

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
```

```
$ nslookup env-8796793-wp02.hidora.com
Server:         192.168.1.254
Address:        192.168.1.254#53

Non-authoritative answer:
Name:   env-8796793-wp02.hidora.com
Address: 185.34.102.100
```

Test de la connectivité avec ping

```
$ ping -c 3 185.34.102.100
PING 185.34.102.100 (185.34.102.100) 56(84) bytes of data.
64 bytes from 185.34.102.100: icmp_seq=1 ttl=54 time=28.3 ms
64 bytes from 185.34.102.100: icmp_seq=2 ttl=54 time=28.4 ms
64 bytes from 185.34.102.100: icmp_seq=3 ttl=54 time=29.1 ms

— 185.34.102.100 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 28.320/28.627/29.136/0.362 ms
```

1. Résumé des Technologies du Site:

The screenshot shows the Wappalyzer web application interface. At the top is a purple header with the Wappalyzer logo and navigation icons. Below the header are three tabs: 'TECHNOLOGIES' (selected), 'PLUS D'INFORMATION', and 'Export'. The main content area is divided into two columns. The left column lists categories: CMS (WordPress 6.6.2), Blog (WordPress 6.6.2), Sécurité (HSTS), and Script de police (Twitter Emoji (Twemoji)). The right column lists categories: Divers (RSS, HTTP/3), Serveur web (LiteSpeed), Langage de programmation (PHP), and Base de données (MySQL). Each item is represented by a circular icon and a text label with a link.

Catégorie	Technologie	Version
CMS	WordPress	6.6.2
Blog	WordPress	6.6.2
Sécurité	HSTS	
Script de police	Twitter Emoji (Twemoji)	
Divers	RSS	
Divers	HTTP/3	
Serveur web	LiteSpeed	
Langage de programmation	PHP	
Base de données	MySQL	

- 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 Twemoji.

Analyse de la Sécurité Réseau et des Services du Serveur

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

```
$ nmap -sV --script=vuln -v 45.66.220.237
(Possible cause: COULDN'T RESOLVE HOST)
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-19 15:12 CET
NSE: Loaded 150 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:12
NSE Timing: About 47.37% done; ETC: 15:13 (0:00:36 remaining)
Completed NSE at 15:13, 34.48s elapsed
Initiating NSE at 15:13
Completed NSE at 15:13, 0.00s elapsed
Pre-scan script results:
| broadcast-avahi-dos: 796793-wp02-ter.hidora.com/wp-content/plugins/ /u
|   Discovered hosts:
|   224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|   Hosts are all up (not vulnerable).
Initiating Ping Scan at 15:13
Scanning 45.66.220.237 [2 ports]
Completed Ping Scan at 15:13, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:13
Completed Parallel DNS resolution of 1 host. at 15:13, 6.53s elapsed
Initiating Connect Scan at 15:13
Scanning 45.66.220.237 [1000 ports]
Discovered open port 80/tcp on 45.66.220.237
Discovered open port 443/tcp on 45.66.220.237
Discovered open port 22/tcp on 45.66.220.237
Discovered open port 8443/tcp on 45.66.220.237
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
```

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
Error: Unknown response received Code: 403
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).
Error: Unknown response received Code: 403
PORT: STATE SERVICE
22/tcp open  ssh
| ssh-auth-methods:
|_ Supported authentication methods:
|_  publickey
|_  gssapi-keyex
|_  gssapi-with-mic
Error: Unknown response received Code: 403
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.

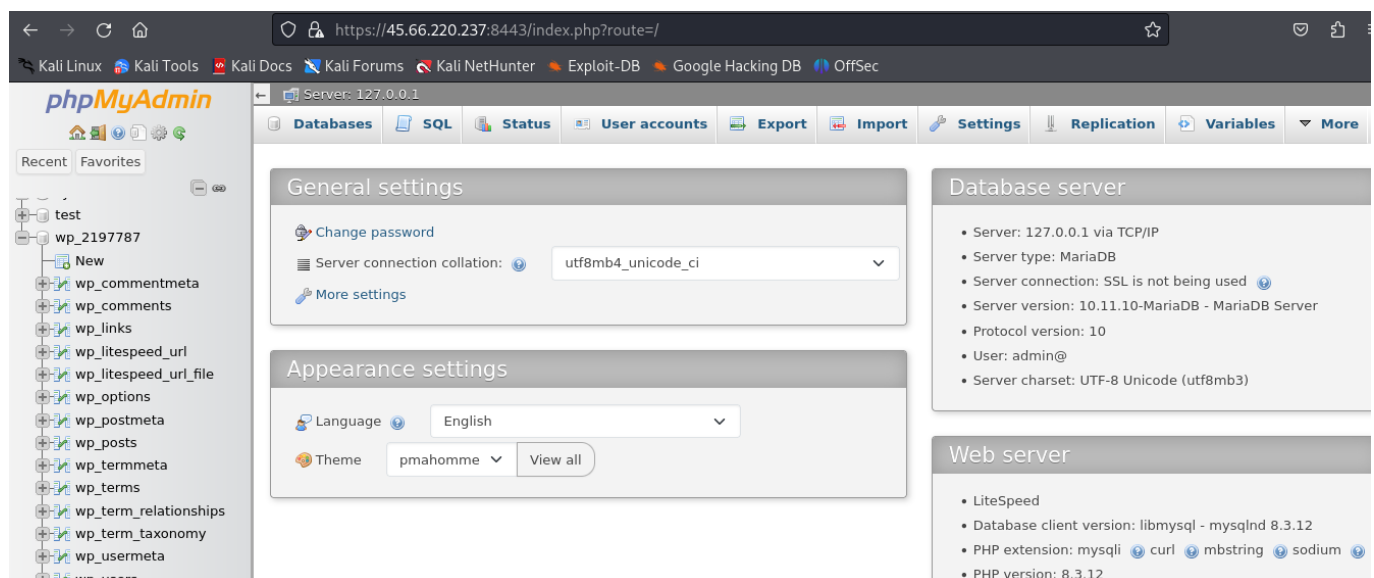
- Port 8443/tcp (HTTPS alternatif)

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 vulnérabilités

- Détecter des vulnérabilités courantes avec Nikto

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

```

$ nikto -h http://185.34.102.100 -C all
- Nikto v2.5.0

+ Target IP:      185.34.102.100
+ Target Hostname: 185.34.102.100
+ Target Port:    80
+ Start Time:     2025-03-18 04:21:28 (GMT1)

+ Server: LiteSpeed
+ /: Drupal Link header found with value: <https://env-8796793-wp02.hidora.com/wp-json/>; rel="https://api.w.org/". See: https://www.drupal.org/
+ /: Uncommon header 'cross-origin-embedder-policy' found, with contents: unsafe-none;.
+ /: Uncommon header 'x-litespeed-cache' found, with contents: hit.
+ /4i18vXrN.xbb: Uncommon header 'x-litespeed-tag' found, with contents: 01e_HTTP.404,01e_404,01e_URL.582bfb491455c89c31da751ce3c1109a,01e_.
+ /4i18vXrN.xbb: Uncommon header 'x-litespeed-cache-control' found, with contents: public,max-age=3600.
+ /4i18vXrN.: Uncommon header 'x-redirect-by' found, with contents: WordPress.
+ /robots.txt: contains 2 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ .: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the
ps://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /favicon.ico: Server may leak inodes via ETags, header found with file /favicon.ico, inode: 47e, size: 67d2cce5, mtime: ab5495fa291182a;;;. See:
g/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 10 item(s) reported on remote host
+ End Time:      2025-03-18 04:22:42 (GMT1) (74 seconds)

