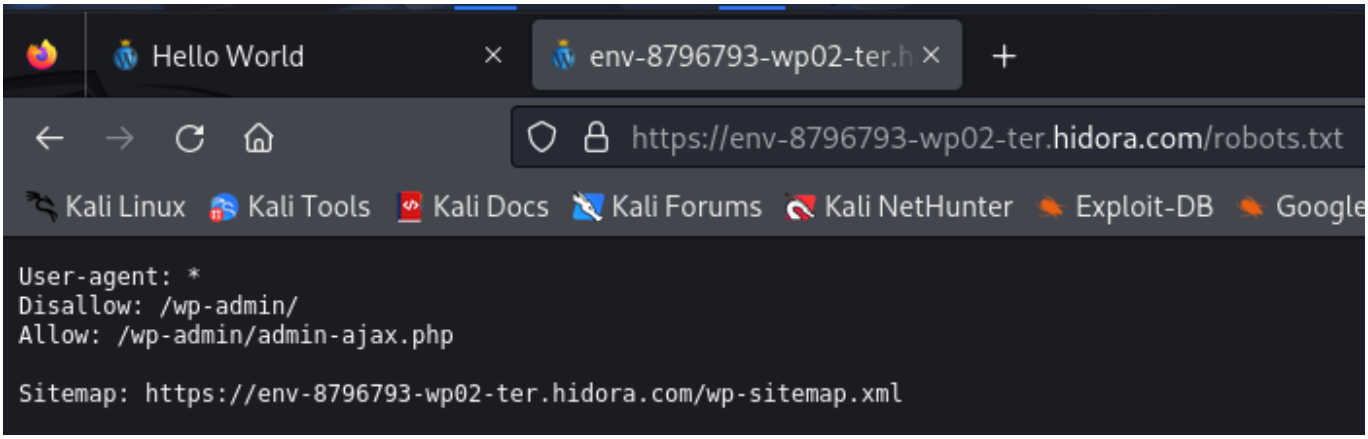


La réponse 403 Forbidden est un bon indicateur que des mesures de sécurité ont été correctement mises en place pour protéger le fichier .env. Ainsi le site est protéger conte des compromissions du site.

Analyser les fichiers robots.txt et sitemap.xml

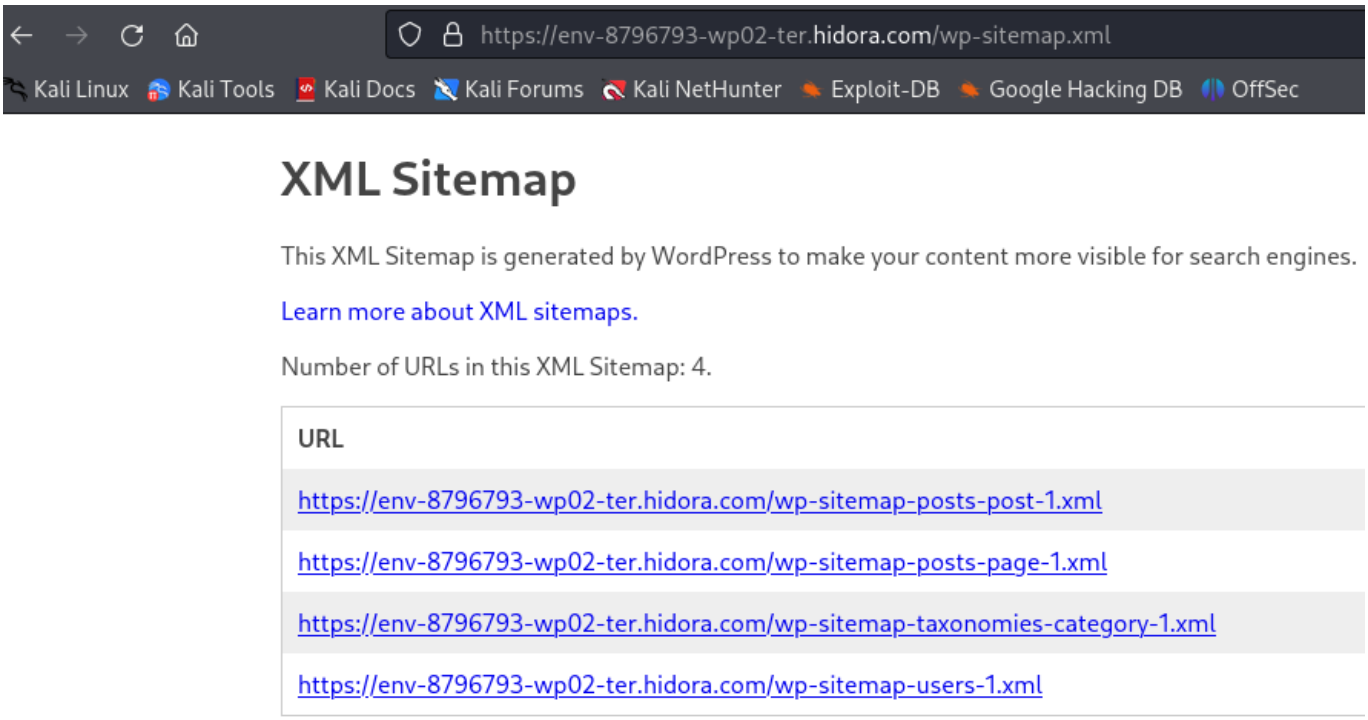
- fichier robots.txt

```
https://env-8796793-wp02-ter.hidora.com/robots.txt
```

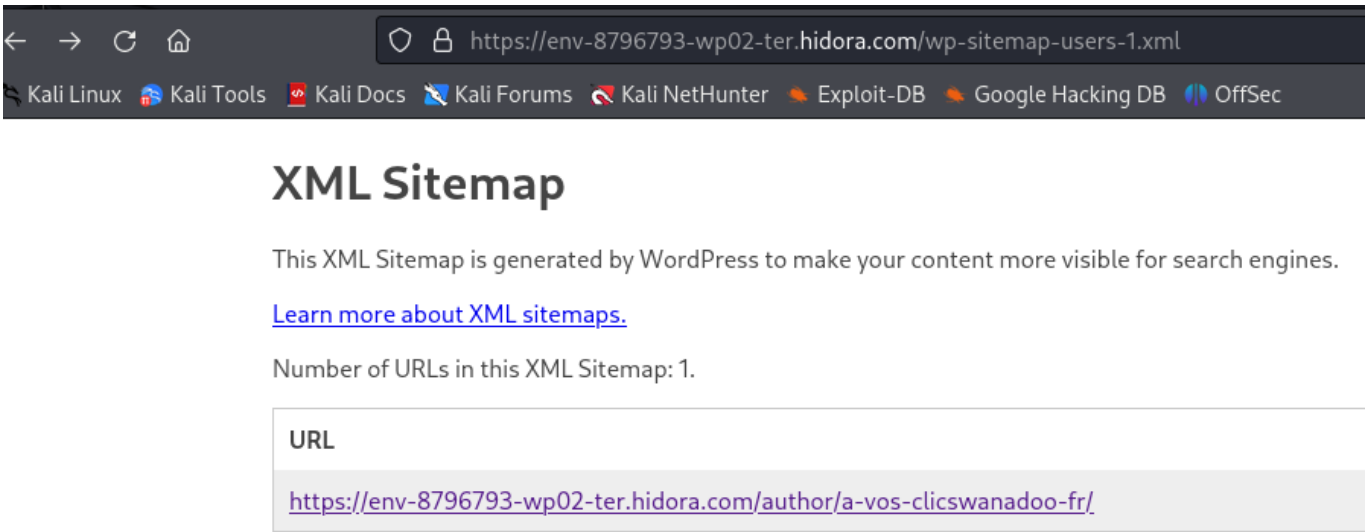


Le fichier robots.txt est bien configuré pour empêcher l'indexation du répertoire d'administration tout en permettant l'accès au fichier admin-ajax.php, De plus, l'inclusion du fichier sitemap.xml améliore l'indexation du site par les moteurs de recherche.

```
https://env-8796793-wp02-ter.hidora.com/wp-sitemap.xml
```



Le fichier wp-sitemap.xml semble bien structuré pour la visibilité sur les moteurs de recherche, mais il expose des informations sensibles, telles que les utilisateurs. Prendre des mesures pour sécuriser ces informations et examiner la possibilité de restreindre l'accès aux sitemaps ou d'y appliquer des filtres afin de protéger la vie privée des utilisateurs et la sécurité du site.



