

Projet CMS HUGO LEMP

Créé le : 26/09/2023

Modifié le : 02/10/2023

Auteur : LACOMME Ethan

SIDIBE Demba



Table des matières

Recherches – partie 1	3
Installation du serveur Debian12 avec HUGO	8
Recherches – partie 2	14
Installation wordpress	15
Recherches – partie 3	21

Recherches – partie 1

Le rôle du logiciel Jekyll avec ses avantages/inconvénients.

Eleventy, Gatsby et Hugo sont tous des générateurs de site statique qui permettent de créer des sites web sans base de données ni serveur d'application. Cependant, ils présentent des différences en termes de fonctionnalités, d'avantages et d'inconvénients. Voici un aperçu de chacun, suivi d'une comparaison avec Hugo :

Eleventy :

Rôle : Eleventy est un générateur de site statique qui transforme le contenu écrit en Markdown, HTML, JavaScript ou d'autres langages en un site web statique.

Avantages :

1. **Flexibilité :** Eleventy est très flexible et permet aux développeurs de choisir leurs propres outils, templates et structures de dossier, ce qui en fait un choix idéal pour les projets personnalisés.
2. **Performance :** Les sites générés par Eleventy sont rapides, car ils sont statiques par nature et ne nécessitent pas de traitement côté serveur.
3. **Simplicité :** Il est relativement simple à prendre en main, en particulier pour ceux qui sont familiers avec les technologies web de base.

Inconvénients :

1. **Courbe d'apprentissage :** Bien qu'il soit plus simple que certains autres générateurs de site statique, Eleventy peut quand même nécessiter un temps d'apprentissage pour maîtriser toutes ses fonctionnalités.

Gatsby :

Rôle : Gatsby est un générateur de site statique qui se concentre sur la création de sites web modernes et dynamiques en utilisant React et GraphQL.

Avantages :

1. **Performance :** Gatsby offre des performances exceptionnelles grâce à son approche de préchargement des données et à son utilisation de la technologie Progressive Web App (PWA).
2. **Grande communauté :** Gatsby dispose d'une communauté active et d'une vaste bibliothèque de plugins, ce qui facilite l'ajout de fonctionnalités à votre site.
3. **Facilité d'intégration :** Gatsby permet d'intégrer des sources de données externes telles que des API REST, des bases de données ou des CMS headless.

Inconvénients :

1. **Complexité :** En raison de sa complexité, Gatsby peut nécessiter une courbe d'apprentissage plus longue, en particulier si vous n'êtes pas déjà familier avec React et GraphQL.

Hugo :

Rôle : Hugo est également un générateur de site statique qui transforme le contenu Markdown en un site web statique.

Avantages :

1. **Performance :** Les sites générés par Hugo sont extrêmement rapides, car il est écrit en Go, un langage de programmation très performant.
2. **Facilité d'utilisation :** Hugo est connu pour sa simplicité d'installation et d'utilisation, ce qui en fait un excellent choix pour les débutants.
3. **Performance :** Hugo offre d'excellentes performances grâce à sa vitesse de génération élevée.

Inconvénients :

1. **Moins de flexibilité :** Hugo peut être moins flexible que certains autres générateurs de site statique en ce qui concerne la personnalisation avancée, en particulier pour les projets très personnalisés.

Comparaison :

- **Flexibilité :** Eleventy est le plus flexible des trois, suivi de près par Hugo, tandis que Gatsby a tendance à imposer plus de structure et de conventions.
- **Performance :** Tous les générateurs offrent de bonnes performances, mais Hugo est généralement reconnu comme étant le plus rapide en raison de sa base en Go.
- **Complexité :** Gatsby peut être plus complexe en raison de son utilisation de React et de GraphQL, tandis qu'Eleventy et Hugo sont plus simples à prendre en main.
- **Écosystème :** Gatsby dispose d'une vaste communauté et de nombreuses ressources, tandis qu'Eleventy et Hugo ont des communautés plus petites mais actives.

Le rôle de ces logiciels Eleventy et Gatsby avec leurs avantages/inconvénients puis comparez-les avec le logiciel retenu HUGO.

Eleventy, Gatsby et Hugo sont tous des générateurs de site statique qui permettent de créer des sites web sans base de données ni serveur d'application. Cependant, ils présentent des différences en termes de fonctionnalités, d'avantages et d'inconvénients. Voici un aperçu de chacun, suivi d'une comparaison avec Hugo :

Eleventy :

Rôle : Eleventy est un générateur de site statique qui transforme le contenu écrit en Markdown, HTML, JavaScript ou d'autres langages en un site web statique.

Avantages :

1. **Flexibilité :** Eleventy est très flexible et permet aux développeurs de choisir leurs propres outils, templates et structures de dossier, ce qui en fait un choix idéal pour les projets personnalisés.
2. **Performance :** Les sites générés par Eleventy sont rapides, car ils sont statiques par nature et ne nécessitent pas de traitement côté serveur.
3. **Simplicité :** Il est relativement simple à prendre en main, en particulier pour ceux qui sont familiers avec les technologies web de base.

Inconvénients :

1. **Courbe d'apprentissage :** Bien qu'il soit plus simple que certains autres générateurs de site statique, Eleventy peut quand même nécessiter un temps d'apprentissage pour maîtriser toutes ses fonctionnalités.

Gatsby :

Rôle : Gatsby est un générateur de site statique qui se concentre sur la création de sites web modernes et dynamiques en utilisant React et GraphQL.

Avantages :

1. **Performance :** Gatsby offre des performances exceptionnelles grâce à son approche de préchargement des données et à son utilisation de la technologie Progressive Web App (PWA).
2. **Grande communauté :** Gatsby dispose d'une communauté active et d'une vaste bibliothèque de plugins, ce qui facilite l'ajout de fonctionnalités à votre site.
3. **Facilité d'intégration :** Gatsby permet d'intégrer des sources de données externes telles que des API REST, des bases de données ou des CMS headless.

Inconvénients :

1. **Complexité :** En raison de sa complexité, Gatsby peut nécessiter une courbe d'apprentissage plus longue, en particulier si vous n'êtes pas déjà familier avec React et GraphQL.