+ 1 host(s) tested

```

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/wsutil/filter_files.c124
Spider mode enabled. Check if remote file exists. [Info] ./wsutil/filter_files.c124
--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
Content-Type: text/html; charset=UTF-8
Keep-Alive: timeout=5, max=100
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 identifier 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
```



```
WPScan®

WordPress Security Scanner by the WPScan Team
Version 3.8.28
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: https://env-8796793-wp02-ter.hidora.com/ [45.66.220.237]
[+] Started: Wed Mar 19 12:47:39 2025

Interesting Finding(s):

[+] Headers
| Interesting Entries:
| - x-litespeed-cache: hit
| - 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
| - alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443";
92000; v="43,46"
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] WordPress version 6.6.2 identified (Outdated, released on 2024-09-10).
| Found By: Emoji Settings (Passive Detection)
| - https://env-8796793-wp02-ter.hidora.com/, Match: 'wp-includes/js/wp-emoji-release.min.js?ver=6.6.2'
| Confirmed By: Meta Generator (Passive Detection)
| - https://env-8796793-wp02-ter.hidora.com/, Match: 'WordPress 6.6.2'

[+] WordPress theme in use: twentytwentyfour
| Location: https://env-8796793-wp02-ter.hidora.com/wp-content/themes/twentytwentyfour/
| Latest Version: 1.3
| Last Updated: 2024-11-13T00:00:00.000Z
| Style URL: https://env-8796793-wp02-ter.hidora.com/wp-content/themes/twentytwentyfour/style.css
| Found By: Urls In Homepage (Passive Detection)
| The version could not be determined.

[+] Enumerating Vulnerable Plugins (via Passive and Aggressive Methods)
Checking Known Locations - Time: 00:05:21 ←

[i] No plugins Found.

[+] WPScan DB API OK
| Plan: free
| Requests Done (during the scan): 2
| Requests Remaining: 19

[+] Finished: Wed Mar 19 12:53:29 2025
[+] Requests Done: 14726
[+] Cached Requests: 5
[+] Data Sent: 3.737 MB
[+] Data Received: 17.151 MB
[+] Memory used: 289.332 MB
[+] Elapsed time: 00:05:50
```

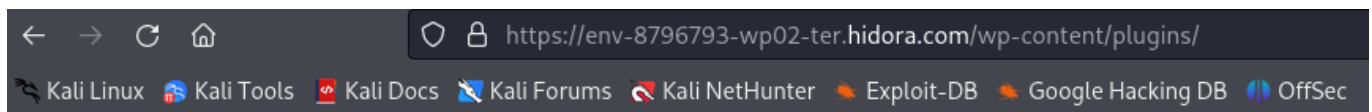
Version de WordPress détectée: 6.6.2 **Problème:** Cette version est obsolète. Il est fortement recommandé de mettre à jour WordPress vers la version la plus récente pour bénéficier des derniers correctifs de sécurité.

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 patches 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
```

```
[i] User(s) Identified:  
[+] a-vos-clicswanadoo-fr  
| Found By: Author Posts - Author Pattern (Passive Detection)  
[+] WPScan DB API OK  
| Plan: free  
| Requests Done (during the scan): 0  
| Requests Remaining: 17
```

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
```

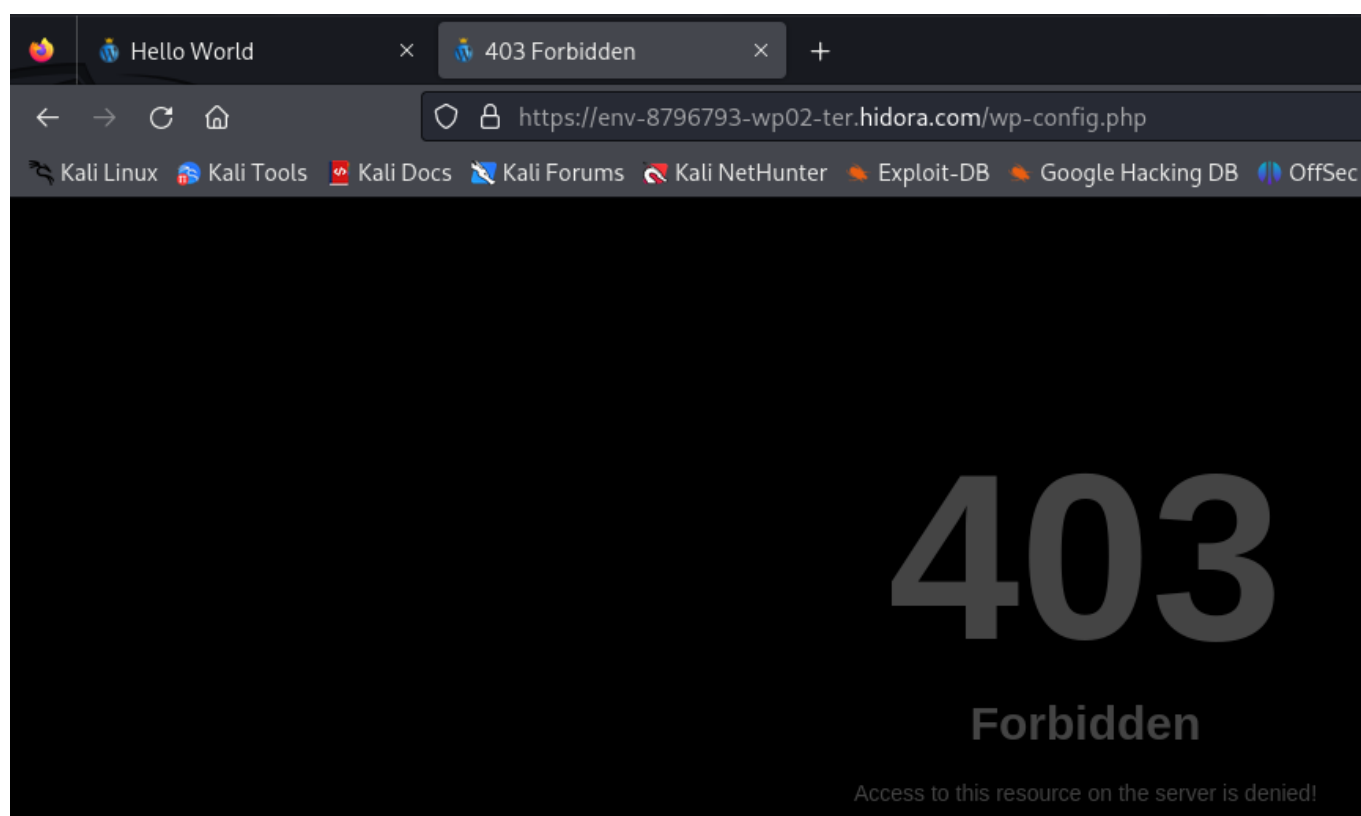
Aucun mot de passe valide n'a été trouvé pour l'utilisateur a-vos-clicswanadoo-fr parmi les mots de passe populaires de la liste rockyou.txt.