Analyser les vulnérabilités spécifiques aux plugins WordPress

Vérifier la structure des répertoires par un scan de repertoire:

```
dirb https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/
/usr/share/wordlists/dirb/common.txt
```

```
└─$ dirb https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/ /usr/share/wordlists/dirb/common.txt

DIRB v2.22
By The Dark Raver

START_TIME: Wed Mar 19 14:58:52 2025
URL_BASE: https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt

GENERATED WORDS: 4612

---- Scanning URL: https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/ ----
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/.config (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/_vti_bin/_vti_adm/admin.dll (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/_vti_bin/_vti_aut/author.dll (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/_vti_bin/shtml.dll (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/akeeba.backend.log (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/atom (CODE:301|SIZE:0)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/awstats.conf (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/development.log (CODE:403|SIZE:1242)
==> DIRECTORY: https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/global.asa (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/global.asax (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/index.php (CODE:200|SIZE:0)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/main.mdb (CODE:403|SIZE:1242)
```

```
---- Entering directory: https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/ ----
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/.config (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/_vti_bin/_vti_adm/admin.dll (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/_vti_bin/_vti_aut/author.dll (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/_vti_bin/shtml.dll (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/akeeba.backend.log (CODE:403|SIZE:1242)
==> DIRECTORY: https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/atom/
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/awstats.conf (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/development.log (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/feed (CODE:301|SIZE:0)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/global.asa (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/global.asax (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/index.php (CODE:301|SIZE:0)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/main.mdb (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/php.ini (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/production.log (CODE:403|SIZE:1242)
==> DIRECTORY: https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/rdf/
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/rss (CODE:301|SIZE:0)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/rss2 (CODE:301|SIZE:0)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/spamlog.log (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/thumbs.db (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/Thumbs.db (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/WS_FTP.LOG (CODE:403|SIZE:1242)
```

```
---- Entering directory: https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/atom/ ----
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/atom/.config (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/atom/_vti_bin/_vti_adm/admin.dll (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/atom/_vti_bin/_vti_aut/author.dll (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/atom/_vti_bin/shtml.dll (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/atom/akeeba.backend.log (CODE:403|SIZE:1242)
+ https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/feed/atom/awstats.conf (CODE:403|SIZE:1242)
(!) FATAL: Too many errors connecting to host
    (Possible cause: SSL CONNECT ERROR)

END_TIME: Wed Mar 19 15:17:37 2025
DOWNLOADED: 9943 - FOUND: 47
```

Fichiers sensibles détectés (HTTP 403):

Des fichiers sensibles comme des fichiers de configuration (php.ini), des logs (*.log) et des bases de données (*.mdb) sont présents mais protégés par des erreurs d'accès (403). Il est recommandé de restreindre l'accès à ces fichiers ou de les supprimer s'ils ne sont pas nécessaires.

Redirections HTTP et répertoires vides (HTTP 301):

Certains répertoires sont redirigés, ce qui peut indiquer une mauvaise configuration ou une exposition de ressources sensibles. Il faut analyser ces redirections pour s'assurer qu'elles ne compromettent pas la sécurité du site.

Structure des répertoires et fichiers sensibles:

Des répertoires comme /wp-content/plugins/feed/ contiennent des fichiers sensibles tels que des logs et des fichiers de configuration. Ces répertoires doivent être protégés pour éviter l'accès non autorisé.

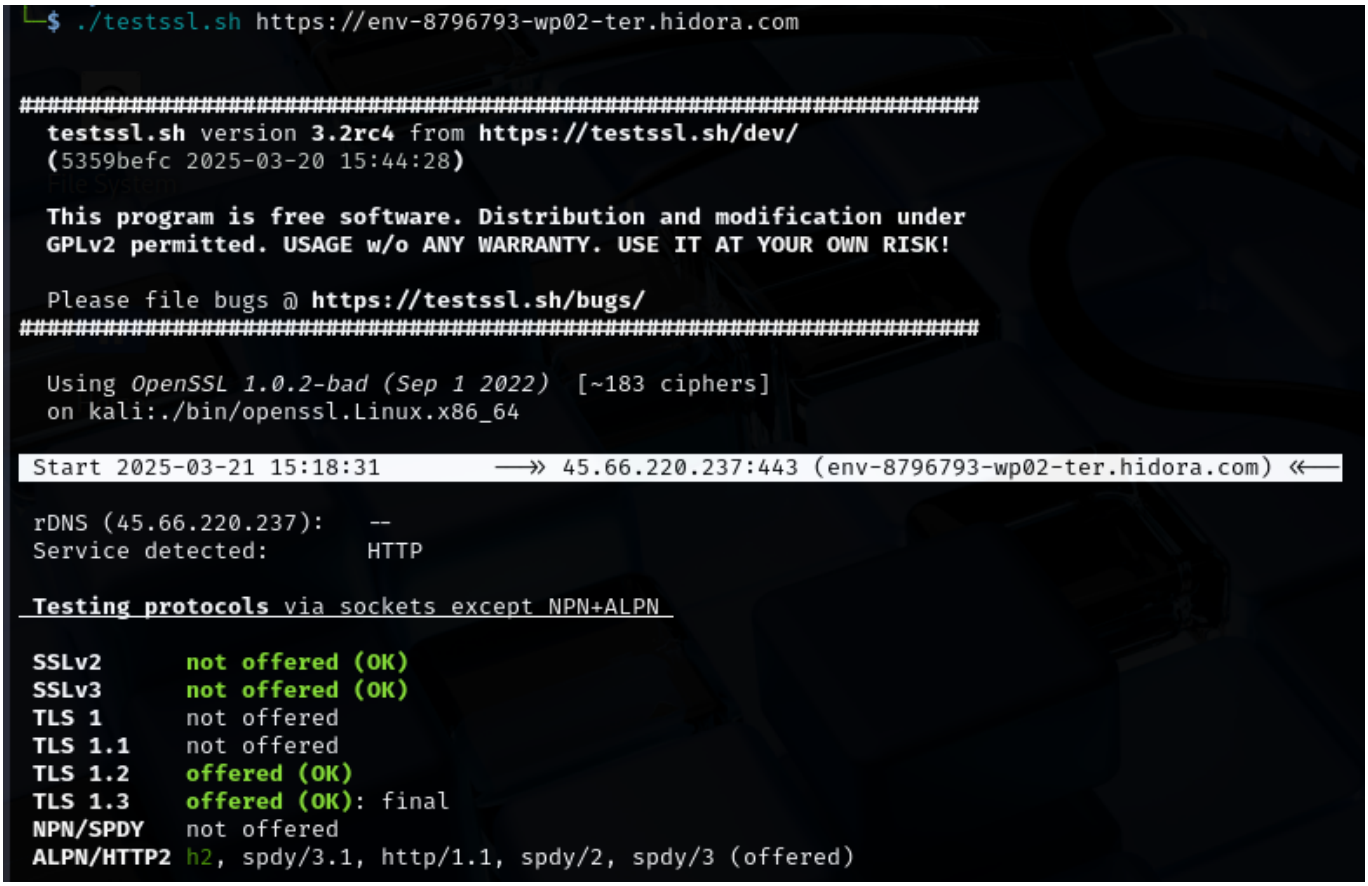
Vérification de la configuration SSL/TLS

