ELMABROUK DEVELOPMENT

Rapport sur l’état actuel du site WordPress - Association ATFD

Date : 03 mai 2025
Préparé par : Mabrouk Moataz - ELMABROUK DEVELOPMENT
Client : Association ATFD

1. Résumé exécutif

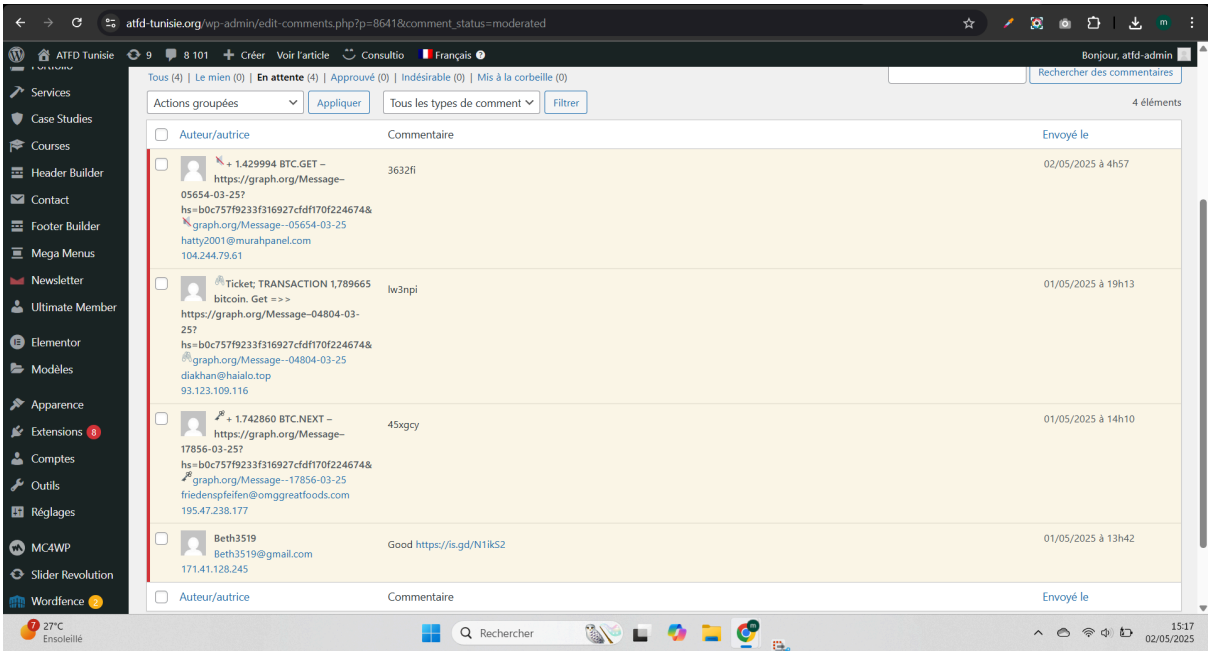
Le site WordPress de l’Association ATFD rencontre plusieurs problèmes critiques affectant son fonctionnement, sa sécurité et son expérience utilisateur. Une inondation massive de commentaires spam, avec **7 638 commentaires** sur une seule publication et **plus de 406 720 commentaires spam au total**, surcharge la base de données.
Des vulnérabilités dans WordPress et les plugins exposent le site à des risques de piratage, et une erreur lors du téléversement d’une image (797 Ko) indique des limitations de ressources serveur. Le pare-feu Wordfence a bloqué **1 296 attaques** au cours du dernier mois, avec un total de **264 353 474 attaques** repoussées sur l’ensemble des sites protégés par Wordfence en 30 jours, soulignant l’exposition élevée du site aux menaces. Le site est hébergé chez OVH sur un plan **Performance 2**, avec des ressources limitées (2,08 Go utilisés sur 500 Go, 4 bases de données MySQL) insuffisantes pour ce type de projet et les plugins volumineux utilisés. Une analyse des options de migration chez OVH montre des plans plus puissants disponibles.
Ce rapport détaille l’état actuel du site et du serveur pour informer l’Association ATFD des défis rencontrés.