1. Vérification des fichiers sensibles

Vérification manuelle

Accès au fichier wp-config.php

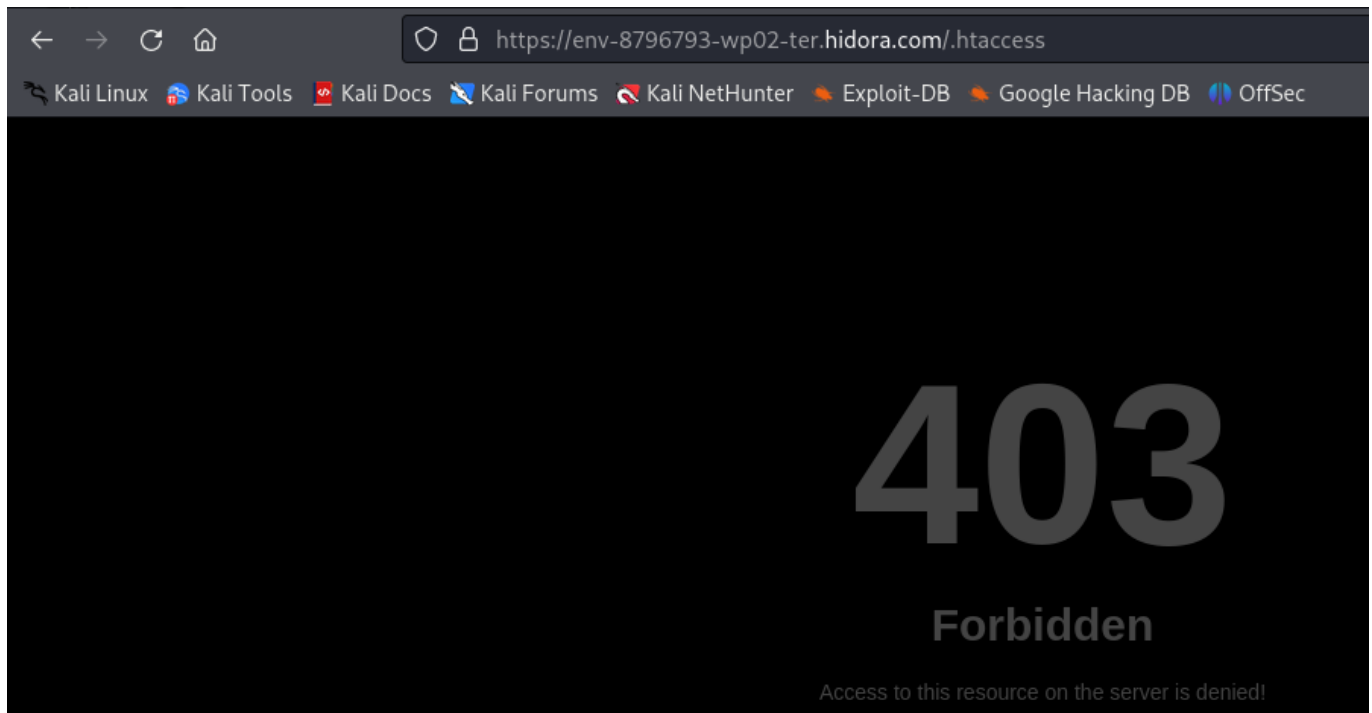
```
https://env-8796793-wp02-ter.hidora.com/wp-config.php
```



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

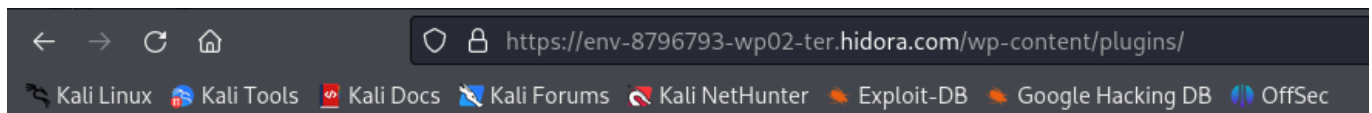
```
https://env-8796793-wp02-ter.hidora.com/.htaccess
```



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/

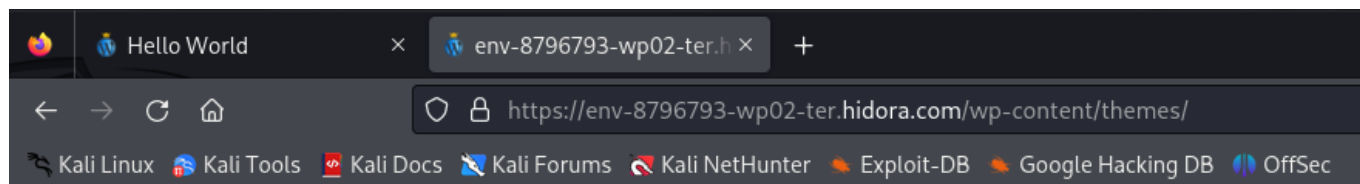
```
https://env-8796793-wp02-ter.hidora.com/wp-content/plugins/
```



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/

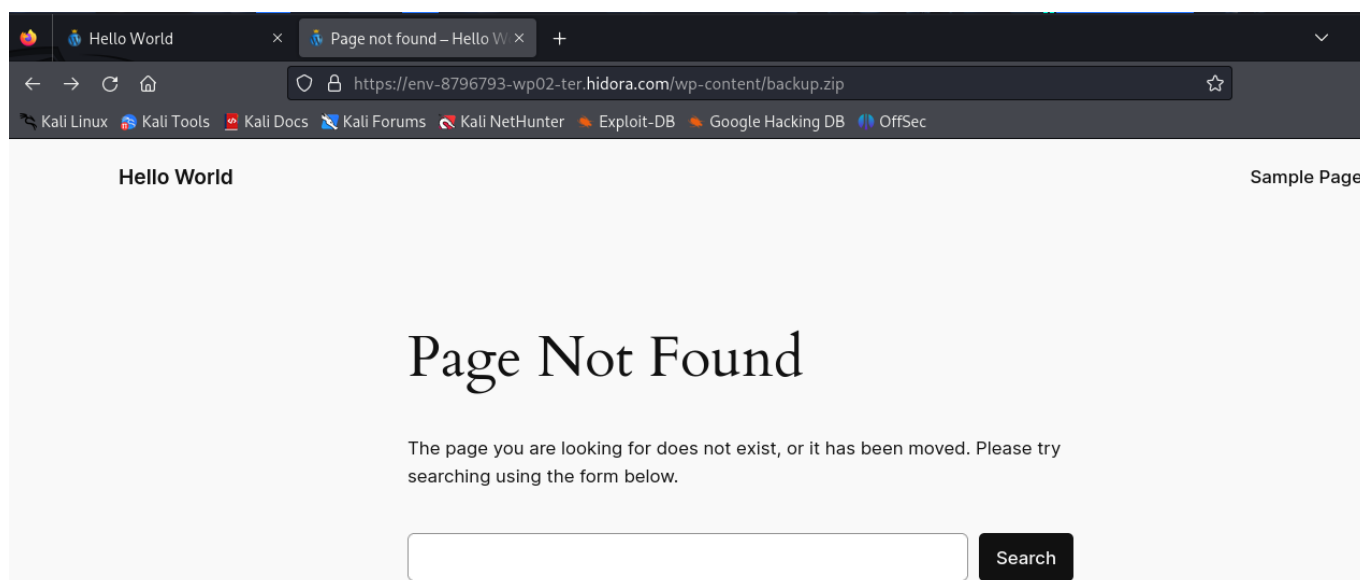
```
https://env-8796793-wp02-ter.hidora.com/wp-content/themes/
```



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)