Hugo :

Rôle : Hugo est également un générateur de site statique qui transforme le contenu Markdown en un site web statique.

Avantages :

1. **Performance :** Les sites générés par Hugo sont extrêmement rapides, car il est écrit en Go, un langage de programmation très performant.
2. **Facilité d'utilisation :** Hugo est connu pour sa simplicité d'installation et d'utilisation, ce qui en fait un excellent choix pour les débutants.
3. **Performance :** Hugo offre d'excellentes performances grâce à sa vitesse de génération élevée.

Inconvénients :

1. **Moins de flexibilité :** Hugo peut être moins flexible que certains autres générateurs de site statique en ce qui concerne la personnalisation avancée, en particulier pour les projets très personnalisés.

Comparaison :

- **Flexibilité :** Eleventy est le plus flexible des trois, suivi de près par Hugo, tandis que Gatsby a tendance à imposer plus de structure et de conventions.
- **Performance :** Tous les générateurs offrent de bonnes performances, mais Hugo est généralement reconnu comme étant le plus rapide en raison de sa base en Go.
- **Complexité :** Gatsby peut être plus complexe en raison de son utilisation de React et de GraphQL, tandis qu'Eleventy et Hugo sont plus simples à prendre en main.
- **Écosystème :** Gatsby dispose d'une vaste communauté et de nombreuses ressources, tandis qu'Eleventy et Hugo ont des communautés plus petites mais actives.

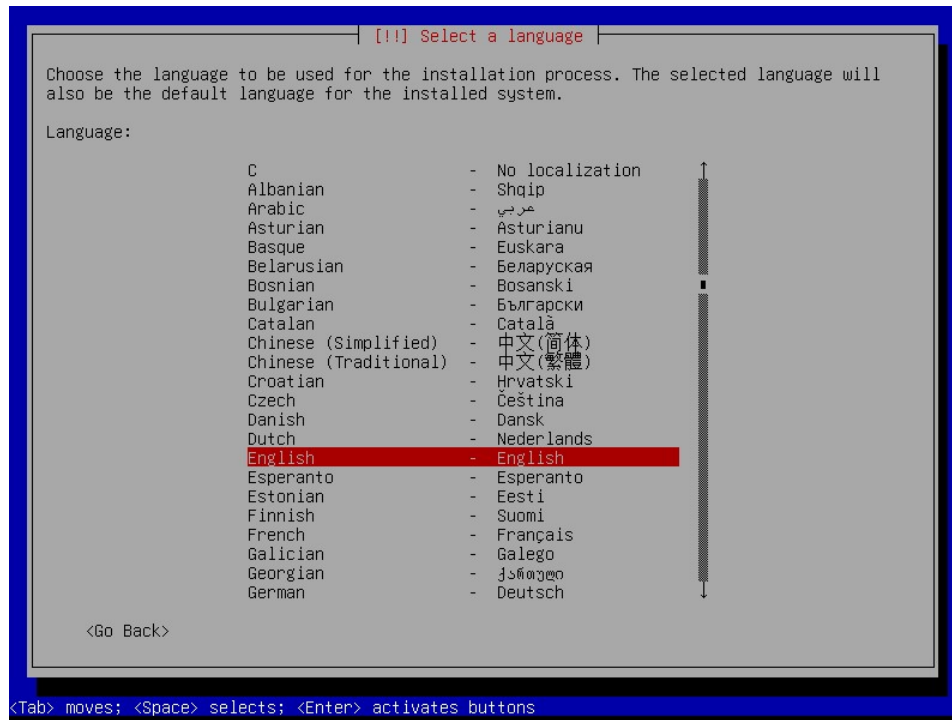
Pourquoi c'est le logiciel HUGO qui a été retenu plutôt que Eleventy ou Gatsby ?

Le choix entre Hugo, Eleventy et Gatsby dépend généralement de plusieurs facteurs, notamment les compétences de l'équipe, la complexité du projet, les exigences en matière de performance, et les préférences personnelles. Voici quelques raisons possibles pour lesquelles Hugo pourrait être préféré à Eleventy ou Gatsby :

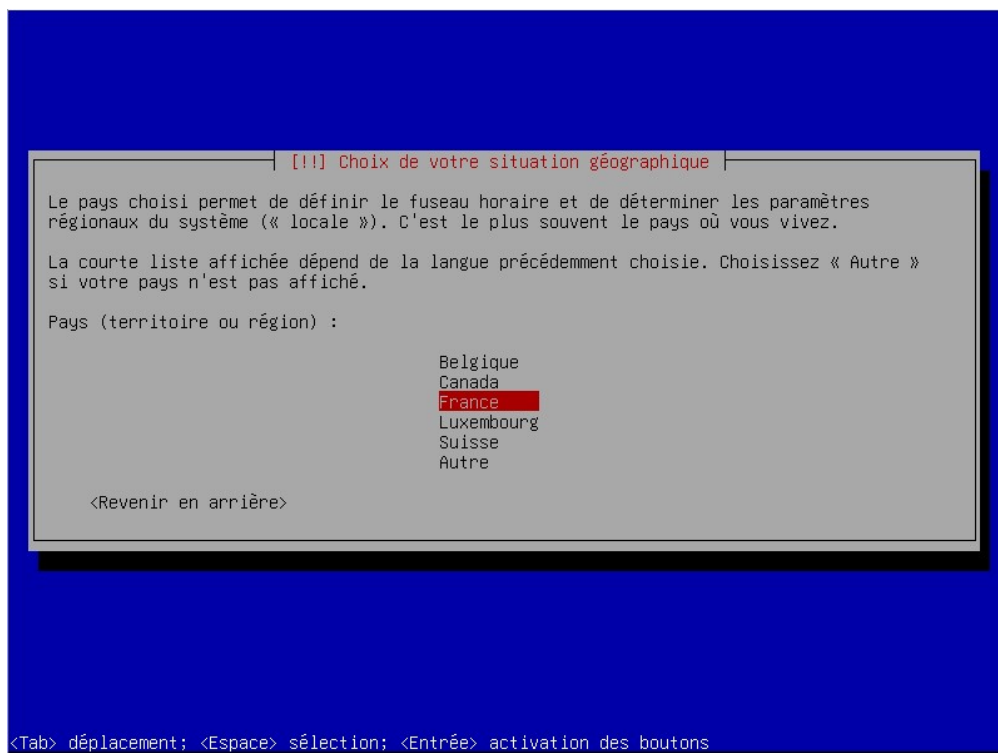
1. **Performance** : Hugo est reconnu pour sa rapidité de génération de sites, en grande partie grâce à sa mise en œuvre en Go. Si les performances sont une priorité pour le projet, Hugo pourrait être le choix logique.
2. **Facilité d'utilisation** : Hugo est souvent considéré comme l'un des générateurs de site statique les plus simples à utiliser, ce qui en fait un bon choix pour les débutants ou les projets où la simplicité est essentielle.
3. **Compétences de l'équipe** : Si l'équipe de développement possède déjà des compétences en Go ou est plus à l'aise avec ce langage, cela pourrait influencer le choix en faveur de Hugo.
4. **Besoins de personnalisation** : Si le projet exige une personnalisation avancée et que Hugo offre suffisamment de flexibilité pour répondre à ces besoins, il pourrait être préféré à Eleventy ou Gatsby.
5. **Communauté et documentation** : La disponibilité de ressources, de plugins et de documentation pour Hugo peut également influencer le choix, en particulier si le projet doit être développé rapidement.
6. **Hébergement** : Le choix de la plateforme d'hébergement peut également jouer un rôle. Par exemple, si l'équipe prévoit d'héberger le site sur Netlify, qui prend en charge Hugo de manière native, cela pourrait favoriser Hugo.
7. **Préférences personnelles** : Parfois, le choix d'un générateur de site statique est basé sur les préférences personnelles de l'équipe de développement ou du développeur principal.