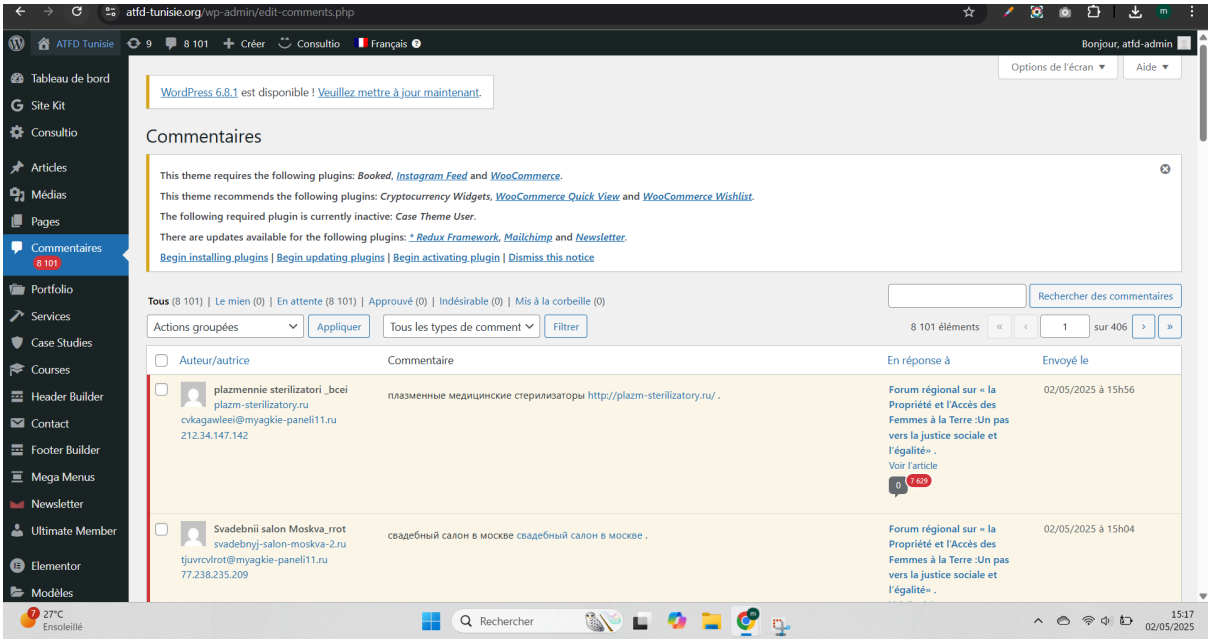
2. État actuel du site

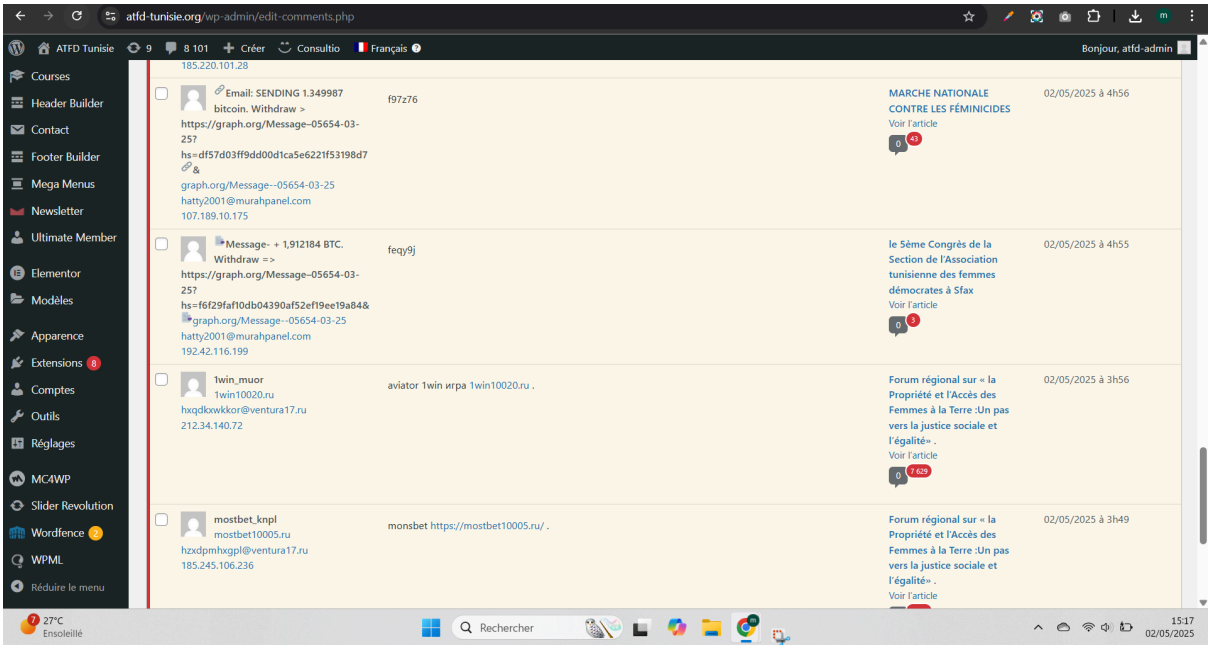
2.1 Inondation de commentaires spam

- **Description** : Chaque article publié reçoit des commentaires automatisés provenant de faux comptes (bots). Ces commentaires contiennent :
  - Des noms d'utilisateur aléatoires (ex. : mostbet_kg_tzol, 1win_nipr).
  - Des adresses e-mail jetables (ex. : popgdfyrwol@ventura17.ru, oplfkqslhpr@ventura17.ru).
  - Des adresses IP suspectes (ex. : 91.84.106.2, 195.26.224.102).