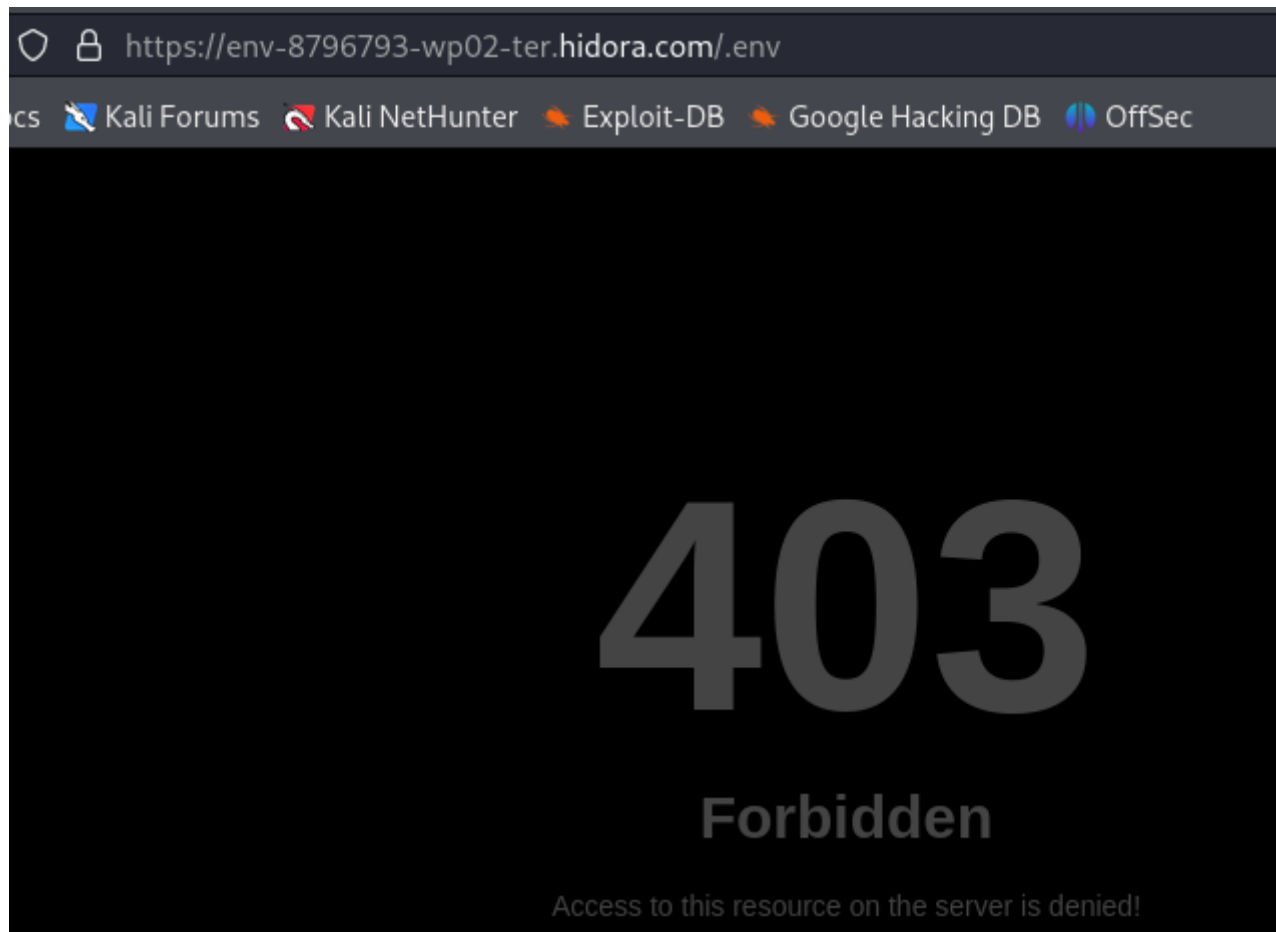
<https://env-8796793-wp02-ter.hidora.com/wp-content/backup.zip>



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>

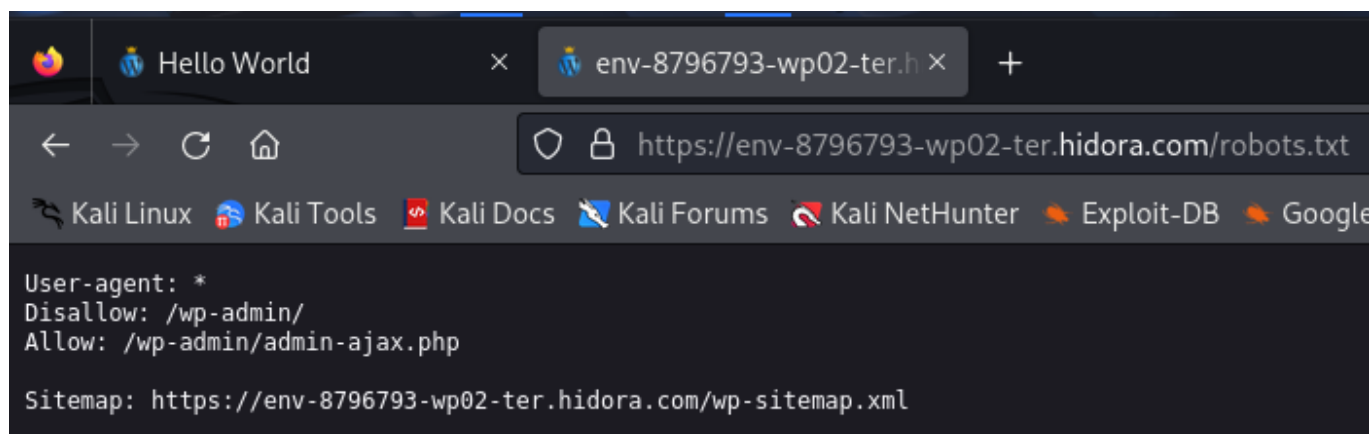


La réponse 403 Forbidden est un bon indicateur que des mesures de sécurité ont été correctement mises en place pour protéger le fichier .env. Ainsi le site est protégé contre des compromissions du site.

Analyser les fichiers robots.txt et sitemap.xml

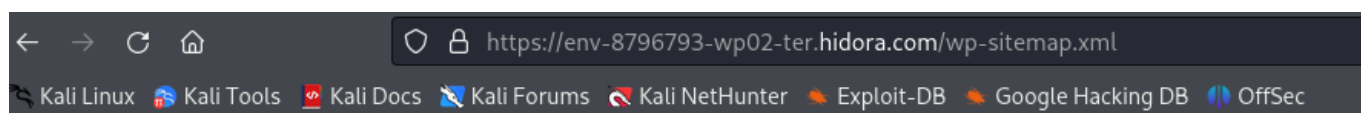
- fichier robots.txt

```
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
```



XML Sitemap

This XML Sitemap is generated by WordPress to make your content more visible for search engines.

[Learn more about XML sitemaps.](#)

Number of URLs in this XML Sitemap: 4.

URL

<https://env-8796793-wp02-ter.hidora.com/wp-sitemap-posts-post-1.xml>

<https://env-8796793-wp02-ter.hidora.com/wp-sitemap-posts-page-1.xml>

<https://env-8796793-wp02-ter.hidora.com/wp-sitemap-taxonomies-category-1.xml>

<https://env-8796793-wp02-ter.hidora.com/wp-sitemap-users-1.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.



XML Sitemap

This XML Sitemap is generated by WordPress to make your content more visible for search engines.

[Learn more about XML sitemaps.](#)

Number of URLs in this XML Sitemap: 1.