Installation du serveur Debian12 avec HUGO

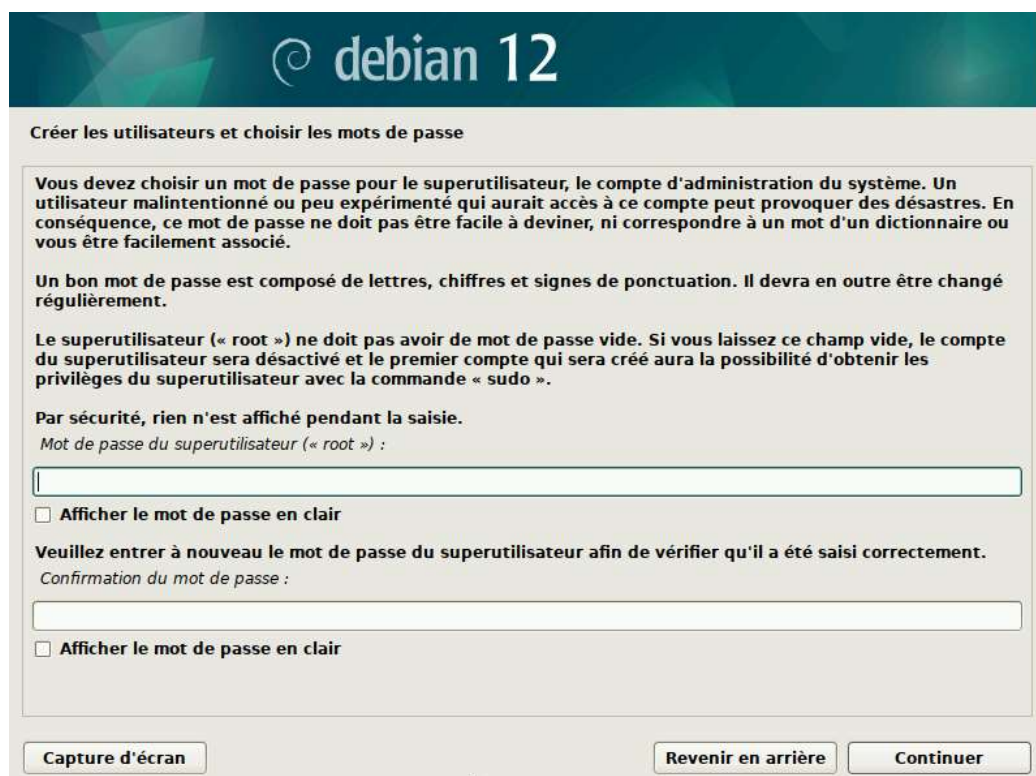
1^{ère} étape : On choisit la langue « Français »



2^{ème} étape : On choisit la situation géographique « France »



3^{ème} étape : On créer un utilisateur avec un mot de passe



Créer les utilisateurs et choisir les mots de passe

Vous devez choisir un mot de passe pour le superutilisateur, le compte d'administration du système. Un utilisateur malintentionné ou peu expérimenté qui aurait accès à ce compte peut provoquer des désastres. En conséquence, ce mot de passe ne doit pas être facile à deviner, ni correspondre à un mot d'un dictionnaire ou vous être facilement associé.

Un bon mot de passe est composé de lettres, chiffres et signes de ponctuation. Il devra en outre être changé régulièrement.

Le superutilisateur (« root ») ne doit pas avoir de mot de passe vide. Si vous laissez ce champ vide, le compte du superutilisateur sera désactivé et le premier compte qui sera créé aura la possibilité d'obtenir les privilèges du superutilisateur avec la commande « sudo ».

Par sécurité, rien n'est affiché pendant la saisie.

Mot de passe du superutilisateur (« root ») :

☐ Afficher le mot de passe en clair

Veillez entrer à nouveau le mot de passe du superutilisateur afin de vérifier qu'il a été saisi correctement.

Confirmation du mot de passe :

☐ Afficher le mot de passe en clair

Capture d'écran Revenir en arrière Continuer

4^{ème} étape : On créer un utilisateur



Créer les utilisateurs et choisir les mots de passe


Un compte d'utilisateur va être créé afin que vous puissiez disposer d'un compte différent de celui du superutilisateur (« root »), pour l'utilisation courante du système.

Veillez indiquer le nom complet du nouvel utilisateur. Cette information servira par exemple dans l'adresse d'origine des courriels émis ainsi que dans tout programme qui affiche ou se sert du nom complet. Votre propre nom est un bon choix.