  - Des liens vers des sites douteux (ex. : http://mostbet10006.ru/, 1win10004.ru).
- **Volume** :
  - Une seule publication, intitulée *Forum régional sur « la Propriété et l'Accès des Femmes à la Terre : Un pas vers la justice sociale et l'égalité »*, a reçu **7 638 commentaires spam** en attente de modération.
  - Le site compte au total **plus de 406 720 commentaires spam**, aucun n'étant approuvé.

Exemples de commentaires :







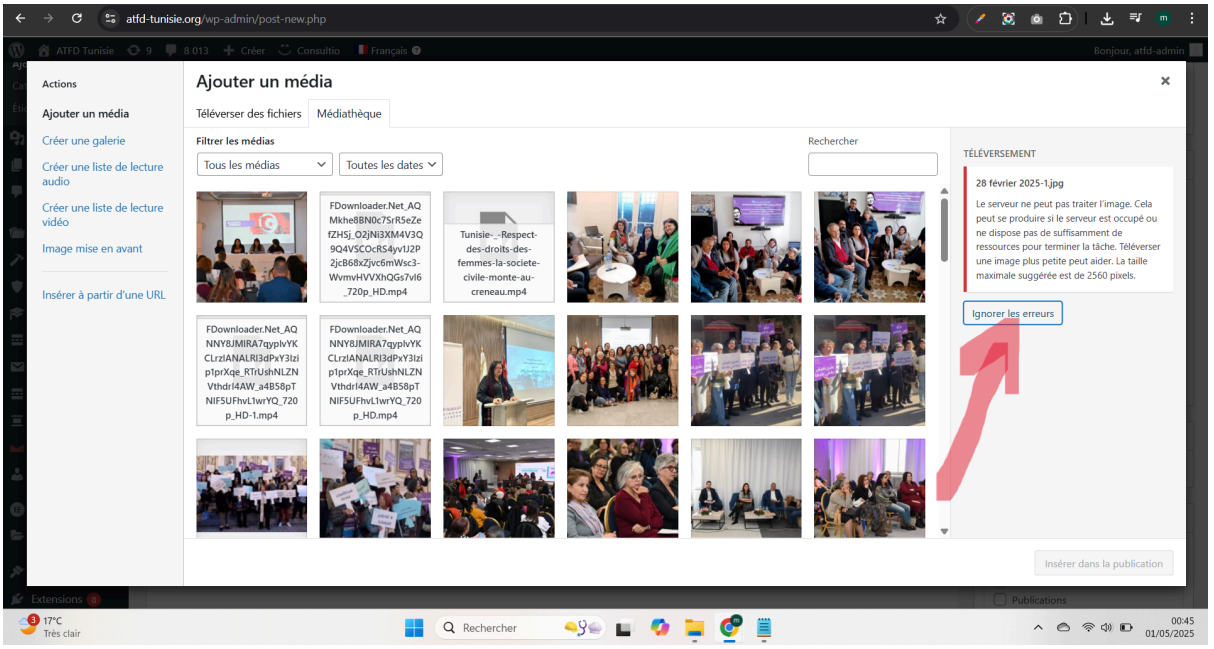
Impact :