URL

<https://env-8796793-wp02-ter.hidora.com/author/a-vos-clicswanadoo-fr/>

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
```


16 / 34

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
```

```

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

#####
testssl.sh version 3.2rc4 from https://testssl.sh/dev/
(5359befc 2025-03-20 15:44:28)

This program is free software. Distribution and modification under
GPLv2 permitted. USAGE w/o ANY WARRANTY. USE IT AT YOUR OWN RISK!

Please file bugs @ https://testssl.sh/bugs/
#####

Using OpenSSL 1.0.2-bad (Sep 1 2022) [~183 ciphers]
on kali:./bin/openssl.Linux.x86_64

Start 2025-03-21 15:18:31 —> 45.66.220.237:443 (env-8796793-wp02-ter.hidora.com) <—

rDNS (45.66.220.237): --
Service detected: HTTP

Testing protocols via sockets except NPN+ALPN

SSLv2      not offered (OK)
SSLv3      not offered (OK)
TLS 1      not offered
TLS 1.1    not offered
TLS 1.2    offered (OK)
TLS 1.3    offered (OK): final
NPN/SPDY   not offered
ALPN/HTTP2 h2, spdy/3.1, http/1.1, spdy/2, spdy/3 (offered)

Testing cipher categories

NULL ciphers (no encryption)          not offered (OK)
Anonymous NULL Ciphers (no authentication) not offered (OK)
Export ciphers (w/o ADH+NULL)         not offered (OK)
LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export) not offered (OK)
Triple DES Ciphers / IDEA             not offered
Obsoleted CBC ciphers (AES, ARIA etc.) not offered
Strong encryption (AEAD ciphers) with no FS not offered
Forward Secrecy strong encryption (AEAD ciphers) offered (OK)

Testing server's cipher preferences

Hexcode  Cipher Suite Name (OpenSSL)  KeyExch.  Encryption  Bits  Cipher Suite Name (IANA/RFC)
-----
SSLv2
-
SSLv3
-
TLSv1
-
TLSv1.1

```

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
```

```
l-$ 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:l/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

http

No.	Time	Source	Destination	Protocol	Length	Info
502	56.435501721	95.101.137.134	192.168.1.46	OCSP	957	Response
719	57.993982060	192.168.1.46	95.101.137.167	OCSP	484	Request
723	58.014232339	95.101.137.167	192.168.1.46	OCSP	957	Response
725	58.040798531	192.168.1.46	95.101.137.167	OCSP	484	Request
730	58.060598325	95.101.137.167	192.168.1.46	OCSP	957	Response
736	58.070909215	192.168.1.46	95.101.137.167	OCSP	484	Request
764	58.090504364	95.101.137.167	192.168.1.46	OCSP	957	Response

Content-Length: 85\r\nConnection: keep-alive\r\nPragma: no-cache\r\nCache-Control: no-cache\r\n\r\n[Full request URI: http://r10.o.lencr.org/][HTTP request 1/5][Response in frame: 36][Next request in frame: 82]File Data: 85 bytes

Online Certificate Status Protocol

tbsRequest

requestList: 1 item

Request

reqCert

hashAlgorithm (SHA-1)issuerNameHash: 690fe41567ed6f7fb534446406066f0967077172issuerKeyHash: 74a47629171854853137be67e60658c0bcc50572serialNumber: 0x03836f556311c3d89976bb342fa0dd3d262c

c0 41 63 63
d0 65 70 74
e0 2d 55 53
f0 63 65 70
00 7a 69 70
10 6e 74 65
20 69 63 61
30 75 65 73
40 6e 67 74
50 74 69 6f
60 0d 0a 50
70 68 65 0d
80 6c 3a 20
90 53 30 51
a0 02 1a 05
b0 44 64 06
c0 17 18 54
d0 02 12 03
e0 dd 3d 26

Surveiller les connexions non sécurisées

Le protocole OSCP 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
```

No.	Time	Source	Destination	Protocol	Length	Info
5	0.028482097	192.168.1.46	34.117.188.166	QUIC	1401	Initial, DCID=dbba0ae8d3...
6	0.060820705	34.117.188.166	192.168.1.46	QUIC	1401	Handshake, DCID=e17998, ...
107	2.818245113	192.168.1.46	34.149.100.209	TLSv1.2	286	Client Hello (SNI=firefo...
109	2.839505627	34.149.100.209	192.168.1.46	TLSv1.2	1468	Server Hello
111	2.840059556	34.149.100.209	192.168.1.46	TLSv1.2	1468	Certificate
112	2.840059776	34.149.100.209	192.168.1.46	TLSv1.2	345	Server Key Exchange, Ser...
115	2.853691040	192.168.1.46	34.149.100.209	TLSv1.2	161	Client Key Exchange, Cha...
116	2.872566228	34.149.100.209	192.168.1.46	TLSv1.2	363	New Session Ticket, Chan...
117	2.872566607	34.149.100.209	192.168.1.46	TLSv1.2	137	Application Data

▶ Frame 107: 286 bytes on wire (2288 bits), 286 byte

▶ Linux cooked capture v1

▶ Internet Protocol Version 4, Src: 192.168.1.46, Ds

▼ Transmission Control Protocol, Src Port: 49782, Ds

Source Port: 49782

Destination Port: 443

[Stream index: 3]

▶ [Conversation completeness: Complete, WITH_DATA

[TCP Segment Len: 218]

Sequence Number: 1 (relative sequence number

Sequence Number (raw): 1303780578

[Next Sequence Number: 219 (relative sequenc

Acknowledgment Number: 1 (relative ack numbe

Acknowledgment number (raw): 1169437155

1000 = Header Length: 32 bytes (8)

▶ Flags: 0x018 (PSH, ACK)

Window: 502

[Calculated window size: 64256]

[Window size scaling factor: 128]

0000 00 04 00 01 00 06 08 00 27 64 26 62 00 00 08

0010 45 00 01 0e 0f f6 40 00 40 06 e0 b7 c0 a8 01

0020 22 95 64 d1 c2 76 01 bb 4d b6 1c e2 45 b4 31

0030 80 18 01 f6 4a 3d 00 00 01 01 08 0a 54 26 8b

0040 e2 26 67 dd 16 03 01 00 d5 01 00 00 d1 03 03

0050 31 21 63 5f bd 0a 05 72 6b 36 18 f2 35 47 2b

0060 e4 f5 9f c7 a6 51 40 c3 b9 47 43 4a 0d 19 e3

0070 00 1c c0 2b c0 2f cc a9 cc a8 c0 2c c0 30 c0

0080 c0 09 c0 13 c0 14 00 9c 00 9d 00 2f 00 35 01

0090 00 8c 00 00 00 2a 00 28 00 00 25 66 69 72 65

00a0 6f 78 2e 73 65 74 74 69 6e 67 73 2e 73 65 72

00b0 69 63 65 73 2e 6d 6f 7a 69 6c 6c 61 2e 63 6f

00c0 00 17 00 00 ff 01 00 01 00 00 0a 00 0a 00 08

00d0 1d 00 17 00 18 00 19 00 0b 00 02 01 00 00 23

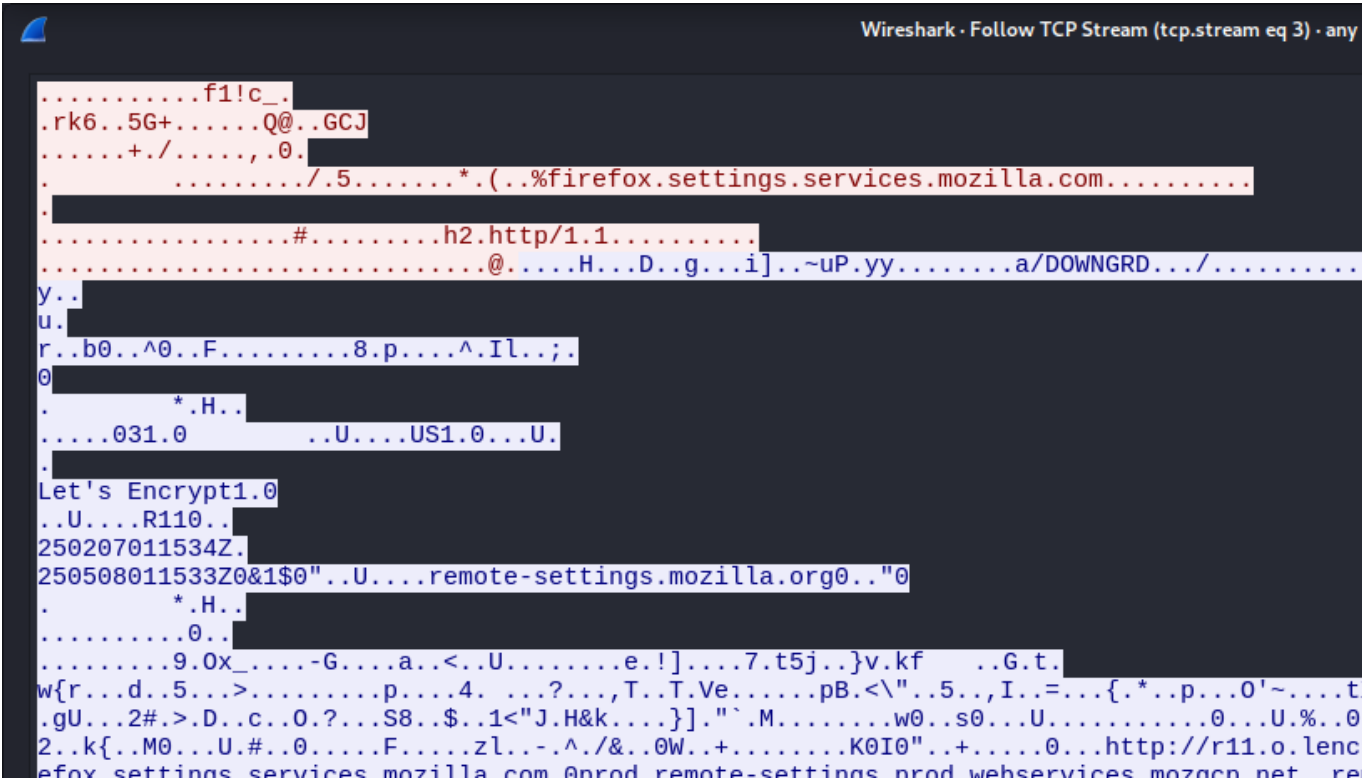
00e0 00 00 10 00 0e 00 0c 02 68 32 08 68 74 74 70

00f0 31 2e 31 00 05 00 05 01 00 00 00 00 00 0d 00

0100 00 16 04 03 05 03 06 03 08 04 08 05 08 06 04

0110 05 01 06 01 02 03 02 01 00 1c 00 02 40 00

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

No.	Time	Source	Destination	Protocol	Length	Info
179	26.711672485	192.168.1.46	34.149.100.209	TLSv1.2	286	Client Hello (SNI=firefo...
181	26.734430394	34.149.100.209	192.168.1.46	TLSv1.2	2868	Server Hello, Certificate
182	26.734430677	34.149.100.209	192.168.1.46	TLSv1.2	345	Server Key Exchange, Ser...
185	26.769748917	192.168.1.46	34.149.100.209	TLSv1.2	161	Client Key Exchange, Cha...
186	26.771871821	34.107.243.93	192.168.1.46	TLSv1.3	260	Application Data
187	26.789115964	34.149.100.209	192.168.1.46	TLSv1.2	363	New Session Ticket, Chan...
188	26.789116406	34.149.100.209	192.168.1.46	TLSv1.2	137	Application Data
200	27.100339087	192.168.1.46	34.149.100.209	TLSv1.2	286	Client Hello (SNI=firefo...
202	27.123798531	34.149.100.209	192.168.1.46	TLSv1.2	1468	Server Hello
204	27.124024807	34.149.100.209	192.168.1.46	TLSv1.2	1468	Certificate
205	27.124025080	34.149.100.209	192.168.1.46	TLSv1.2	345	Server Key Exchange, Ser...
208	27.136690097	192.168.1.46	34.149.100.209	TLSv1.2	161	Client Key Exchange, Cha...
209	27.154650948	34.149.100.209	192.168.1.46	TLSv1.2	363	New Session Ticket, Chan...
210	27.154651390	34.149.100.209	192.168.1.46	TLSv1.2	137	Application Data
233	27.347359289	192.168.1.46	34.149.100.209	TLSv1.2	245	Application Data

Frame 9: 585 bytes on wire (4680 bits), 585 bytes captured (4680 bits) on interface eth0
Linux cooked capture v1

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
MDMxCzAJBgNVBAYTAlVTMRYWFAyDVQKKEw1MZXQncyBFbmNyeXB0MQwwCgYDVQQD
EwNSMTAwHhcNMjUwMzE5MDk5MDk5MDk5MDk5MDk5MDk5MDk5MDk5MDk5MDk5MDk5
Ex9lbnYtODc5Njc5My13cDAyLXRlcj5oaWRvcmluY29tMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEApxT90BypNNMg6rm9PiAefzmg17TYvc5+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
```