Nom complet du nouvel utilisateur :

Capture d'écran Revenir en arrière Continuer

5^{ème} étape : On choisit un mot de passe



Créer les utilisateurs et choisir les mots de passe

Un bon mot de passe est composé de lettres, chiffres et signes de ponctuation. Il devra en outre être changé régulièrement.

Mot de passe pour le nouvel utilisateur :

●●●●●●●●

☐ Afficher le mot de passe en clair

Veuillez entrer à nouveau le mot de passe pour l'utilisateur, afin de vérifier que votre saisie est correcte.

Confirmation du mot de passe :

●●●●●●●●

☐ Afficher le mot de passe en clair

Capture d'écran

Revenir en arrière

Continuer

6^{ème} étape : On utilise le disque entier



Partitionner les disques

Le programme d'installation peut vous assister pour le partitionnement d'un disque (avec plusieurs choix d'organisation). Vous pouvez également effectuer ce partitionnement vous-même. Si vous choisissez le partitionnement assisté, vous aurez la possibilité de vérifier et personnaliser les choix effectués.

Si vous choisissez le partitionnement assisté pour un disque complet, vous devrez ensuite choisir le disque à partitionner.

Méthode de partitionnement :

- Assisté - utiliser un disque entier
- Assisté - utiliser tout un disque avec LVM
- Assisté - utiliser tout un disque avec LVM chiffré
- Manuel

Capture d'écran

Revenir en arrière

Continuer

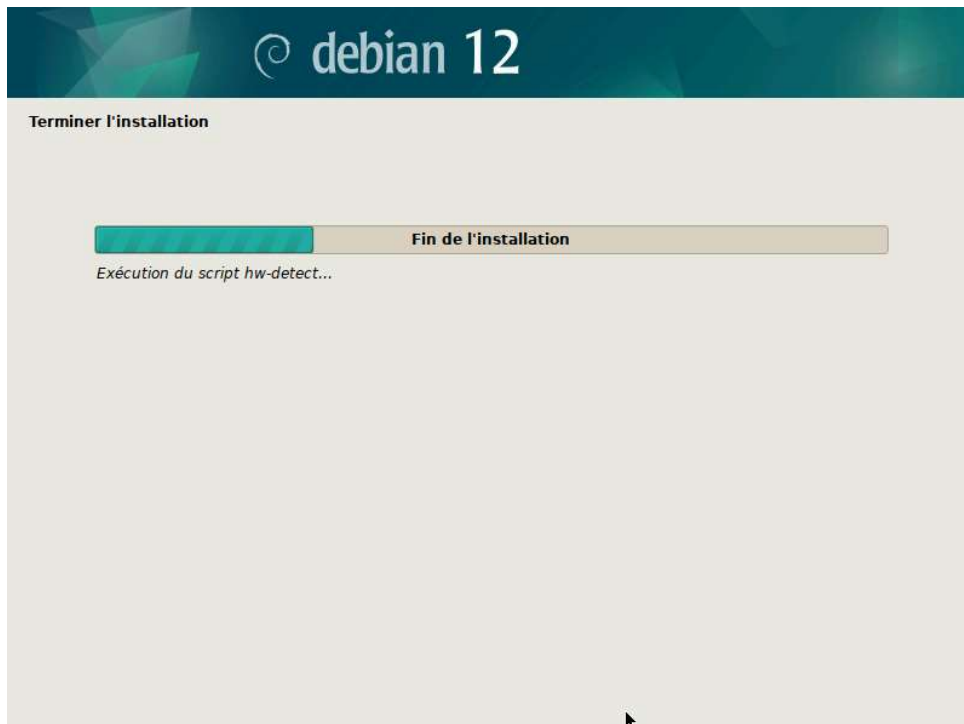
Configuration en cours



7^{ème} étape : On coche « Serveur web » et « Serveur SSH »



Finalisation du la machine Debian



4)Une fois que la machine debian12 est installé on installe le serveur hugo avec la commande :

Apt install hugo -y hugo

```
root@debian:~# apt install hugo -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
hugo est déjà la version la plus récente (0.111.3-1).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
```

Ensuite on va créer un site nommé « tp »

```
root@debian:~# hugo new site Tp
Congratulations! Your new Hugo site is created in /root/Tp.

Just a few more steps and you're ready to go:

1. Download a theme into the same-named folder.
   Choose a theme from https://themes.gohugo.io/ or
   create your own with the "hugo new theme <THEMENAME>" command.
2. Perhaps you want to add some content. You can add single files
   with "hugo new <SECTIONNAME>/<FILENAME>.<FORMAT>".
3. Start the built-in live server via "hugo server".
```


On a été sur le git pour récupérer un thème

```
root@debian:~/Tp# git init
astuce: Utilisation de 'master' comme nom de la branche initiale. Le nom de la branche
astuce: par défaut peut changer. Pour configurer le nom de la branche initiale
astuce: pour tous les nouveaux dépôts, et supprimer cet avertissement, lancez :
astuce:
astuce:     git config --global init.defaultBranch <nom>
astuce:
astuce: Les noms les plus utilisés à la place de 'master' sont 'main', 'trunk' et
astuce: 'development'. La branche nouvellement créée peut être renommée avec :
astuce:
astuce:     git branch -m <nom>
Dépôt Git vide initialisé dans /root/Tp/.git/
root@debian:~/Tp# git submodule add https://github.com/undus5/hugo-pure themes/hugo-pure
Clonage dans '/root/Tp/themes/hugo-pure'...
remote: Enumerating objects: 202, done.
remote: Counting objects: 100% (202/202), done.
remote: Compressing objects: 100% (128/128), done.
remote: Total 202 (delta 72), reused 178 (delta 50), pack-reused 0
Réception d'objets: 100% (202/202), 512.63 Kio | 6.03 Mio/s, fait.
Résolution des deltas: 100% (72/72), fait.
```

```
root@debian:~/Tp# git submodule add https://github.com/undus5/hugo-pure themes/hugo-pure
Clonage dans '/root/Tp/themes/hugo-pure'...
remote: Enumerating objects: 202, done.
remote: Counting objects: 100% (202/202), done.
remote: Compressing objects: 100% (128/128), done.
remote: Total 202 (delta 72), reused 178 (delta 50), pack-reused 0
Réception d'objets: 100% (202/202), 512.63 Kio | 6.03 Mio/s, fait.
Résolution des deltas: 100% (72/72), fait.
root@debian:~/Tp# dir
archetypes  assets      config.toml content     data       layouts    public     static     themes
root@debian:~/Tp# echo "theme = 'hugo-pure'" >> config.toml
```