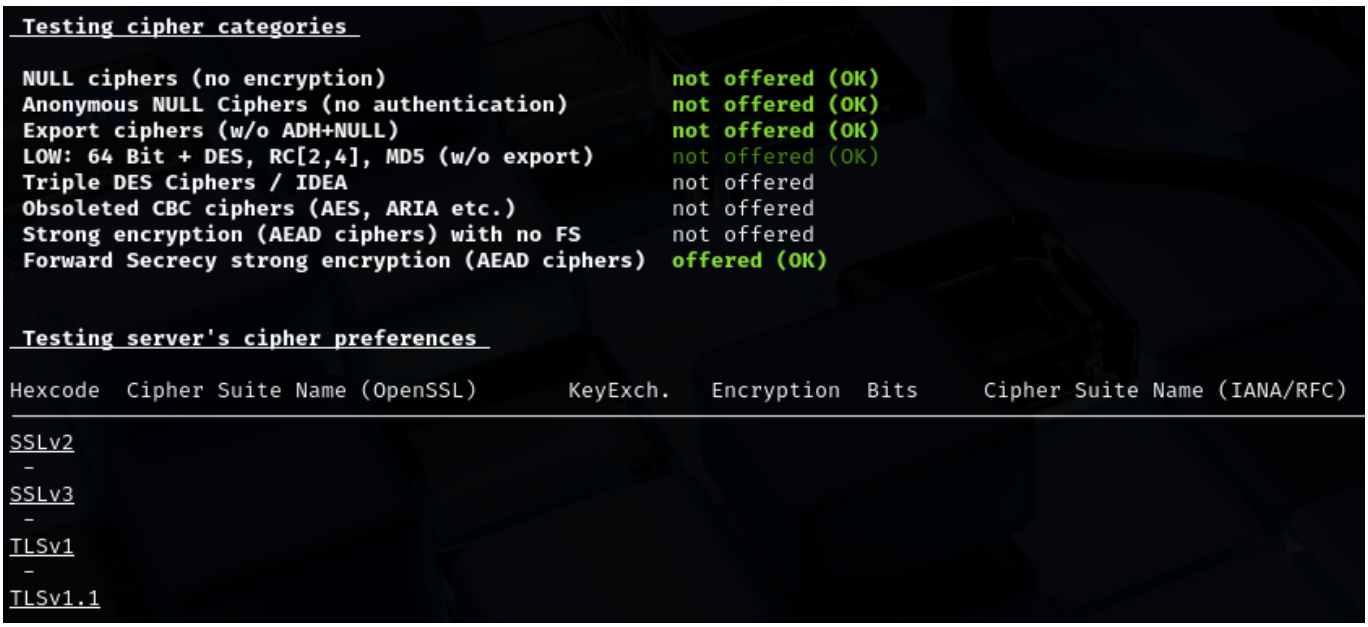
```
git clone https://github.com/drwetter/testssl.sh.git
```

```
cd testssl.sh
chmod +x testssl.sh
```

Exécution du test

```
./testssl.sh https://env-8796793-wp02-ter.hidora.com
```





Le serveur présente une bonne configuration SSL/TLS, avec des protocoles sécurisés, des chiffres robustes, et un certificat valide. Cependant, il y a quelques aspects à améliorer:

HSTS devrait être configuré avec un max-age beaucoup plus long. La compression HTTP gzip active pourrait potentiellement rendre le site vulnérable à BREACH, mais cela dépend du contenu de la page.

Test des mécanismes de connexion et de sécurité

```
sudo apt update
sudo apt install hydra
```

- Tester SSH avec Hydra 👍 effectuer un test de force brute sur le service SSH :

```
hydra -l [nom_utilisateur] -P [chemin_vers_le_dictionnaire] ssh://[IP_CIBLE]
```

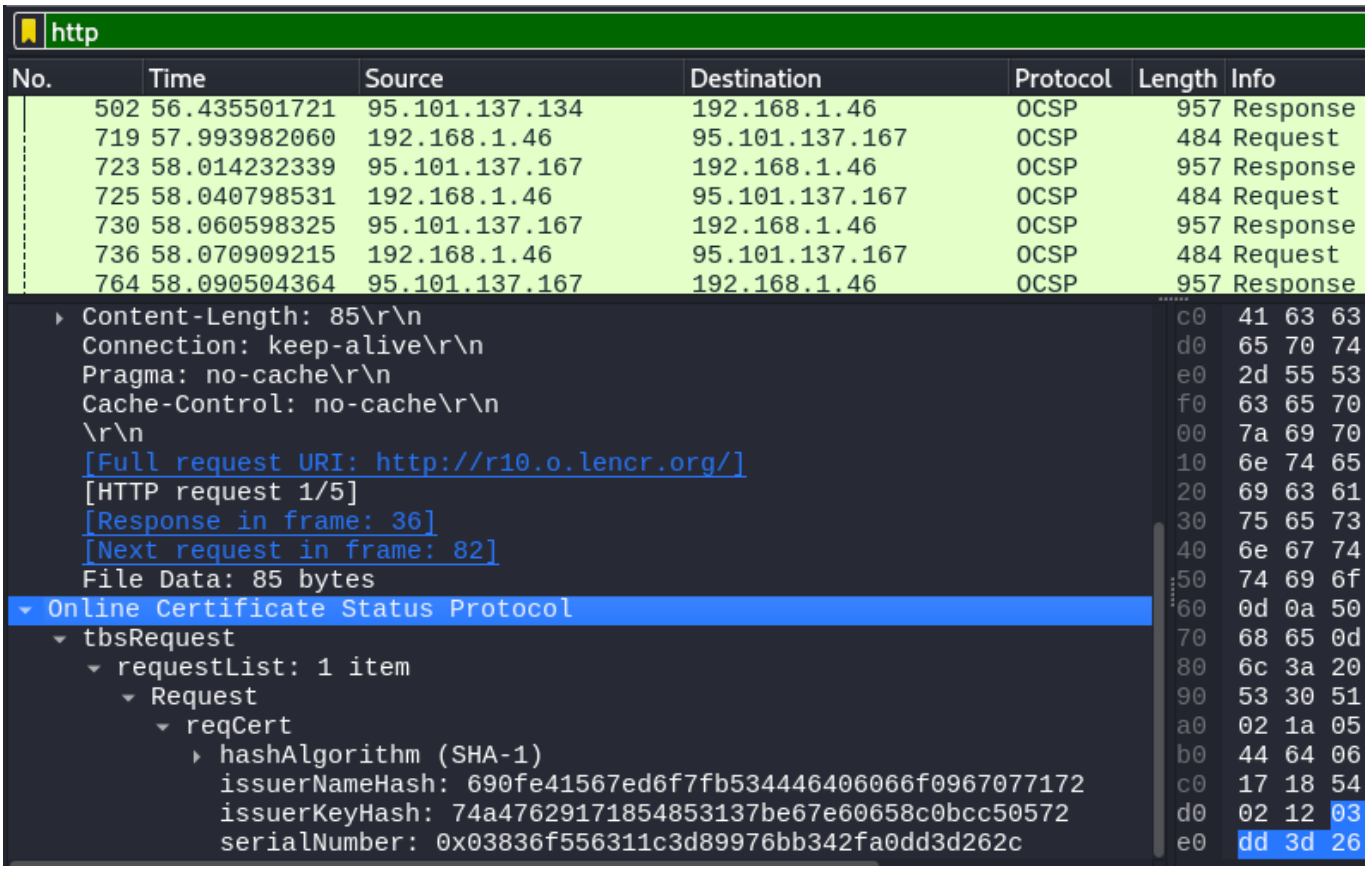
```
hydra -l a-vos-clicswanadoo-fr -P /usr/share/wordlists/ ssh://45.66.220.237
```

```
└─$ hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://45.66.220.237
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes
these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-19 17:11:18
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://45.66.220.237:22/
[ERROR] target ssh://45.66.220.237:22/ does not support password authentication (method reply 36).
```

l'authentification par mot de passe est désactivée sur ce serveur SSH. Ce qui est une bonne pratique pour sécuriser le serveur contre les attaques par brute force.