No.	Time	Source	Destination	Protocol	Length	Info
2524	-17.130505873	192.168.1.46	45.66.220.237	ICMP	419	Echo (ping) request id=...
2569	-17.125937590	192.168.1.46	45.66.220.237	ICMP	419	Echo (ping) request id=...
2614	-17.122328731	192.168.1.46	45.66.220.237	ICMP	419	Echo (ping) request id=...
2659	-17.117555162	192.168.1.46	45.66.220.237	ICMP	419	Echo (ping) request id=...
2704	-17.114087124	192.168.1.46	45.66.220.237	ICMP	419	Echo (ping) request id=...
2749	-17.109104628	192.168.1.46	45.66.220.237	ICMP	419	Echo (ping) request id=...
2794	-17.105628640	192.168.1.46	45.66.220.237	ICMP	419	Echo (ping) request id=...
2839	-17.101944792	192.168.1.46	45.66.220.237	ICMP	419	Echo (ping) request id=...
2884	-17.098384753	192.168.1.46	45.66.220.237	ICMP	419	Echo (ping) request id=...
2929	-17.093817881	192.168.1.46	45.66.220.237	ICMP	419	Echo (ping) request id=...
2974	-17.090824782	192.168.1.46	45.66.220.237	ICMP	419	Echo (ping) request id=...
3019	-17.086679279	192.168.1.46	45.66.220.237	ICMP	419	Echo (ping) request id=...
3064	-17.082672068	192.168.1.46	45.66.220.237	ICMP	419	Echo (ping) request id=...
3109	-17.079291114	192.168.1.46	45.66.220.237	ICMP	419	Echo (ping) request id=...
3154	-17.075920574	192.168.1.46	45.66.220.237	ICMP	419	Echo (ping) request id=...

Frame 2524: 419 bytes on wire (3352 bits), 419 bytes captured (3352 bits) on interface

Linux cooked capture v1

Internet Protocol Version 4, Src: 192.168.1.46, Destination: 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
```

```
litespeed@node190500-env-8796793-wp02-ter ~ $ sudo cat /var/log/lynis-report.dat
# Lynis Report
report_version_major=1
report_version_minor=0
report_datetime_start=2025-03-23 11:37:57
auditor=[Not Specified]
lynis_version=3.1.4
os=Linux
os_name=AlmaLinux 9.5 (Teal Serval)
os_fullname=AlmaLinux 9.5 (Teal Serval)
os_version=9.5
linux_version=AlmaLinux
os_kernel_version=5.14.0
os_kernel_version_full=5.14.0
hostname=node190500-env-8796793-wp02-ter
test_category=all
test_group=all
plugin_directory=/usr/share/lynis/plugins
lynis_update_available=0
vm=1
vmtype=openvz
container=0
systemd=1
exception_event[]=GetHostID|Can't create hostid (no MAC addresses found)|
exception_event[]=GetHostID|No eth0 found (and no ether was found with ifconfig)|
exception_event[]=GetHostID|HostID could not be generated|
hostid=330cd9f7b5dfc6120b6a322a35a4951032ca5662
hostid2=3e548034657dacfc0ee3af50201f41020b6b162bf313e566003860a3f81770f6
```