Puis on tape « hugo server »

```
root@debian:~/Tp# hugo server
Start building sites ...
hugo v0.111.3+extended linux/amd64 BuildDate=2023-03-16T08:41:31Z VendorInfo=debian:0.111.3-1

| EN
-----|-----
Pages           | 10
Paginator pages | 0
Non-page files  | 0
Static files    | 7
Processed images| 0
Aliases         | 1
Sitemaps        | 1
Cleaned         | 0

Built in 37 ms
Watching for changes in /root/Tp/{archetypes,assets,content,data,layouts,static,themes}
Watching for config changes in /root/Tp/config.toml, /root/Tp/themes/hugo-pure/config.toml
Environment: "development"
Serving pages from memory
Running in Fast Render Mode. For full rebuilds on change: hugo server --disableFastRender
Web Server is available at http://localhost:1313/ (bind address 127.0.0.1)
Press Ctrl+C to stop
```

On a configuré l'ip et l'adresse du site

```
root@debian:~/Tp# hugo server --bind=172.20.33.50 --baseURL=http://172.20.33.50 --port=1313
Start building sites ...
hugo v0.111.3+extended linux/amd64 BuildDate=2023-03-16T08:41:31Z VendorInfo=debian:0.111.3-1
```

Et on a accès au site depuis son adresse

← → ↻ ⚠ Non sécurisé | 172.20.33.50:1313

Home Posts

hugo-pure

Dark mode support (auto switch).



Recherches – partie 2

6) Une infrastructure LEMP est un ensemble de logiciels pour héberger des sites web dynamiques

Une infrastructure LEMP est en effet un ensemble de logiciels souvent utilisé pour héberger des sites web dynamiques. Le terme "LEMP" est un acronyme qui représente les composants principaux de cette infrastructure :

1. **Linux** : C'est le système d'exploitation sur lequel l'ensemble de l'infrastructure repose. Linux est un choix courant en raison de sa stabilité, de sa sécurité et de sa flexibilité.
2. **Nginx** : Nginx (prononcé "Engine-X") est un serveur web réputé pour sa haute performance et sa capacité à gérer de nombreuses connexions simultanées. Il est souvent utilisé en tant que serveur web frontal dans une infrastructure LEMP pour traiter les requêtes HTTP des clients.
3. **MySQL** : MySQL est un système de gestion de base de données relationnelle (RDBMS) largement utilisé dans le cadre du développement web. Il stocke les données nécessaires pour les sites web dynamiques, tels que les informations des utilisateurs, les articles de blog, etc.
4. **PHP** : PHP est un langage de script côté serveur qui est couramment utilisé pour créer des sites web dynamiques. Il permet de générer du contenu web à la volée en interagissant avec la base de données (MySQL) et en générant des pages web en fonction des demandes des utilisateurs.

7) Avantages de Nginx par rapport à Apache inconvénients.

Voici quelques-uns des avantages de Nginx par rapport à Apache :

-
1. **Performance** : Nginx est largement reconnu pour ses performances élevées. Il est conçu pour gérer efficacement un grand nombre de connexions simultanées avec une faible utilisation des ressources système. Cela en fait un choix idéal pour les sites web à fort trafic.
 2. **Modèle asynchrone** : Nginx utilise un modèle de traitement asynchrone et événementiel, ce qui signifie qu'il peut gérer plusieurs requêtes en même temps sans créer un nouveau processus ou un nouveau thread pour chaque connexion. Cela réduit la surcharge du système et améliore la réactivité du serveur.
 3. **Faible consommation de mémoire** : En raison de son architecture légère, Nginx utilise généralement moins de mémoire qu'Apache pour gérer un nombre donné de connexions. Cela le rend efficace pour les serveurs avec des ressources limitées.
 4. **Proxy inverse et équilibrage de charge** : Nginx excelle dans la configuration de proxy inverse et l'équilibrage de charge, ce qui en fait un choix courant pour la mise en cache de contenu statique et la répartition de charge entre plusieurs serveurs d'application en aval.
 5. **Configuration modulaire simple** : La configuration de Nginx est basée sur des fichiers de configuration simples et compréhensibles. Il est relativement facile de comprendre et de gérer les directives de configuration, ce qui facilite la personnalisation.
 6. **Gestion des connexions** : Nginx est capable de gérer efficacement les connexions lentes ou suspendues sans surcharger le serveur, ce qui améliore la robustesse face aux attaques DDoS et aux situations de surcharge.
 7. **Support HTTP/2 et HTTPS** : Nginx offre un support intégré pour le protocole HTTP/2, ce qui améliore la vitesse de chargement des sites web. Il prend également en charge HTTPS grâce à l'intégration de certificats SSL/TLS.
 8. **Redirections et réécriture d'URL** : La configuration de redirections et de réécriture d'URL est relativement simple avec Nginx, ce qui est utile pour optimiser la structure des URL de votre site web.