Analyse des flux réseau

- HTTP



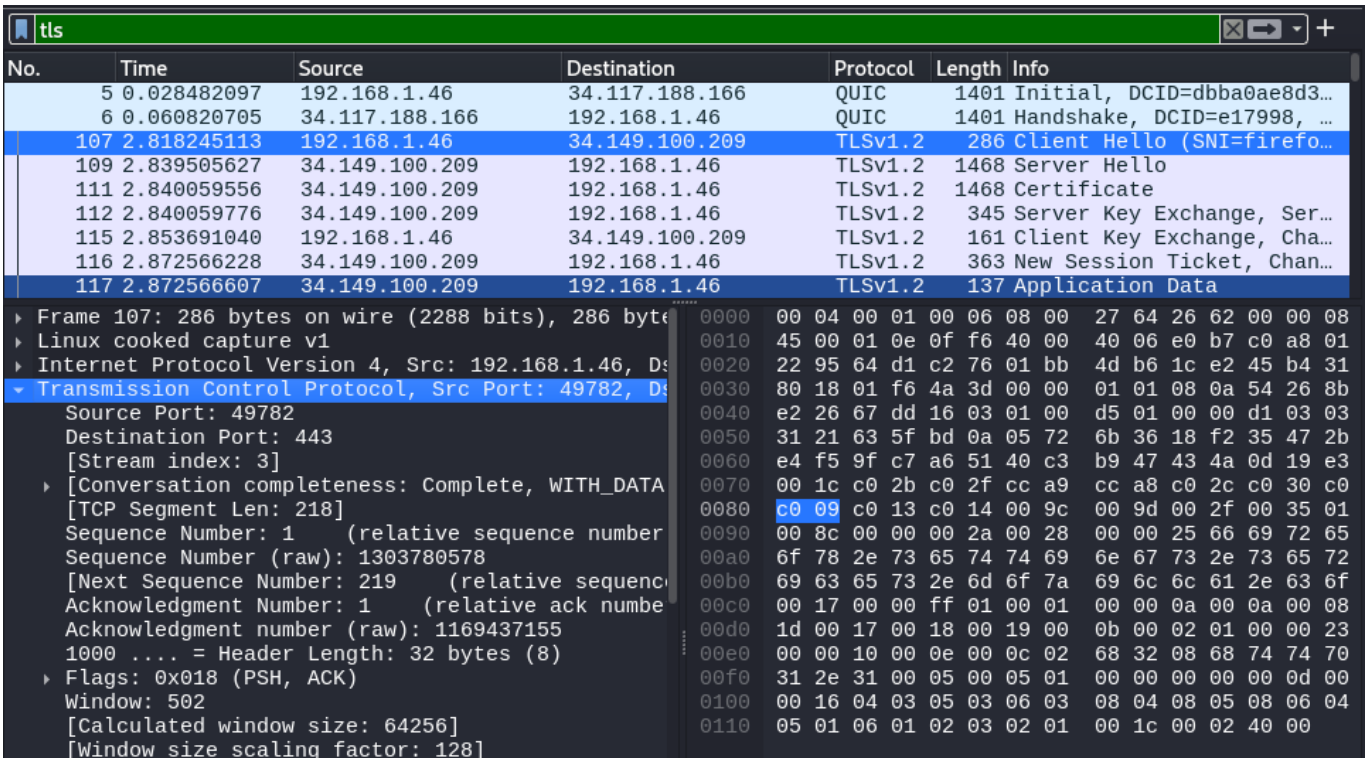
Surveiller les connexions non sécurisées

Le protocole OCSP assure que le certificat du serveur est valide et non révoqué, renforçant ainsi la sécurité des communications.

OCSP permet d'éviter les connexions à des serveurs avec des certificats compromis, protégeant contre les attaques "man-in-the-middle".

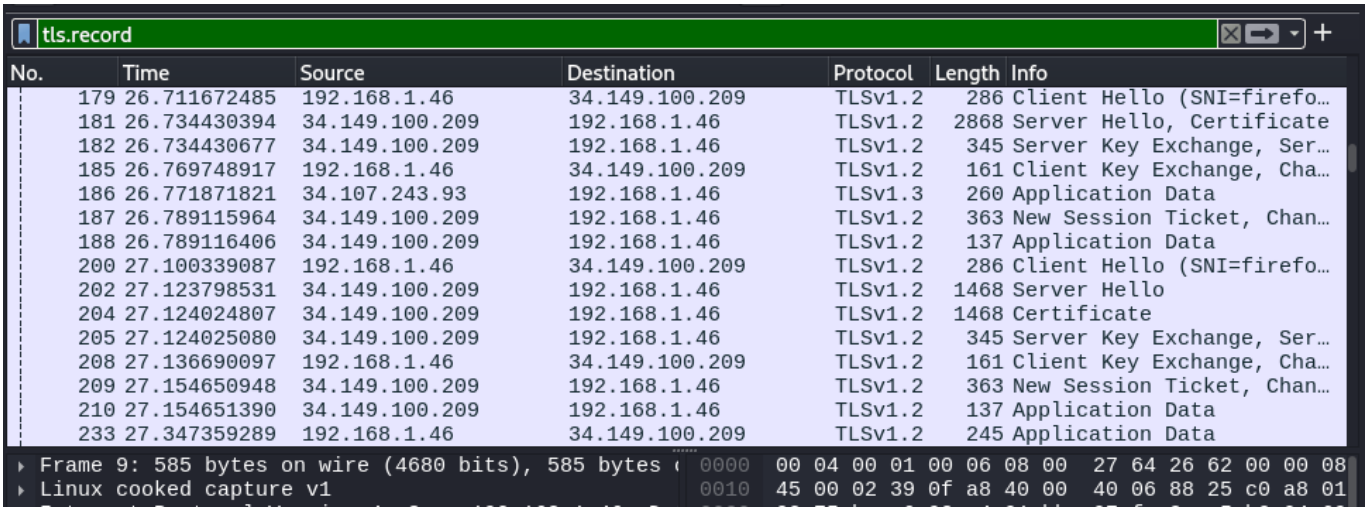
Cache OCSP : La mise en cache des réponses OCSP améliore les performances, mais doit être utilisée avec précaution pour garantir que les informations de statut des certificats soient régulièrement mises à jour.

```
tls
```



L'audit des paquets TLS montre l'utilisation de TLS 1.2, garantissant des échanges sécurisés avec des mécanismes de chiffrement modernes et des extensions de sécurité appropriées.les données sont cryptées.


```
tls.record
```



Utiliser OpenSSL pour vérifier le certificat SSL/TLS

```
openssl s_client -connect env-8796793-wp02-ter.hidora.com:443
```

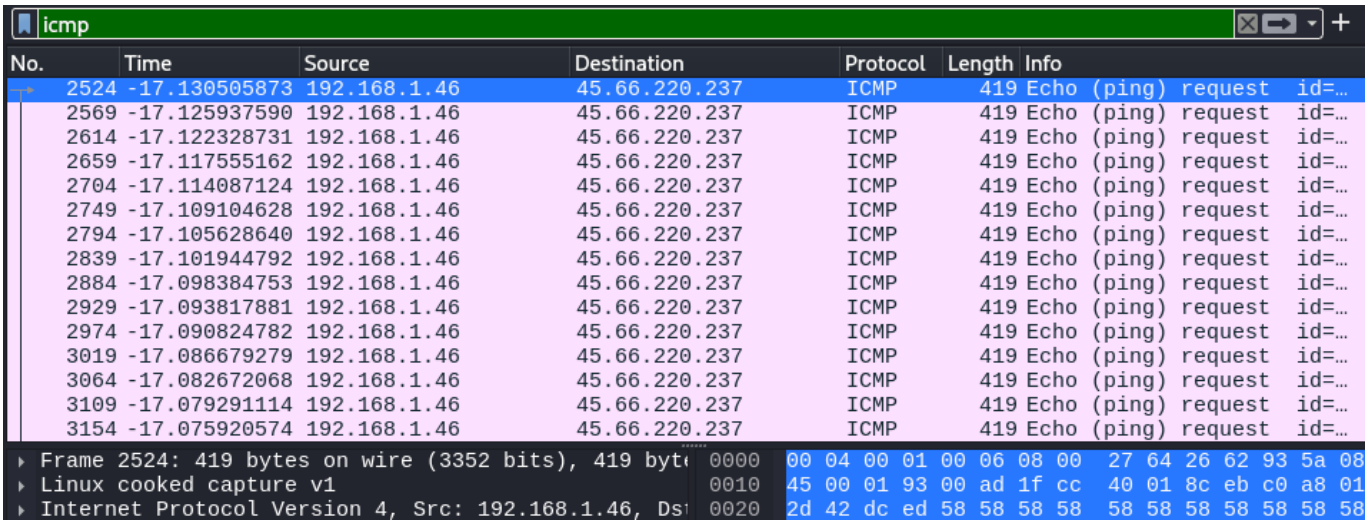
```
└─$ openssl s_client -connect env-8796793-wp02-ter.hidora.com:443 -showcerts

Connecting to 45.66.220.237
CONNECTED(00000003)
depth=2 C=US, O=Internet Security Research Group, CN=ISRG Root X1
verify return:1
depth=1 C=US, O=Let's Encrypt, CN=R10
verify return:1
depth=0 CN=env-8796793-wp02-ter.hidora.com
verify return:1
---
Certificate chain
 0 s:CN=env-8796793-wp02-ter.hidora.com
   i:C=US, O=Let's Encrypt, CN=R10
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Mar 19 09:22:34 2025 GMT; NotAfter: Jun 17 09:22:33 2025 GMT
-----BEGIN CERTIFICATE-----
MIIFQDCCBCigAwIBAgISBcF8Yp+zIihZCJrO65bk54l8MA0GCSqGSIb3DQEBCwUA
MDMxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQwwCgYDVQQD
EwNSMTAwHhcNMjUwMzE5MDkyMjM0WhcNMjUwNjE3MDkyMjMzWjAqMSgwJgYDVQQD
Ex9lbnYtODc5Njc5My13cDAyLXRlci5oaWRvcmEuY29tMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEApXT9OBypNNMg6rm9PiAefzmgi7TYvc5+5e12vqdD
```

TLS 1.3 est utilisé avec un chiffrement de qualité (TLS_AES_256_GCM_SHA384), ce qui est idéal. Le certificat est valide et signé par une autorité reconnue (Let's Encrypt). Aucune faiblesse apparente dans la configuration SSL/TLS.