```
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.prfl
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.prfl)
2025-03-23 11:37:58 Plugin 'compliance' enabled according profile (/etc/lynis/default.prfl)
2025-03-23 11:37:58 Plugin 'configuration' enabled according profile (/etc/lynis/default.prfl)
2025-03-23 11:37:58 Plugin 'control-panels' enabled according profile (/etc/lynis/default.prfl)
2025-03-23 11:37:58 Plugin 'crypto' enabled according profile (/etc/lynis/default.prfl)
2025-03-23 11:37:58 Plugin 'dns' enabled according profile (/etc/lynis/default.prfl)
2025-03-23 11:37:58 Plugin 'docker' enabled according profile (/etc/lynis/default.prfl)
2025-03-23 11:37:58 Plugin 'file-integrity' enabled according profile (/etc/lynis/default.prfl)
2025-03-23 11:37:58 Plugin 'file-systems' enabled according profile (/etc/lynis/default.prfl)
2025-03-23 11:37:58 Plugin 'firewalls' enabled according profile (/etc/lynis/default.prfl)
2025-03-23 11:37:58 Plugin 'forensics' enabled according profile (/etc/lynis/default.prfl)
2025-03-23 11:37:58 Plugin 'hardware' enabled according profile (/etc/lynis/default.prfl)
2025-03-23 11:37:58 Plugin 'intrusion-detection' enabled according profile (/etc/lynis/default.prfl)
2025-03-23 11:37:58 Plugin 'intrusion-prevention' enabled according profile (/etc/lynis/default.prfl)
2025-03-23 11:37:58 Plugin 'kernel' enabled according profile (/etc/lynis/default.prfl)
2025-03-23 11:37:58 Plugin 'malware' enabled according profile (/etc/lynis/default.prfl)
2025-03-23 11:37:58 Plugin 'memory' enabled according profile (/etc/lynis/default.prfl)
2025-03-23 11:37:58 Plugin 'nginx' enabled according profile (/etc/lynis/default.prfl)
2025-03-23 11:37:58 Plugin 'pam' enabled according profile (/etc/lynis/default.prfl)
2025-03-23 11:37:58 Plugin 'processes' enabled according profile (/etc/lynis/default.prfl)
2025-03-23 11:37:58 Plugin 'security-modules' enabled according profile (/etc/lynis/default.prfl)
2025-03-23 11:37:58 Plugin 'software' enabled according profile (/etc/lynis/default.prfl)
```

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
```

```
litespeed@node190500-env-8796793-wp02-ter ~ $ uname -a
Linux node190500-env-8796793-wp02-ter.hidora.com 5.14.0 #1 SMP Wed Jul 12 12:00:44 MSK 2023 x86_64 x86_64 x86_64 GNU/Linux
litespeed@node190500-env-8796793-wp02-ter ~ $ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/ploop44045p1 94G  5.9G   84G   7% /
none            4.0M   0  4.0M   0% /sys/fs/cgroup
none            1.0G   0   1.0G   0% /dev
tmpfs            1.0G  532K   1.0G   1% /dev/shm
tmpfs            410M  108K   410M   1% /run
tmpfs            1.0M   0   1.0M   0% /run/credentials/systemd-sysctl.service
tmpfs            1.0M   0   1.0M   0% /run/credentials/systemd-tmpfiles-setup-dev.service
tmpfs            1.0M   0   1.0M   0% /run/credentials/systemd-tmpfiles-setup.service
litespeed@node190500-env-8796793-wp02-ter ~ $ free -h
              total        used        free      shared  buff/cache   available
Mem:           2.0Gi          245Mi        1.6Gi          35Mi         154Mi        1.8Gi
Swap:           1.0Gi           0B          1.0Gi
```

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;
```

```
MariaDB [(none)]> SELECT user, host, authentication_string, plugin FROM mysql.user;
+-----+-----+-----+-----+
| User | Host | authentication_string | plugin |
+-----+-----+-----+-----+
| mariadb.sys | localhost | *13309C5303A802810AE5EE330AFB228216222FBF | mysql_native_password |
| root | localhost | *13309C5303A802810AE5EE330AFB228216222FBF | mysql_native_password |
| mysql | localhost | *13309C5303A802810AE5EE330AFB228216222FBF | mysql_native_password |
| PUBLIC | | | |
| user-6981255 | % | *13309C5303A802810AE5EE330AFB228216222FBF | mysql_native_password |
| user-6981255 | localhost | *13309C5303A802810AE5EE330AFB228216222FBF | mysql_native_password |
| root | % | *13309C5303A802810AE5EE330AFB228216222FBF | mysql_native_password |
| root | 127.0.0.1 | *13309C5303A802810AE5EE330AFB228216222FBF | mysql_native_password |
+-----+-----+-----+-----+
8 rows in set (0.005 sec)
```

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.

```
litespeed@node190500-env-8796793-wp02-ter ~ $ ls -l /home/
total 4
drwxrwxrwx 1 root root 15 Mar 13 12:13 jelastic -> /home/litespeed
drwxr-xr-x 5 litespeed litespeed 4096 Mar 13 12:17 litespeed
```

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.

```
litespeed@node190500-env-8796793-wp02-ter ~ $ ls -l /var/www/
total 128
drwxr-xr-x 15 litespeed litespeed 4096 Mar 13 12:13 add-ons
drwxr-xr-x 10 litespeed litespeed 4096 Mar 13 12:13 admin
drwx----- 2 litespeed litespeed 4096 Mar 13 12:13 autoupdate
drwxr-xr-x 2 litespeed litespeed 4096 Mar 13 12:13 bin
lrwxrwxrwx 1 root root 13 Mar 13 12:13 BUILD -> ./BUILD.6.3.2
-rw-r--r-- 1 litespeed litespeed 2 Feb 19 08:09 BUILD.6.3.2
drwxr-xr-x 2 root root 4096 Oct 2 18:46 cgi-bin
drwxrwxr-x 5 litespeed litespeed 4096 Mar 20 08:00 conf
drwxr-xr-x 7 litespeed litespeed 4096 Mar 13 12:13 DEFAULT
drwxr-xr-x 4 litespeed litespeed 4096 Mar 13 12:13 docs
drwxr-x--x 2 litespeed litespeed 4096 Mar 19 14:17 extapp-sock
drwxr-xr-x 2 litespeed litespeed 4096 Mar 13 12:13 fcgi-bin
drwxr-xr-x 2 root root 4096 Oct 2 18:46 html
drwxr-xr-x 2 litespeed litespeed 4096 Feb 19 08:09 lib
-rw-r--r-- 1 litespeed litespeed 6926 Feb 19 08:09 LICENSEheaders + 65495 data
-rw----- 1 root root 256 Mar 20 08:00 license.key
-rw----- 1 root root 256 Mar 13 14:17 license.key.old
-rw-r--r-- 1 litespeed litespeed 2214 Feb 19 08:09 LICENSE.OpenLDAP
-rw-r--r-- 1 litespeed litespeed 6279 Feb 19 08:09 LICENSE.OpenSSL
-rw-r--r-- 1 litespeed litespeed 3208 Feb 19 08:09 LICENSE.PHP
drwxr-xr-x 2 litespeed litespeed 12288 Mar 19 15:36 logs
lrwxrwxrwx 1 root root 16 Mar 13 12:13 modules -> ./modules.6.3.2/
drwxr-xr-x 2 litespeed litespeed 4096 Mar 13 12:13 modules.6.3.2
drwx----- 2 litespeed litespeed 4096 Feb 19 08:09 phpbuild
-rw-r--r-- 1 root root 20 Mar 20 08:00 serial.no
drwxr-xr-x 3 litespeed litespeed 4096 Mar 13 12:13 share
drwxr-xr-x 2 litespeed litespeed 4096 Mar 19 10:21 ssl
```

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.