Installation wordpress

8) pour installer wordpress sur debian on va dans /tmp pour l'installer

```
cd /tmp
```

```
wget https://wordpress.org/latest.zip
```



```

root@debian:~# cd /tmp
root@debian:/tmp# wget https://wordpress.org/latest.zip
--2023-10-09 08:20:46-- https://wordpress.org/latest.zip
Résolution de wordpress.org (wordpress.org)... 198.143.164.252
Connexion à wordpress.org (wordpress.org)[198.143.164.252]:443... connecté.
requête HTTP transmise, en attente de la réponse... 200 OK
Taille : 24938800 (24M) [application/zip]
Sauvegarde en : « latest.zip »

latest.zip          100%[=====>] 23,78M  16,0MB/s  ds 1,5s
2023-10-09 08:20:48 (16,0 MB/s) - « latest.zip » sauvegardé [24938800/24938800]

root@debian:/tmp# dir
latest.zip
systemd-private-37235a0251a54870ae7a637efbc5921f-apache2.service-FMvIyl
systemd-private-37235a0251a54870ae7a637efbc5921f-systemd-logind.service-W0T2jM
systemd-private-37235a0251a54870ae7a637efbc5921f-systemd-timesyncd.service-1XQbwE

```

Ensuite il faut créer sa base de données

mysql -u root -p

root

```

root@debian:/tmp# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.3-MariaDB-1 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>


```

CREATE DATABASE wpsite;

```

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| sys |
| wpsite |
+-----+
5 rows in set (0,011 sec)

```



CREATE USER 'adminwp'@'localhost' IDENTIFIED BY 'root';

```

MariaDB [(none)]> create user 'adminwp'@'localhost' identified by 'root';
Query OK, 0 rows affected (0,003 sec)

```

On lui met tous les privilèges sur cette BD

GRANT ALL PRIVILEGES ON wpsite.* TO adminwp@localhost;

```
MariaDB [(none)]> Grant all privileges on wpsite.* to adminwp@localhost;  
Query OK, 0 rows affected (0,011 sec)
```

Il faut actualiser les droits avant de quitter

```
MariaDB [(none)]> flush privileges;  
Query OK, 0 rows affected (0,000 sec)  
  
MariaDB [(none)]> exit  
Bye  
root@debian:/tmp#
```

Il faut maintenant décompresser wordpress

rm /var/www/html/index.html

Apt update && apt upgrade -y

Apt install zip

unzip latest.zip -d /var/www/html

cd /var/www/html

mv wordpress/* /var/www/html/

rm wordpress/ -Rf

chown -R www-data:www-data /var/www/html/

```
root@debian:/var/www/html# mv wordpress/* /var/www/html/  
root@debian:/var/www/html# rm wordpress/ -Rf  
root@debian:/var/www/html# shown -R www-data:www-data /var/www/html/  
-bash: shown : commande introuvable  
root@debian:/var/www/html# chown -R www-data:www-data /var/www/html/
```

Avant il faut installer php et redémarrer apache

Puis se connecter à l'ip de la machine



English (United States)

Afrikaans

አማርኛ

Aragonés

العربية

العربية المغربية

অসমীয়া

گۆنئی آذربایجان

Azərbaycan dili

Беларуская мова

Български

বাংলা

සිංහල

Bosanski

Català

Cebuano

Čeština

Cymraeg

Dansk

Deutsch (Österreich)

Deutsch (Schweiz)

Deutsch (Sie)

Continue



Vous devez saisir ci-dessous les détails de connexion à votre base de données. Si vous ne les connaissez pas, contactez votre hébergeur.

Nom de la base de données

wpsite

Le nom de la base de données avec laquelle vous souhaitez utiliser WordPress.

Identifiant

adminwp

Votre identifiant MySQL.

Mot de passe

root

Hide

Votre mot de passe de base de données.

Adresse de la base de données

localhost

Si localhost ne fonctionne pas, demandez cette information à l'hébergeur de votre site.

Préfixe des tables

wp_

Si vous souhaitez faire tourner plusieurs installations de WordPress sur une même base de données, modifiez ce réglage.

Envoyer



C'est parfait ! Vous avez passé la première partie de l'installation. WordPress peut désormais communiquer avec votre base de données. Préparez-vous, il est maintenant temps de...

Lancer l'installation

Bienvenue

Bienvenue dans la très célèbre installation en 5 minutes de WordPress ! Vous n'avez qu'à remplir les informations demandées ci-dessous et vous serez prêt à utiliser la plus extensible et puissante plateforme de publication de contenu au monde.

Informations nécessaires

Veuillez renseigner les informations suivantes. Ne vous inquiétez pas, vous pourrez les modifier plus tard.

Titre du site

Identifiant

Les identifiants ne peuvent utiliser que des caractères alphanumériques, des espaces, des tirets bas ("_"), des traits d'union ("-"), des points et le symbole @.

Mot de passe [Masquer](#)
Very weak

Important : Vous aurez besoin de ce mot de passe pour vous connecter. Pensez à le stocker dans un lieu sûr.

Confirmer le mot de passe ☒ Confirmer l'utilisation du mot de passe faible

Votre e-mail

Vérifiez bien cette adresse e-mail avant de continuer.

Visibilité par les moteurs de recherche ☐ Demander aux moteurs de recherche de ne pas indexer ce site
Certains moteurs de recherche peuvent décider de l'indexer malgré tout.

Installer WordPress



Quel succès !

WordPress est installé. Merci et profitez bien !

Identifiant adminwp

Mot de passe *Le mot de passe que vous avez choisi.*

[Se connecter](#)



Erreur : l'identifiant **wpadmin** n'est pas inscrit sur ce site. Si vous doutez de votre identifiant, essayez plutôt votre adresse e-mail.