Actions recommandées: Vérifier le renouvellement du certificat : Le certificat expire en juin 2025

Déni de service

```
hping3 -d 65495 --icmp --flood 45.66.220.237
```



Test avec accès au server web

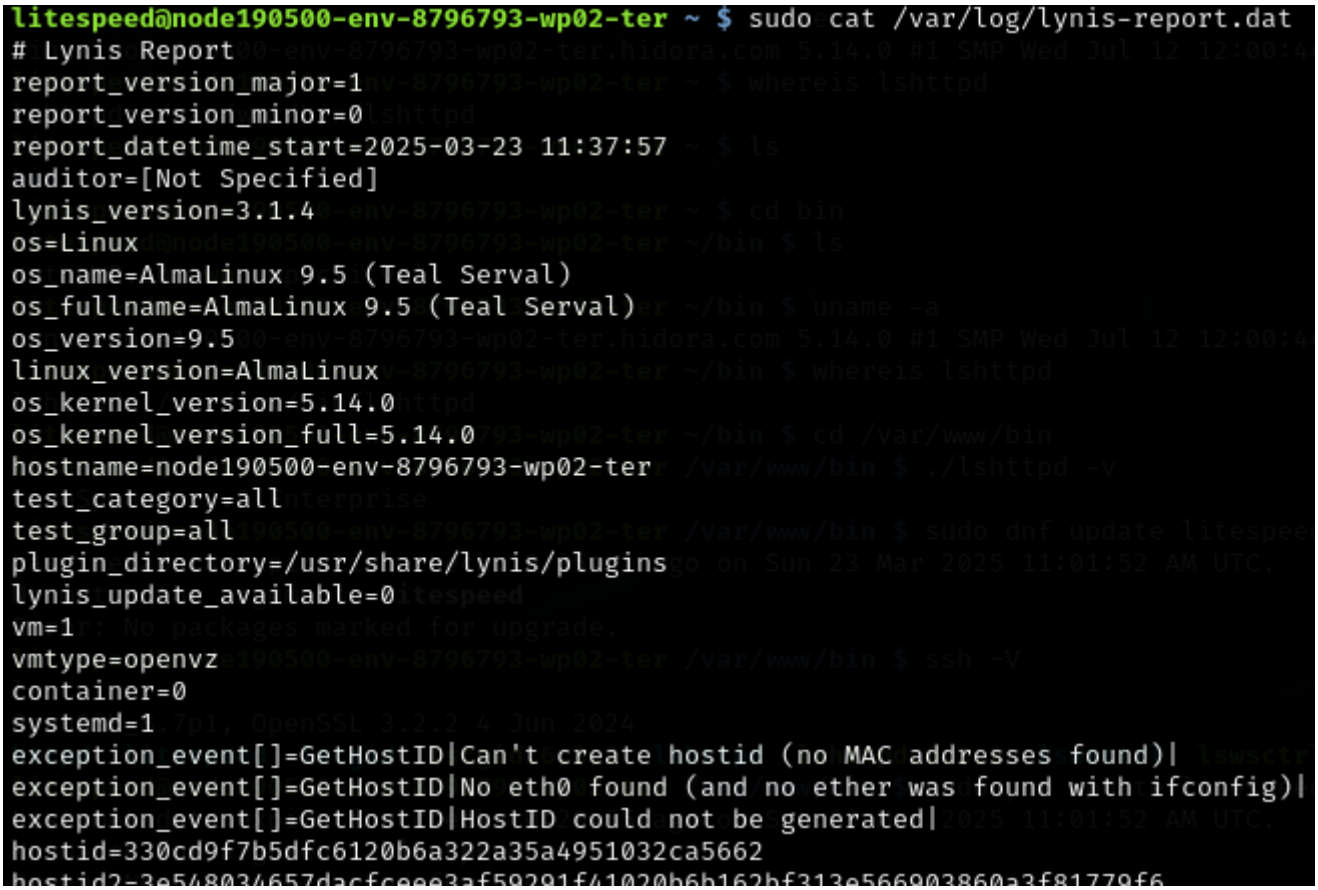
Audit avec Lynis

Exécuter un audit complet de sécurité sur le système à la recherche de vulnérabilités et de mauvaises configurations. à l'aide des profils et plugins définis. Le résultat de l'audit est stocké dans un fichier de rapport

(/var/log/lynis-report.dat).

```
sudo dnf install lynis

sudo lynis audit system

Fichiers de Rapport :
```

```
sudo cat /var/log/lynis-report.dat
```




```
sudo cat cat /var/log/lynis.log
```

```
litespeed@node190500-env-8796793-wp02-ter ~ $ sudo cat cat /var/log/lynis.log
cat: cat: No such file or directory
2025-03-23 11:37:57 Starting Lynis 3.1.4 with PID 37239, build date 2025-01-28
2025-03-23 11:37:57 ====
2025-03-23 11:37:57 ### 2007-2024, CISOfy - https://cisofy.com/lynis/ ###
2025-03-23 11:37:57 Checking permissions of /usr/share/lynis/include/profiles
2025-03-23 11:37:57 File permissions are OK
2025-03-23 11:37:57 Reading profile/configuration /etc/lynis/default.prf
2025-03-23 11:37:57 Action: created temporary file /tmp/lynis.mFRNWJ5DP6
2025-03-23 11:37:57 Language set via profile to ''
2025-03-23 11:37:58 Plugin 'authentication' enabled according profile (/etc/lynis/default.prf)
2025-03-23 11:37:58 Plugin 'compliance' enabled according profile (/etc/lynis/default.prf)
2025-03-23 11:37:58 Plugin 'configuration' enabled according profile (/etc/lynis/default.prf)
2025-03-23 11:37:58 Plugin 'control-panels' enabled according profile (/etc/lynis/default.prf)
2025-03-23 11:37:58 Plugin 'crypto' enabled according profile (/etc/lynis/default.prf)
2025-03-23 11:37:58 Plugin 'dns' enabled according profile (/etc/lynis/default.prf)
2025-03-23 11:37:58 Plugin 'docker' enabled according profile (/etc/lynis/default.prf)
2025-03-23 11:37:58 Plugin 'file-integrity' enabled according profile (/etc/lynis/default.prf)
2025-03-23 11:37:58 Plugin 'file-systems' enabled according profile (/etc/lynis/default.prf)
2025-03-23 11:37:58 Plugin 'firewalls' enabled according profile (/etc/lynis/default.prf)
2025-03-23 11:37:58 Plugin 'forensics' enabled according profile (/etc/lynis/default.prf)
2025-03-23 11:37:58 Plugin 'hardware' enabled according profile (/etc/lynis/default.prf)
2025-03-23 11:37:58 Plugin 'intrusion-detection' enabled according profile (/etc/lynis/default.prf)
2025-03-23 11:37:58 Plugin 'intrusion-prevention' enabled according profile (/etc/lynis/default.prf)
2025-03-23 11:37:58 Plugin 'kernel' enabled according profile (/etc/lynis/default.prf)
2025-03-23 11:37:58 Plugin 'malware' enabled according profile (/etc/lynis/default.prf)
2025-03-23 11:37:58 Plugin 'memory' enabled according profile (/etc/lynis/default.prf)
2025-03-23 11:37:58 Plugin 'nginx' enabled according profile (/etc/lynis/default.prf)
2025-03-23 11:37:58 Plugin 'pam' enabled according profile (/etc/lynis/default.prf)
2025-03-23 11:37:58 Plugin 'processes' enabled according profile (/etc/lynis/default.prf)
2025-03-23 11:37:58 Plugin 'security-modules' enabled according profile (/etc/lynis/default.prf)
2025-03-23 11:37:58 Plugin 'software' enabled according profile (/etc/lynis/default.prf)
```

Tests Effectués:

Le test a couvert une gamme complète de catégories de sécurité, y compris:

- Authentification
- Configuration
- Pare-feu
- Intrusion-detection et prevention
- Sécurité des fichiers et systèmes de fichiers
- Cryptographie et protocoles de communication
- Sécurité des utilisateurs et des processus
- Systèmes d'exploitation et modules de sécurité