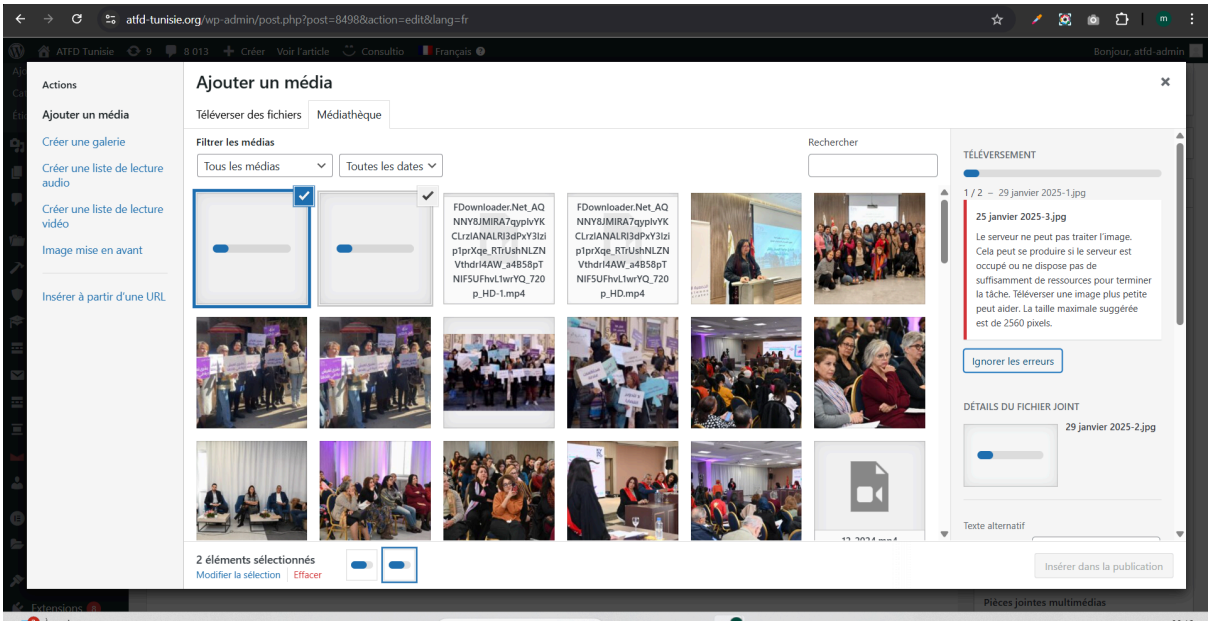
- Surcharge massive de la base de données, entraînant un ralentissement significatif du site.
- Risque pour la réputation si les commentaires deviennent visibles publiquement.
- Potentiel danger pour le SEO si les liens spammy sont indexés par Google.

2.2 Erreur lors du téléversement d’une image

Description : Une tentative de téléversement d’une image de **797 Ko** a généré l’erreur suivante :
Le serveur ne peut pas traiter l’image. Cela peut se produire si le serveur est occupé ou ne dispose pas de suffisamment de ressources pour terminer la tâche. Téléverser une image plus petite peut aider. La taille maximale suggérée est de 2560 pixels.

- **Analyse** :
  - Cette erreur indique une limitation des ressources serveur (mémoire PHP, temps d’exécution, ou bande passante).
  - La taille de l’image (797 Ko) est modeste, suggérant que le serveur est sous pression ou mal configuré pour gérer des fichiers de cette taille.
  - La mention de "2560 pixels" fait référence à une restriction de dimension ou à une configuration par défaut de WordPress, mais le problème principal semble lié aux ressources serveur.
- **Impact** :
  - Incapacité à publier du contenu visuel (images, bannières), ce qui limite la gestion du site.
  - Frustration pour les administrateurs et risque de retard dans la mise à jour du contenu.
- **Captures** :