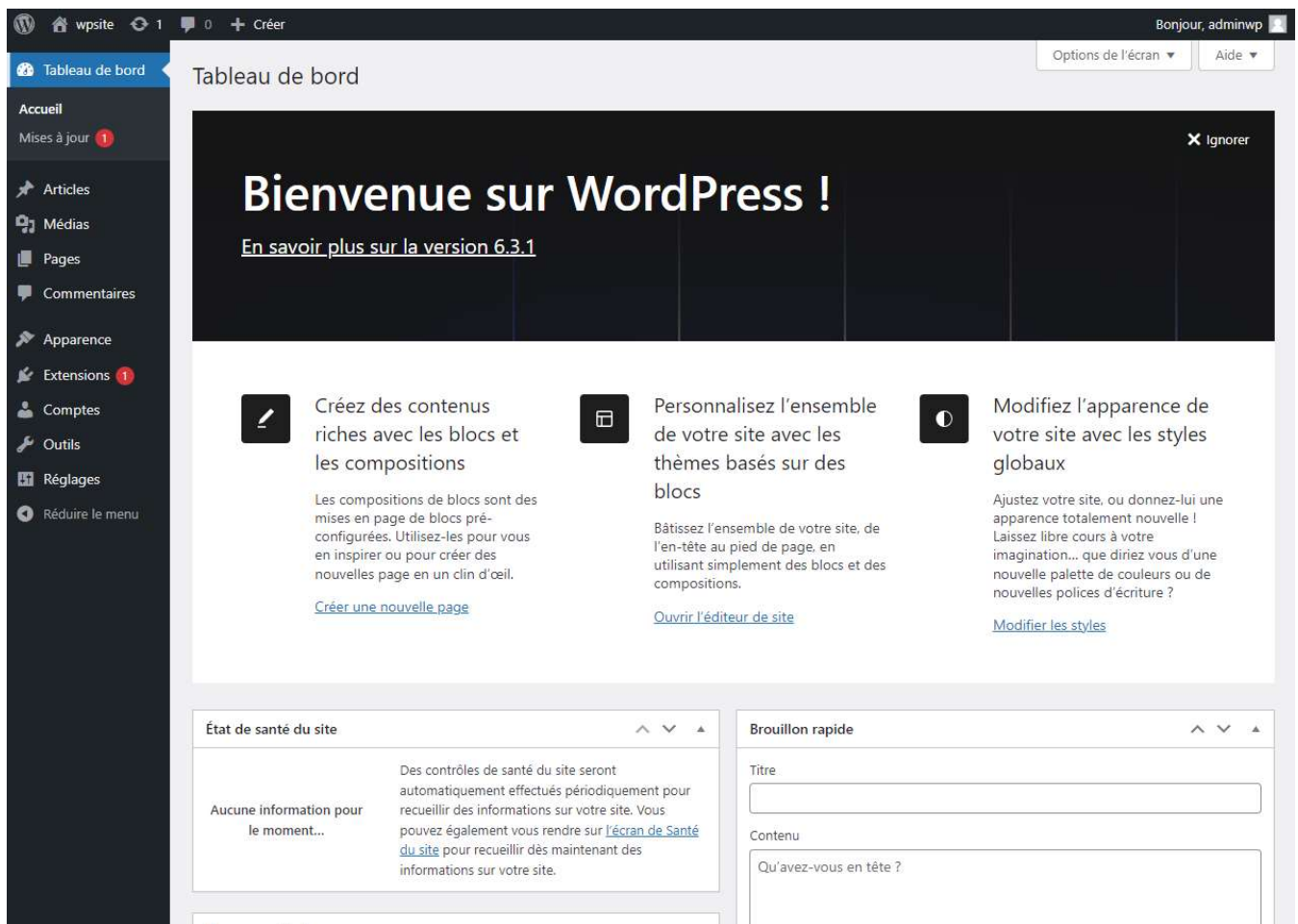
Identifiant ou adresse e-mail

Mot de passe



☒ Se souvenir de moi

Se connecter



Nous avons accès au site de wordpress depuis un lien

Recherches – partie 3

10)

L'OWASP (Open Web Application Security Project) est une organisation sans but lucratif qui se concentre sur l'amélioration de la sécurité des logiciels, en fournissant des ressources, des outils et des informations pour aider les professionnels à concevoir, développer et maintenir des applications web sécurisées. Elle sensibilise aux risques de sécurité, propose des formations, développe des outils open source.

11)

Le but principal du projet "Top Ten OWASP" est de fournir une liste des vulnérabilités de sécurité les plus critiques et les plus courantes auxquelles sont confrontées les applications web, afin d'aider les développeurs, les architectes logiciels et les professionnels de la sécurité à se concentrer sur les problèmes les plus importants

12)

OWASP WebScarab NG Project est un outil de test de sécurité des applications web, tandis qu'OWASP WebGoat est une application web vulnérable utilisée à des fins d'apprentissage et de formation en matière de sécurité des applications web.

13)

HackerOne est une entreprise américaine spécialisée dans la cybersécurité, spécifiquement sur la gestion de résistance contre les attaques en détectant des vulnérabilités, elle fonctionne par la communauté, comme son financement, idées, marketing, développement... et s'occupe d'entreprise tel que Google, Microsoft, Github, Twitter...

14)

Un livre blanc tel que celui de wordpress contient des informations des développeurs, sur le fonctionnement du système, des bonnes pratiques pour éviter des failles de plusieurs types, et d'autre information pour pouvoir l'utiliser à plein potentiel.

15)

Le Syntec Informatique représentant l'industrie des technologies de l'information et de la communication (TIC). Elle collabore avec les pouvoirs publics, encourage le développement de compétences numériques, et effectue une veille stratégique pour le secteur. Son objectif principal est de soutenir la croissance et l'innovation des entreprises du secteur des TIC

16)

Un livre vert est un document publié par un gouvernement ou une organisation pour solliciter des avis et des contributions sur un sujet spécifique. Il est utilisé pour lancer une consultation publique et recueillir des commentaires du public et des experts en vue d'influencer la prise de décision.

17)

Le Green IT (Informatique Verte) est l'utilisation de la technologie de manière éco-responsable tel que :

- L'efficacité énergétique
- Le recyclage et la gestion des déchets
- La virtualisation
- L'utilisation de matériaux respectueux de l'environnement
- La sensibilisation et la formation

18)

Un livre bleu peut se référer à un document technique/guide de référence, décrivant les spécifications, les normes, ou les meilleures pratiques pour un système, un logiciel ou un matériel particulier. Ces documents sont utilisés comme ressources de base pour les pratiques de informatiques.

19)

Dans l'informatique les assises sont un congrès annuel dédié à la sécurité de l'information, où les professionnels se réunissent pour échanger des informations, discuter des défis de la cybersécurité et explorer les dernières solutions pour renforcer la protection des systèmes d'information.

20)

Tous d'abord ces 3 outils vont renforcer la sécurité.

-Fail2Ban est un logiciel de prévention des intrusions qui surveille les logs des services réseau, tels que SSH, FTP, ou Apache, à la recherche de tentatives d'authentification infructueuses ou de comportements suspects. L'intérêt de Fail2Ban réside dans sa capacité à détecter et à répondre automatiquement aux tentatives d'attaques en bloquant temporairement l'accès des adresses IP responsables. Cela limite l'exposition aux attaques répétées.