```
litespeed@node190500-env-8796793-wp02-ter ~ $ ls -l /var/log/
total 1692
-rw-rw-r-- 1 root root 12065 Mar 20 08:00 autoconfig.log
-rw-rw-r-- 1 root utmp 13440 Mar 19 16:13 bttmp
-rw-rw-r-- 1 root root 31009 Mar 20 11:01 cron
-rw-r--r-- 1 root root 168411 Mar 20 11:21 dnf.librepo.log
-rw-r--r-- 1 root root 427440 Mar 20 11:21 dnf.log
-rw-r--r-- 1 root root 63040 Mar 20 11:21 dnf.rpm.log
-rw-r--r-- 1 root root 3720 Mar 13 12:17 hawkey.log
drwx----- 2 root root 4096 Oct 2 18:53 httpd
-rw-rw-rw- 1 root root 28426 Mar 20 10:00 jem.log
drwxr-sr-x+ 3 root systemd-journal 4096 Mar 13 12:14 journal
-rw-rw-r-- 1 root utmp 290540 Mar 20 11:36 lastlog
-rw-rw-rw- 1 root root 0 Mar 20 08:00 launcher.log
drwxr-xr-x 2 root root 4096 Mar 19 10:20 letsencrypt
-rw-r--r-- 1 root root 8164 Mar 20 10:00 letsencrypt.log
lrwxrwxrwx 1 root root 14 Mar 13 12:13 litespeed -> /var/www/logs/
drwxr-xr-x 2 root root 4096 Nov 15 15:24 mail
-rw-rw-r-- 1 root root 1430 Mar 17 14:21 maillog
-rw-rw-r-- 1 root root 473415 Mar 20 11:37 messages
-rw-r--r-- 1 root root 5869 Mar 19 10:17 mysqlresetpas.log
drwxrwxr-x+ 2 lsadm mysql 4096 Mar 13 12:13 mysql
drwx----- 2 root root 4096 Nov 15 15:23 private
lrwxrwxrwx 1 root root 39 Nov 19 09:08 README -> ../../usr/share/doc/systemd/README.logs
drwxrwx+ 2 redis mysql 4096 Mar 13 12:14 redis
-rw-rw-rw- 1 root root 30553 Mar 20 08:00 run.log
-rw-rw-r-- 1 root root 83418 Mar 20 11:36 secure
-rw-rw-r-- 1 root root 0 Nov 15 15:24 spooler
-rw-rw-r-- 1 root root 0 Nov 15 15:23 tallylog
-rw-rw-r-- 1 root utmp 8832 Mar 20 11:36 wtmp
```

```
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/


```

litespeed@node190500-env-8796793-wp02-ter ~ $ ls -l /var/www/
total 128
drwxr-xr-x 15 litespeed litespeed 4096 Mar 13 12:13 add-ons
drwxr-xr-x 10 litespeed litespeed 4096 Mar 13 12:13 admin
drwx----- 2 litespeed litespeed 4096 Mar 13 12:13 autoupdate
drwxr-xr-x 2 litespeed litespeed 4096 Mar 13 12:13 bin
lrwxrwxrwx 1 root root 25 Mar 13 12:13 BUILD -> ./BUILD.6.3.2
-rw-r--r-- 1 litespeed litespeed 2 Feb 19 08:09 BUILD.6.3.2
drwxr-xr-x 2 root root 4096 Oct 2 18:46 cgi-bin
drwxrwxr-x 5 litespeed litespeed 4096 Mar 21 08:00 conf
drwxr-xr-x 7 litespeed litespeed 4096 Mar 13 12:13 DEFAULT
drwxr-xr-x 4 litespeed litespeed 4096 Mar 13 12:13 docs
drwxr-x--x 2 litespeed litespeed 4096 Mar 19 14:17 extapp-sock
drwxr-xr-x 2 litespeed litespeed 4096 Mar 13 12:13 fcgi-bin
drwxr-xr-x 2 root root 4096 Oct 2 18:46 html
drwxr-xr-x 2 litespeed litespeed 4096 Feb 19 08:09 lib
-rw-r--r-- 1 litespeed litespeed 6926 Feb 19 08:09 LICENSE
-rw----- 1 root litespeed 256 Mar 21 08:00 license.key
-rw----- 1 root litespeed 256 Mar 13 14:17 license.key.old
-rw-r--r-- 1 litespeed litespeed 2214 Feb 19 08:09 LICENSE.OpenLDAP
-rw-r--r-- 1 litespeed litespeed 6279 Feb 19 08:09 LICENSE.OpenSSL
-rw-r--r-- 1 litespeed litespeed 3208 Feb 19 08:09 LICENSE.PHP
drwxr-xr-x 2 litespeed litespeed 12288 Mar 21 12:27 logs
lrwxrwxrwx 1 root root 4096 Mar 13 12:13 modules -> ./modules.6.3.2/
drwxr-xr-x 2 litespeed litespeed 4096 Mar 13 12:13 modules.6.3.2
drwx----- 2 litespeed litespeed 4096 Feb 19 08:09 phpbuild
-rw-r--r-- 1 root root 1.0M Mar 21 08:00 serial.no
drwxr-xr-x 3 litespeed litespeed 4096 Mar 13 12:13 share
drwxr-xr-x 2 litespeed litespeed 4096 Mar 19 10:21 ssl
drwx----- 3 litespeed litespeed 4096 Mar 13 12:15 tmp
-rw-r--r-- 1 litespeed litespeed 6 Feb 19 08:09 VERSION
drwxr-xr-x 4 litespeed litespeed 4096 Mar 13 12:15 webroot

```

```

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
```

```
litespeed@node190500-env-8796793-wp02-ter ~ $ cat /etc/pam.d/system-auth | grep pam_pwquality
password requisite pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
```

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
```

```
litespeed@node190500-env-8796793-wp02-ter ~ $ cat /etc/pam.d/system-auth | grep pam_pwquality
password requisite pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
litespeed@node190500-env-8796793-wp02-ter ~ $ sudo nano /etc/pam.d/system-auth
litespeed@node190500-env-8796793-wp02-ter ~ $ cat /etc/pam.d/system-auth | grep pam_pwquality
password requisite pam_pwquality.so try_first_pass local_users_only retry=3 minlen=12 minclass=4 difok=3
```

Vérification du processus de sauvegarde et restauration

```
litespeed@node190500-env-8796793-wp02-ter ~ $ sudo find /var -type f -name "*.tar"
litespeed@node190500-env-8796793-wp02-ter ~ $ sudo find / -path /proc -prune -o -type f -name "*.tar" -print
litespeed@node190500-env-8796793-wp02-ter ~ $ ls
bin
litespeed@node190500-env-8796793-wp02-ter ~ $ ls /var/www
add-ons      bin          cgi-bin      docs          html          license.key  LICENSE.OpenSSL  modules      serial.no  tmp
admin        BUILD        conf         extapp-sock  lib           license.key.old  LICENSE.PHP      modules.6.3.2  share      VERSION
autoupdate   BUILD.6.3.2  DEFAULT     fcgi-bin     LICENSE       LICENSE.OpenLDAP  logs            phpbuild     ssl        webroot
litespeed@node190500-env-8796793-wp02-ter ~ $ cat /etc/crontab
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root

# For details see man 4 crontabs

# Example of job definition:
# ._____ minute (0 - 59)
# | ._____ hour (0 - 23)
# | | ._____ day of month (1 - 31)
# | | | ._____ month (1 - 12) OR jan,feb,mar,apr ...
# | | | | ._____ day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# * * * * * user-name  command to be executed
```

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
```