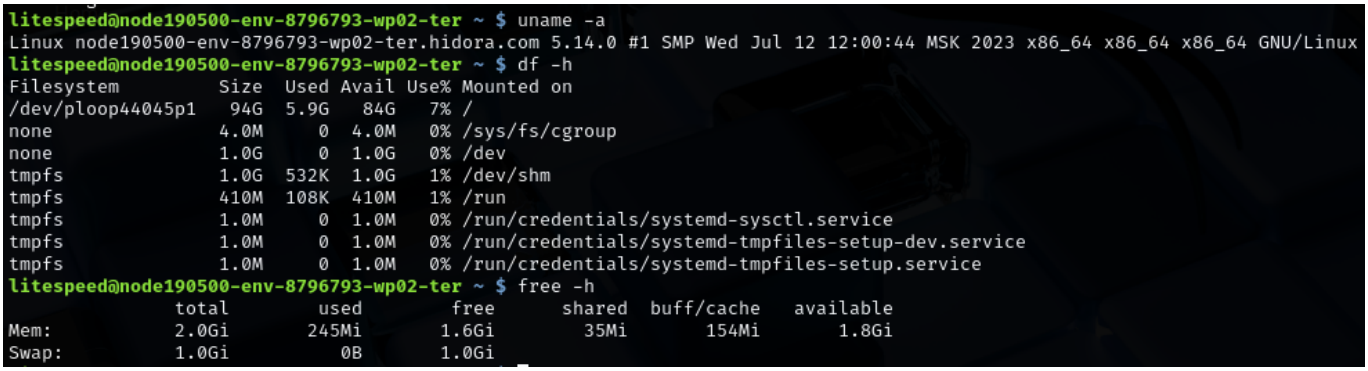
Chaque catégorie de test est associée à des plugins activés et configurés pour vérifier la conformité aux meilleures pratiques de sécurité.

Audit réussi, mais des configurations réseau doivent être vérifiées, notamment concernant l'identification du système via MAC (si nécessaire).

- Collecter les informations du serveur :

```
uname -a
df -h
```

```
free -h
```



Le serveur est dans une situation satisfaisante en termes de version du noyau, d'espace disque, et de mémoire. Aucun problème majeur de ressources n'a été détecté à ce stade. Il est recommandé de maintenir une surveillance continue sur l'espace disque et la mémoire, et de s'assurer que le noyau est régulièrement mis à jour pour appliquer les derniers correctifs de sécurité.

Recommandations :

- Maintenir à jour le noyau
- Surveillance continue de l'espace disque
- Surveiller la swap

Verification des droits

- Sécuriter de la base de donnée:

La ligne skip-grant-tables dans votre fichier /etc/my.cnf ou /etc/mysql/my.cnf est bien supprimé .

```
SELECT user, host, authentication_string, plugin FROM mysql.user;
```

1. Utilisateurs avec accès à la base de données : Les utilisateurs suivants ont été trouvés dans la table mysql.user :

- mariadb.sys : Utilisé pour des tâches internes de MariaDB, aucun mot de passe n'est défini.

- root : L'utilisateur root est présent à la fois localement (localhost) et accessible depuis d'autres hôtes (%, 127.0.0.1), avec un mot de passe sécurisé.
- mysql : Utilisé par MariaDB pour ses propres processus, avec un mot de passe défini.
- PUBLIC : Utilisateur avec accès anonyme, ce qui est une vulnérabilité potentielle.
- user-6981255 : Utilisateur avec accès depuis n'importe quel hôte (%) ainsi que localement (localhost), avec un mot de passe défini.

2. Recommandations de sécurité: Utilisateur PUBLIC : La présence de l'utilisateur anonyme PUBLIC peut être une vulnérabilité importante. Il est recommandé de supprimer cet utilisateur pour éviter un accès non autorisé. La commande pour le faire est :

```
DROP USER 'PUBLIC';
```

Désactivation de l'accès à root depuis des hôtes distants :

```
UPDATE mysql.user SET host = 'localhost' WHERE user = 'root' AND host !=
'localhost';
FLUSH PRIVILEGES;
```

Limiter l'accès à une adresse IP spécifique:

```
UPDATE mysql.user SET host = 'specific_ip_address' WHERE user = 'user-6981255';
FLUSH PRIVILEGES;
```

Tests de vulnérabilité sur les mots de passe MySQL à l'aide de Hashcat

Vérification du Type de Hash

```
hashid hashes.txt
```

- cracker des mots de passe

```
hashcat -O -m 300 -a 0 hashes.txt /usr/share/wordlists/rockyou.txt
```

L'attaque est terminée, mais elle n'a pas réussi à cracker les hachages.

- Vérification des permissions des fichiers et répertoires

Cette commande doit être utilisée sur les répertoires sensibles, comme 👍🏽

```

```

```
ls -l nom_repertoire
```

/etc/ : contient des fichiers de configuration système et des informations sensibles.

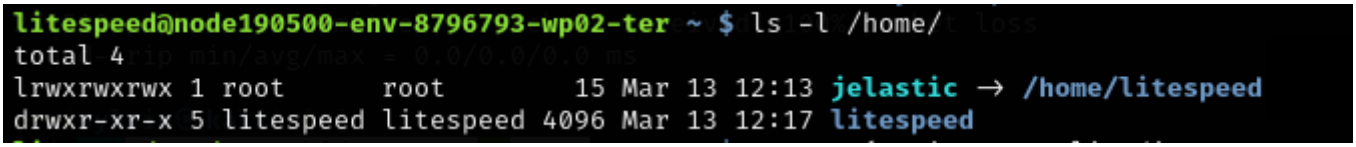
Sécuriser les Fichiers de Configuration des Services

```
sudo chmod 640 /etc/redis.conf
sudo chown root:root /etc/redis.conf
```

Réduire les Permissions des Fichiers Sensibles

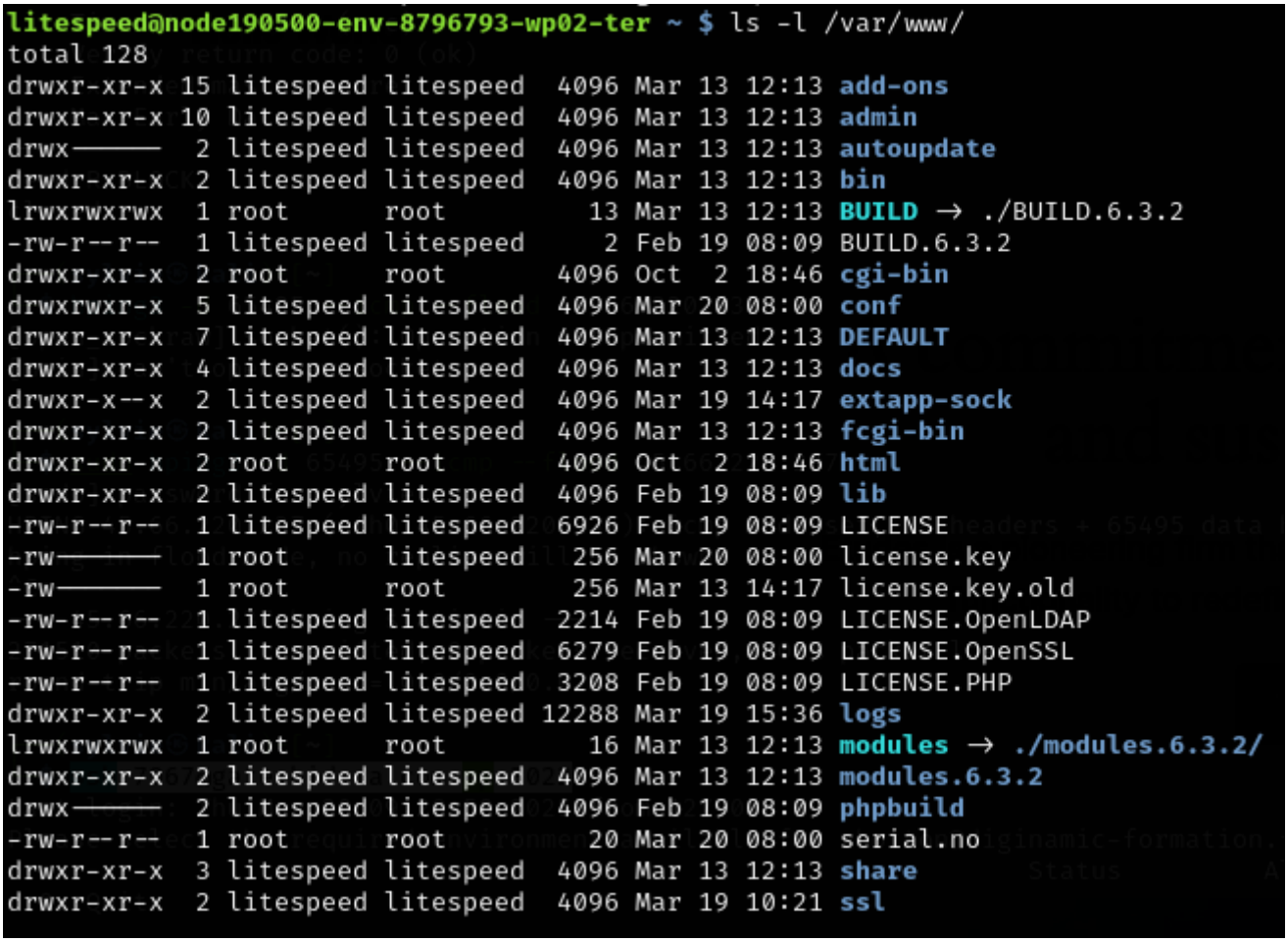
```
sudo chmod 640 /etc/my.cnf
sudo chown root:root /etc/my.cnf
```

/home/ : répertoires personnels des utilisateurs.