-Iptables est un pare-feu logiciel sous Linux qui permet de contrôler le trafic réseau entrant et sortant en utilisant des règles de filtrage basées sur les adresses IP, les ports et les protocoles. Il est essentiel pour définir des règles de sécurité personnalisées pour un serveur ou un réseau. Il permet de bloquer ou d'autoriser le trafic en fonction de critères spécifiques, aidant ainsi à protéger les ressources réseau contre les accès non autorisés ou les attaques.

-Portsentry est un outil de détection d'intrusion qui surveille les ports du système et réagit en cas de tentatives d'accès non autorisées. Il va détecter les scans de ports et les tentatives d'intrusion sur un serveur en surveillant les connexions entrantes et en réagissant en conséquence. Il peut ajouter des adresses IP suspectes à une liste de blocage temporaire ou effectuer d'autres actions pour protéger le système.

21)

(Mettre en place ces 3 outils dans la vm avec documentation...)

apt install fail2ban -y

réglage de fail2ban :

systemctl status fail2ban

systemctl start fail2ban

systemctl enable fail2ban

Nano /etc/fail2ban/jail.conf

```
GNU nano 7.2 /etc/fail2ban/jail.conf *
# -----
# "ignoreself" specifies whether the local resp. own IP addresses should be ignored
# (default is true). Fail2ban will not ban a host which matches such addresses.
#ignoreself = true
#
# "ignoreip" can be a list of IP addresses, CIDR masks or DNS hosts. Fail2ban
# will not ban a host which matches an address in this list. Several addresses
# can be defined using space (and/or comma) separator.
#ignoreip = 127.0.0.1/8 ::1
#
# External command that will take an tagged arguments to ignore, e.g. <ip>,
# and return true if the IP is to be ignored. False otherwise.
#
# ignorecommand = /path/to/command <ip>
ignorecommand =
#
# "bantime" is the number of seconds that a host is banned.
bantime = 2m
#
# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime = 10m
#
# "maxretry" is the number of failures before a host get banned.
maxretry = 3
#
# "maxmatches" is the number of matches stored in ticket (resolvable via tag <matches> in actions).
maxmatches = %(maxretry)s
#
# "backend" specifies the backend used to get files modification.
# Available options are "pyinotify", "gamin", "polling", "systemd" and "auto".
#
# Aide      Écrire Chercher Couper Exécuter Emplacement Annuler
# Quitter  Lire fich. Remplacer Coller Justifier Aller ligne Refaire
```

```

GNU nano 7.2 /etc/fail2ban/jail.conf *
# or separate .conf files under jail.d/ directory, e.g.:
#
# HOW TO ACTIVATE JAILS:
#
# YOU SHOULD NOT MODIFY THIS FILE.
#
# It will probably be overwritten or improved in a distribution update.
#
# Provide customizations in a jail.local file or a jail.d/customisation.local.
# For example to change the default bantime for all jails and to enable the
# ssh-iptables jail the following (uncommented) would appear in the .local file.
# See man 5 jail.conf for details.
#
[DEFAULT]
bantime = 2m
#
[sshd]
enabled = true

# See jail.conf(5) man page for more information

```

Nano /etc/fail2ban/jail.local

```

GNU nano 7.2 /etc/fail2ban/jail.local
[DEFAULT]
#Debian 12 has no log files, just journalctl
backend = systemd

#"bantime" is the number of seconds that a host is banned
bantime = 2m

#"bantime" is the number of failures before a host get banned
maxretry = 5
# A host is banned if it has generated "maxretry" during the last "findtime"
findtime = 1h

[sshd]
enabled = true

```

Installation du Iptables :

Apt install iptable -y

```

root@debian:/# iptables -L -V
iptables v1.8.9 (nf_tables)

```

22)

(Parcourez le « catalogue » des extensions Wordpress et mettez-en place le WAF de votre choix sous forme de plugin Wordpress. Lire : <https://wordpress.org/plugins/web-application-firewall/#installation>. Réalisez la documentation associée.)

23)

L'outil Nmap (Network Mapper) est un scanner de réseau open source. Son principal objectif est d'explorer les réseaux et de découvrir les services en cours d'exécution sur les hôtes. Dans notre contexte, Nmap il pourra :

- Découverte des hôtes : Il peut scanner un réseau pour trouver des hôtes actifs. Il identifie les adresses IP disponibles et les machines connectées au réseau.
- Analyse des ports : Il peut scanner les ports ouverts sur les hôtes pour identifier les services en cours d'exécution. Cela aide à déterminer quelles ressources sont exposées et potentiellement vulnérables.
- Détection de systèmes d'exploitation : Il peut essayer d'identifier le système d'exploitation des hôtes en analysant les réponses aux requêtes réseau. Cela peut aider à comprendre la diversité des systèmes dans un réseau cible.
- Détection de vulnérabilités : Il peut signaler certaines vulnérabilités potentielles en fonction des versions des services identifiés.

24)

Dirbuster est un outil conçu pour effectuer des attaques par force brute sur les noms de fichiers et de répertoires d'un site web. Dans notre contexte, il pourra :

- Identifier les points d'entrée potentiels : Il essaie de trouver des fichiers et des répertoires cachés ou non liés dans une application web. Cela peut révéler des vulnérabilités de sécurité telles que des points d'entrée non sécurisés ou des configurations incorrectes.
- Cartographier la structure du site : Il peut aider à comprendre la structure d'un site web, ce qui peut être utile pour les tests de sécurité et l'analyse des vulnérabilités.

25)

Nikto est un scanner de vulnérabilités dédié aux serveurs web. Il recherche des vulnérabilités connues, des erreurs de configuration et des problèmes de sécurité sur des serveurs web. Dans notre contexte, il pourra :

- Identifier les vulnérabilités : Il recherche des vulnérabilités courantes et des problèmes de sécurité connus sur un serveur web, tels que des fichiers non sécurisés, des configurations mal sécurisées, etc.
- Évaluer la sécurité : Il aide à évaluer la sécurité globale d'un serveur web en signalant les erreurs de configuration qui pourraient être exploitées par des attaquants.