2.3 Problèmes de sécurité et de maintenance

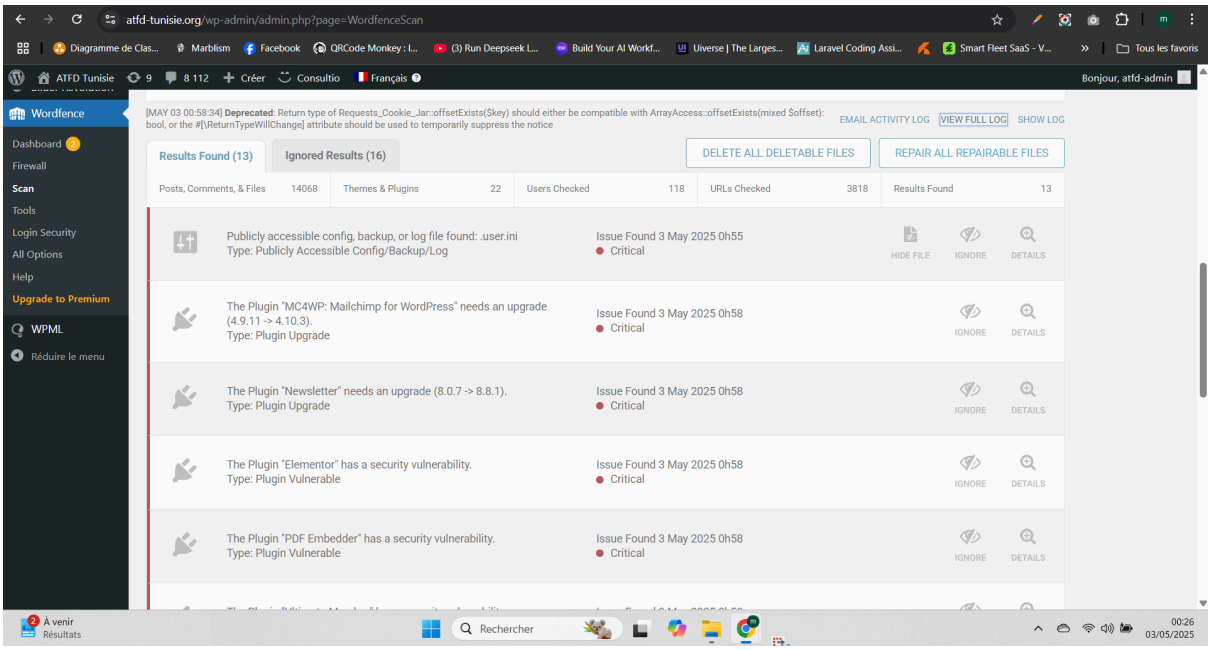
Une analyse via **Wordfence Security** (version gratuite, scan du 2 mai 2025 à 18h46) a révélé **13 problèmes** critiques et moyens :

- **WordPress obsolète** :
  - Version actuelle : **6.8.1**. Une mise à jour est disponible.
  - Impact : Les versions obsolètes contiennent des failles de sécurité exploitables.
- **Fichier sensible accessible** :
  - Un fichier **.user.ini** est publiquement accessible, exposant des configurations PHP sensibles (ex. : limites de mémoire, modules activés).
  - Impact : Les pirates peuvent utiliser ces informations pour planifier des attaques ciblées.
- **Plugins vulnérables** :
  - **Elementor** : Contient une vulnérabilité de sécurité connue.
  - **PDF Embedder** : Contient une vulnérabilité de sécurité connue.
  - **Ultimate Member** : Contient une vulnérabilité de sécurité connue.
  - Impact : Ces failles permettent l'injection de code, l'élévation de privilèges ou des attaques XSS (Cross-Site Scripting).
- **Plugins nécessitant une mise à jour** :
  - **MC4WP: Mailchimp for WordPress** (4.9.11 → 4.10.3).
  - **Newsletter** (8.0.7 → 8.8.1).

    - **Classic Editor** (1.6.3 → 1.6.7).
    - **Duplicate Page and Post** (2.9.3 → 2.9.5).
    - **Site Kit by Google** (1.118.0 → 1.151.0).
    - **Template Library and Redux Framework** (4.3.12 → 4.5.7).
    - **Wordfence Security** (7.11.1 → 8.0.5).
    - **XML Sitemap Generator for Google** (4.1.18 → 4.1.21).
    - Impact : Les versions obsolètes peuvent contenir des failles exploitables.
- **Plugin inactif** :
    - **Case Theme User**, requis par le thème, est désactivé, ce qui peut causer des dysfonctionnements.
- **Plugins requis par le thème** :
    - Booked, Instagram Feed, WooCommerce.
- **Plugins recommandés par le thème** :
    - Cryptocurrency Widgets, WooCommerce Quick View, WooCommerce Wishlist.
- **Impact global** :
    - Risque de piratage (vol de données, injection de malware, défacement du site).
    - Instabilité potentielle due à des plugins incompatibles ou inactifs.

Configuration Wordfence

- **Statut** : Scan activé, mais utilisant la version gratuite avec des signatures communautaires (retard de 30 jours sur les signatures de malware).
- **Options activées** :
    - Scan personnalisé.
    - Vérification des spams et des blocklists désactivée (nécessite la version Premium).
- **Résultats du scan** :
    - **13 problèmes** détectés (voir ci-dessus).
    - **16 résultats ignorés** (non détaillés dans ce rapport).
    - Aucun problème détecté dans les articles, commentaires, thèmes, plugins, utilisateurs ou URLs vérifiés.
- **Analyse** :
    - Le site atfd-tunisie.org est activement ciblé, avec une augmentation des attaques complexes et par force brute au fil du temps (de 82 par jour à 1 296 par mois).