Les permissions sur le répertoire litespeed montrent qu'il est réservé à l'utilisateur litespeed, ce qui pourrait être une bonne pratique pour la sécurité.

/var/www/ : répertoires web, où les fichiers des serveurs web peuvent être exposés.



Appliquer des permissions restrictives

```
sudo chmod 700 /var/www/autoupdate
sudo chmod 700 /var/www/tmp
sudo chmod 700 /var/www/phpbuild
sudo chmod 600 /var/www/license.key
sudo chmod 755 /var/www/logs
sudo chmod 644 /var/www/logs/access.log
```

- Vérification de la rotaion des logs

```
sudo nano /etc/logrotate.conf
```

```
litespeed@node190500-env-8796793-wp02-ter ~ $ sudo cat /etc/logrotate.conf
# see "man logrotate" for details

# global options do not affect preceding include directives

# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
dateext

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# system-specific logs may be also be configured here.
```

Mais peu etre améliorer:

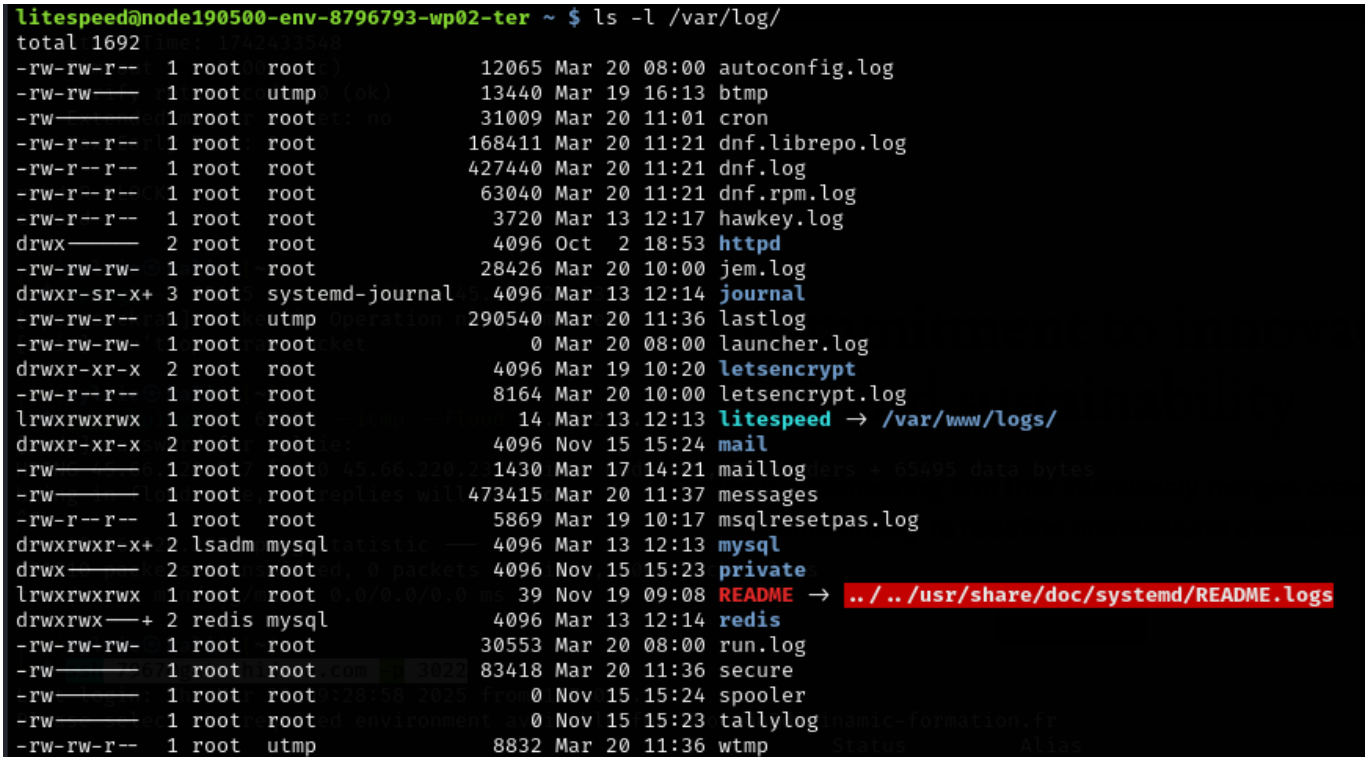
```
litespeed@node190500-env-8796793-wp02-ter ~ $ sudo cat /etc/logrotate.conf
# see "man logrotate" for details

# global options do not affect preceding include directives

# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
dateext

# uncomment this if you want your log files compressed
compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# system-specific logs may be also be configured here.
```

/root/ : répertoire du superutilisateur.

```
litespeed@node190500-env-8796793-wp02-ter ~ $ ls -l /root/
total 36
-rwxr-xr-x 1 root root 3728 Mar 19 10:21 auto-update-ssl-cert.sh
-rwxr-xr-x 1 root root 9635 Mar 19 10:20 generate-ssl-cert.sh
-rwxr-xr-x 1 root root 3311 Mar 19 10:19 install-le.sh
-rw-rw---- 1 root root   41 Mar 20 08:00 oom_adjustment_config
-rw-r--r-- 1 root root  640 Mar 13 12:16 setupUser.sh
-rwxr-xr-x 1 root root 5403 Mar 19 10:20 validation.sh
```

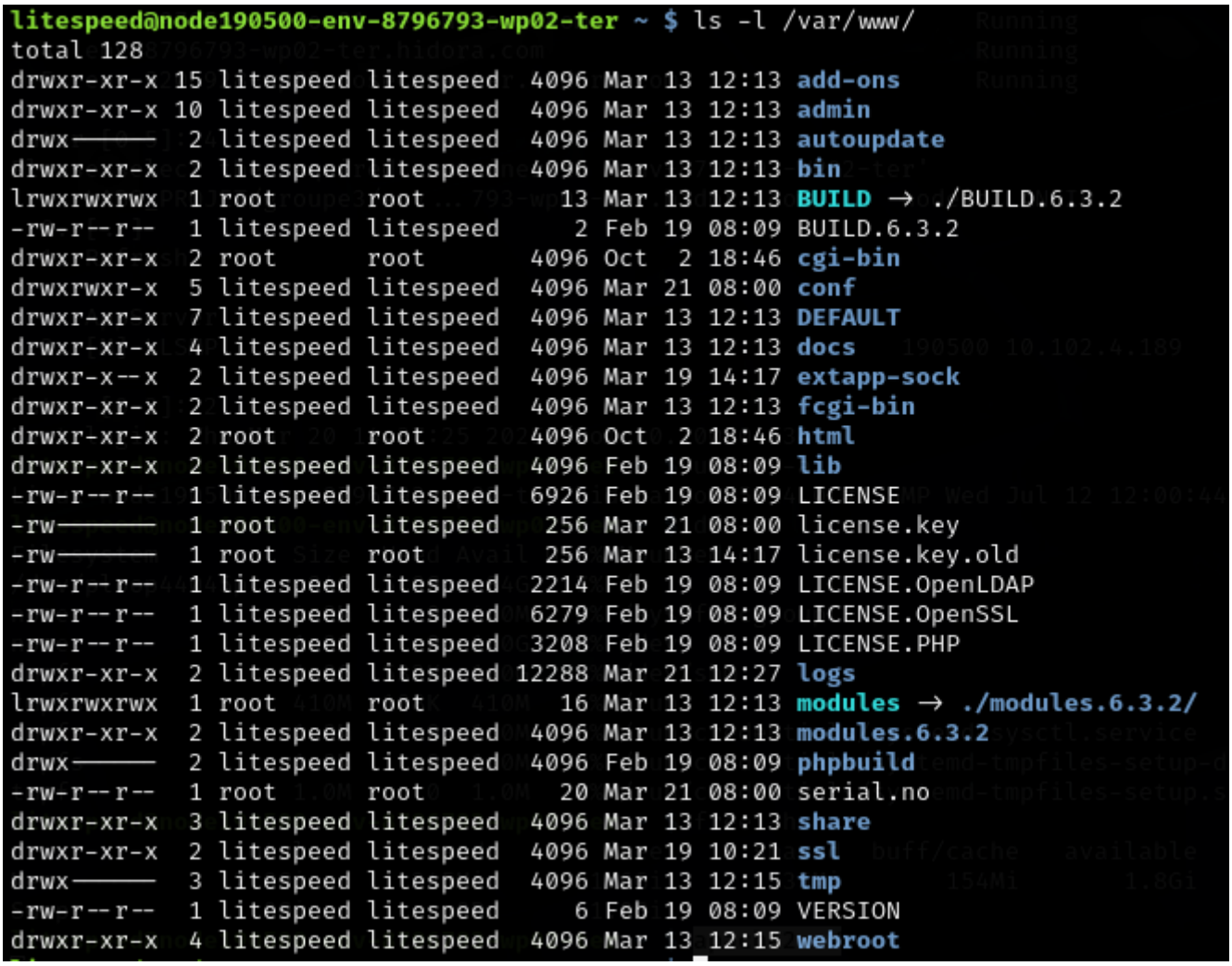
```
chmod 700 /root/auto-update-ssl-cert.sh
chmod 700 /root/generate-ssl-cert.sh
```