- Les attaques complexes visent probablement les vulnérabilités identifiées (plugins, WordPress obsolète, fichier .user.ini).
- Les attaques par force brute tentent de compromettre les comptes administrateurs, ce qui est particulièrement dangereux si les mots de passe sont faibles.
- Le volume global d’attaques (264 millions en 30 jours) indique que le site opère dans un environnement web à haut risque, où les bots et pirates scannent constamment les sites vulnérables.

3. État du serveur web

3.1 Détails de l’hébergement

Le site est hébergé chez **OVH** sur un plan **Performance 2**, avec les caractéristiques suivantes :

- **Statut** : Actif.
- **Date de création** : 17 septembre 2020.
- **Expiration** : 17 septembre 2025.
- **Adresses IP** :
    - IPv4 : 188.165.4.35.
    - IPv6 : 2001:41d0:301:3::26.
- **Espace disque** : 2,08 Go utilisés sur 500 Go disponibles.
- **Centre de données** : eu-west-gra (Gravelines, France).
- **Filer** : 207.
- **Version PHP** : 8.2.
- **Certificat SSL** : Oui (Let’s Encrypt - DV).
- **Adresses e-mail** : Actives (nombre non précisé).
- **Option CDN** : Désactivée.
- **Bases de données** :
    - 3 bases de données MySQL utilisées sur 4 disponibles.
    - 1 base de données Web Cloud non activée.
- **Boost** : Désactivé.
- **Contacts** :
    - Administrateur : by171958-ovh.
    - Technique : by171958-ovh.
    - Facturation : by171958-ovh.

3.2 Analyse du serveur

- **Utilisation de l’espace disque** :
    - Avec seulement 2,08 Go utilisés sur 500 Go, l’espace disque n’est pas un problème.
    - Cependant, la surcharge causée par les **plus de 406 720 commentaires spam** augmente considérablement la taille de la base de données, contribuant à la lenteur.
- **Performance** :

    - L’erreur de téléversement d’image (797 Ko) indique que les ressources allouées (CPU, RAM, limites PHP comme `memory_limit` ou `upload_max_filesize`) ne sont pas suffisantes pour gérer ce type de projet et les plugins volumineux utilisés (ex. : Elementor, WooCommerce, Booked).
    - The plan Performance 2 offers limited resources (2 vCores, 4 GB RAM estimated), insufficient to support a WordPress site with resource-intensive plugins and a high volume of spam comments.
- **Bases de données** :
    - L’utilisation de 3 bases de données sur 4 suggère que le site WordPress est proche de la limite de bases disponibles.
    - The spam comments significantly increase the database load, impacting performance.
- **PHP 8.2** :
    - La version PHP est récente, ce qui est positif pour la sécurité et la compatibilité.
    - Cependant, des configurations PHP inadéquates (ex. : limites de mémoire ou de taille de fichier) sont probablement à l’origine de l’erreur de téléversement d’image.
- **Absence de CDN** :
    - Sans CDN, le site dépend entièrement des performances du serveur OVH, ce qui peut entraîner des temps de chargement plus longs, surtout pour les visiteurs éloignés du centre de données (Gravelines, France).
- **Sécurité** :
    - Le certificat SSL (Let’s Encrypt) est actif, garantissant le chiffrement des connexions.
    - Cependant, le fichier .user.ini accessible publiquement expose des informations sensibles sur la configuration du serveur, augmentant le risque d’attaques ciblées.

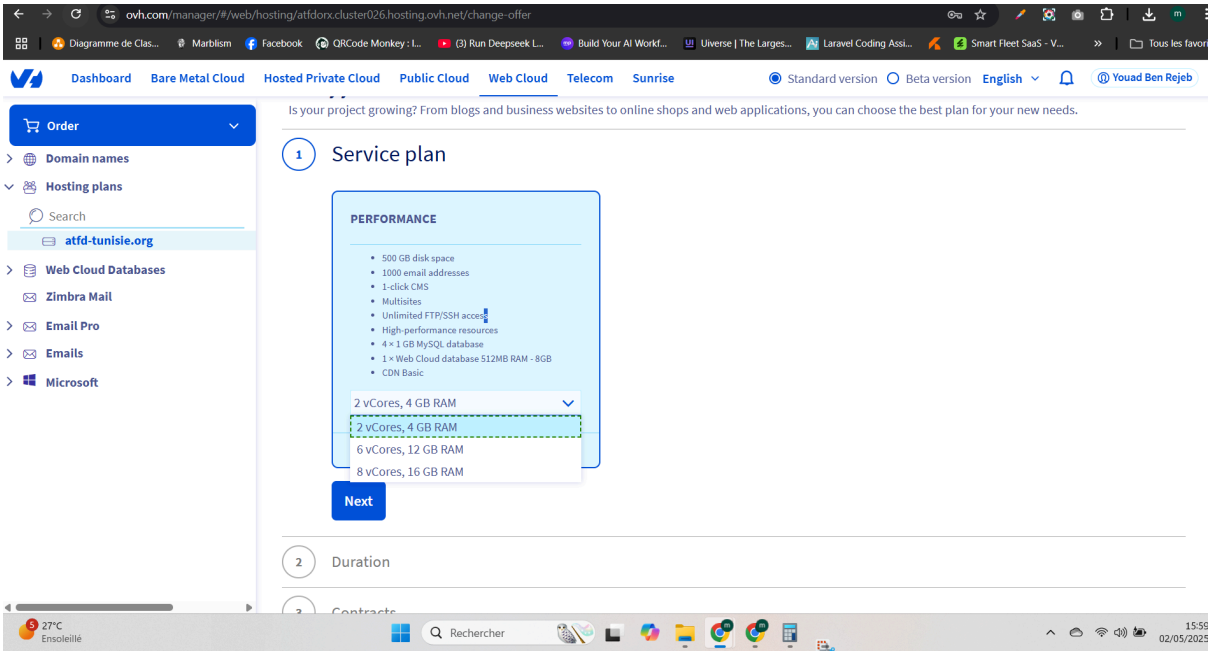
3.3 Options de migration chez OVH

Une analyse des options de migration pour le plan actuel révèle les possibilités suivantes :

- **Plan actuel** : Performance 2.
    - 500 Go d’espace disque.
    - 1 000 adresses e-mail.
    - CMS en 1 clic.
    - Multisites.

- Accès FTP/SSH illimité.
- Ressources haute performance.
- 4 bases de données MySQL (1 Go chacune).
- 1 base de données Web Cloud (512 Mo RAM, 8 Go).
- CDN Basic inclus.

- **Options de migration** :
  - **Performance (6 vCores, 12 Go RAM)** :
    - Prix : 21,99 DT hors taxes/mois.
    - Amélioration significative des ressources CPU et RAM pour gérer des sites plus exigeants.
  - **Performance (8 vCores, 16 Go RAM)** :
    - Prix non précisé dans les informations fournies.
    - Ressources encore plus élevées pour des applications complexes ou un trafic important.



- **Analyse** :
  - Les plans supérieurs offrent plus de CPU et de RAM, ce qui pourrait répondre aux besoins d'un projet utilisant des plugins volumineux et nécessitant plus de ressources pour des tâches comme le téléversement d'images ou la gestion de bases de données.

4. Comment les vulnérabilités peuvent être exploitées et menaces possibles

Les problèmes identifiés exposent le site à des risques significatifs. Voici une analyse des menaces potentielles et de la manière dont elles pourraient être exploitées :

4.1 Vulnérabilités des plugins (Elementor, PDF Embedder, Ultimate Member)

- **Mécanisme d'exploitation** :
    - **Elementor** : Une faille pourrait permettre l'injection de scripts malveillants (XSS) dans les pages, affectant les visiteurs, ou l'exécution de code à distance (RCE) pour modifier le site.
    - **PDF Embedder** : Une vulnérabilité pourrait permettre à un pirate de télécharger des fichiers malveillants déguisés en PDF ou d'exploiter le plugin pour accéder au serveur.
    - **Ultimate Member** : Une faille d'élévation de privilèges pourrait permettre à un attaquant de créer un compte administrateur ou d'accéder aux données des utilisateurs.
- **Menaces** :
    - Vol de données utilisateurs (noms, e-mails, mots de passe).
    - Injection de malwares ou de backdoors pour un accès permanent.
    - Redirection des visiteurs vers des sites frauduleux ou de phishing.
    - Défacement du site (remplacement du contenu par des messages pirates).