/var/log/ : contient les journaux du système qui peuvent contenir des informations sensibles sur l'activité du système.




```
chmod 600 /var/log/jem.log
chmod 600 /var/log/lastlog
chmod 700 /var/log/letsencrypt
chmod 700 /var/www/logs/
chmod 640 /var/log/wtmp
```

- Fichier /var/www/




```
chmod 755 /var/www/html
chmod 700 /var/www/conf
chmod 750 /var/www/logs
```

```
ls -l /etc/passwd
```

- Sécurisation des fichiers sensibles

```
ls -l /etc/shadow
```

```
sudo chmod 600 /etc/shadow
```

Vérification de la complexité des mots de passe

But : Tester si la politique de mots de passe impose des règles de complexité suffisantes (longueur, caractères spéciaux, etc.). Commandes : Consultez les paramètres de pam_pwquality sur les systèmes Linux.

```
cat /etc/pam.d/system-auth | grep pam_pwquality
```

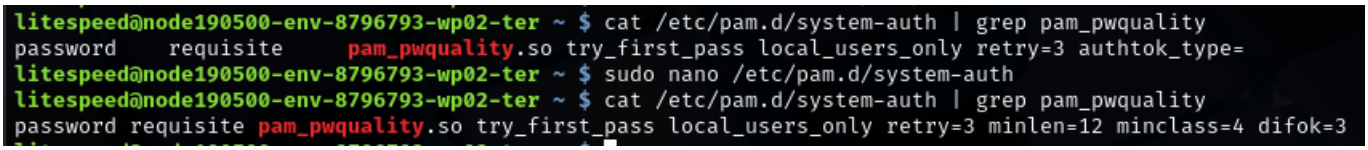
Ajouter des règles de complexité des mots de passe : Vous pouvez imposer des règles plus strictes en ajoutant des paramètres comme :

minlen=12 : Le mot de passe doit comporter au moins 12 caractères.

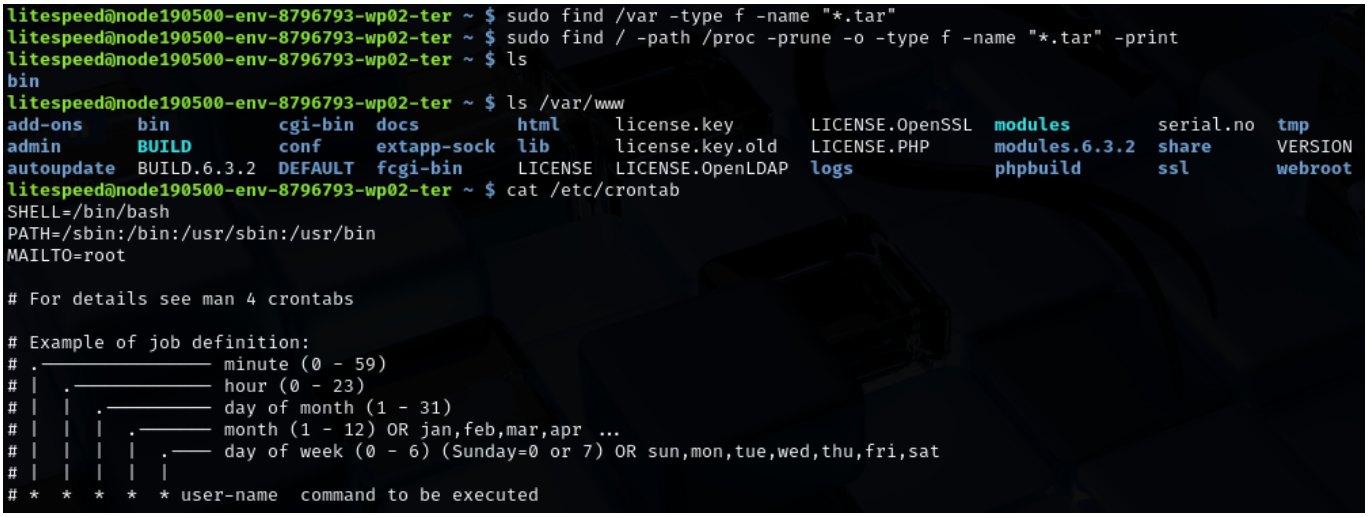
minclass=4 : Le mot de passe doit contenir au moins 4 types de caractères différents (majuscules, minuscules, chiffres, caractères spéciaux).

difok=3 : Il doit y avoir une différence d'au moins 3 caractères entre l'ancien et le nouveau mot de passe.

```
sudo nano /etc/pam.d/system-auth
password requisite pam_pwquality.so retry=3 minlen=12 minclass=4 difok=3
```



Vérification du processus de sauvegarde et restauration



Le manque de sauvegarde et de synchronisation des sauvegardes expose à des risques de perte de données et de récupération difficile en cas de sinistre. Il est crucial de mettre en place une stratégie de sauvegarde automatisée et de synchroniser les sauvegardes sur plusieurs destinations pour garantir la sécurité et la disponibilité des données. L'adoption de solutions de sauvegarde efficaces renforcera la résilience du système et assurera une récupération rapide et fiable des données.

Créer un répertoire de sauvegarde

```
sudo mkdir -p /backup
```

Créer un script de sauvegarde

```
sudo nano /usr/local/bin/backup.sh
```

Ajouter le contenu suivant:

```
#!/bin/bash

# Définir les variables
SOURCE="/var/www"
DESTINATION="/backup/www_backup_$(date +\%F).tar.gz"

# Créer la sauvegarde
tar -czf $DESTINATION $SOURCE

# Optionnel : supprimer les sauvegardes plus anciennes (par exemple, supprimer les
fichiers de plus de 7 jours)
find /backup -type f -name "*.tar.gz" -mtime +7 -exec rm {} \;
```

Rendre le script exécutable

```
sudo chmod +x /usr/local/bin/backup.sh
```

Ajouter la tâche cron pour exécuter la sauvegarde

```
sudo nano /etc/crontab
```

```
0 3 * * * root /usr/local/bin/backup.sh
```

Vérifier

```
sudo crontab -l
```

Installation de openVas

```

```

```
sudo apt update
sudo apt install openvas
```

```
sudo pg_dropcluster --stop 17 main
sudo pg_createcluster 17 main --start
```

Vérifier l'état du service GVM :

```
sudo systemctl status gvmd
sudo systemctl status ospd-openvas
```

```
sudo gvm-setup
sudo gvm-check-setup
```

Accéder à l'interface Web de GVM:

```
sudo gvm-start
```

Accéder a l'interface web

```
https://127.0.0.1:9392
```