4.2 Fichier .user.ini publiquement accessible

- **Mécanisme d'exploitation** :
    - Les pirates peuvent lire le fichier pour découvrir des configurations PHP (ex. : version, modules, limites).
    - Ces informations peuvent être utilisées pour exploiter des failles spécifiques ou identifier des versions obsolètes du serveur.
- **Menaces** :
    - Exposition d'informations sensibles, facilitant les attaques ciblées.
    - Compromission du serveur si une directive mal configurée est exploitée.
    - Perte totale de contrôle du site.

4.3 WordPress et plugins obsolètes

- **Mécanisme d'exploitation** :
    - Les failles dans WordPress 6.8.1 et les plugins obsolètes (ex. : Mailchimp, Newsletter, Redux Framework) sont souvent publiques et exploitées par des outils automatisés.
    - Les attaques courantes incluent :
        - Injection SQL pour voler des données de la base de données.
        - Exécution de code à distance pour installer des malwares.
        - Création de comptes administrateurs frauduleux.
- **Menaces** :
    - Vol de données sensibles (contenu, utilisateurs, configurations).
    - Utilisation du site comme relais pour des spams ou des attaques DDoS.
    - Corruption ou perte de données.

4.4 Commentaires spam

- **Mécanisme d'exploitation** :
    - Les bots surchargent le serveur avec **plus de 406 720 commentaires**, augmentant la charge sur la base de données.
    - Une faille dans le système de commentaires pourrait permettre l'injection de code malveillant via des liens ou du texte.
    - Si un commentaire est approuvé par erreur, il pourrait exécuter un script affectant les visiteurs.
- **Menaces** :
    - Ralentissement ou panne du site due à la surcharge.
    - Propagation de malwares via des liens spammy.
    - Pénalités SEO si les liens sont indexés.

4.5 Plugin Case Theme User inactif

- **Mécanisme d'exploitation** :
    - L'inactivation de ce plugin requis peut entraîner des erreurs dans le thème, exposant des failles si le thème n'est pas sécurisé sans lui.
    - Un thème mal configuré peut être exploité pour injecter du code ou accéder au serveur.
- **Menaces** :
    - Instabilité du site (erreurs d'affichage, fonctionnalités cassées).
    - Risque de sécurité si le thème contient des failles non corrigées.

4.6 Erreur de téléversement d’image

- **Mécanisme d’exploitation** :
    - Bien que l’erreur elle-même ne soit pas une vulnérabilité directe, elle indique une faiblesse des ressources serveur.
    - Un pirate pourrait exploiter cette limitation en surchargeant le serveur avec des requêtes lourdes (ex. : téléversements multiples), provoquant un déni de service (DoS).
- **Menaces** :
    - Incapacité à gérer le contenu, affectant la mise à jour du site.
    - Risque de panne si le serveur est surchargé par d’autres attaques.

4.7 Synthèse des risques globaux

- **Piratage complet** : Accès administrateur non autorisé, modification ou suppression du site.
- **Vol de données** : Perte d’informations sensibles (utilisateurs, contenu, données WooCommerce).
- **Attaques contre les visiteurs** : Redirections malveillantes, phishing, ou infection par malware.
- **Pertes financières** : Temps d’arrêt, coûts de restauration, amendes RGPD si des données sont compromises.
- **Dommages à la réputation** : Perte de confiance des membres et partenaires si le site est piraté ou affiche du contenu inapproprié.

---

5. Conclusion

Le site WordPress de l’Association ATFD est dans un état critique en raison de :

- Une inondation massive de **plus de 406 720 commentaires spam**, dont **7 638** sur une seule publication, surchargeant la base de données.
- Une erreur de téléversement d’image (797 Ko), indiquant des ressources serveur insuffisantes pour ce type de projet et les plugins volumineux.
- **13 problèmes de sécurité** (WordPress obsolète, plugins vulnérables, fichier .user.ini accessible).
- Un serveur OVH (plan Performance 2) avec des ressources limitées, inadaptées aux besoins du site et à l’utilisation de plugins gourmands.

- Une exposition élevée aux attaques, avec **1 296 attaques bloquées** sur le site en un mois et **264 353 474 attaques** repoussées globalement par Wordfence en 30 jours.
- Des options de migration vers des plans plus puissants (6 vCores/12 Go RAM ou 8 vCores/16 Go RAM) disponibles chez OVH.

Ces problèmes compromettent la performance, la sécurité et la fiabilité du site, exposant l'Association ATFD à des risques de piratage, de perte de données et de dommages à sa réputation.