Rapport de Vulnérabilités Web

Analyse de Sécurité Détaillée

Informations Système

Système	Windows
Version	11
Architecture	AMD64
Nom d'hôte	404NotFound
Adresse IP	10.21.1.160
Date du scan	17/06/2025 11:34:56

Équipe de Développement

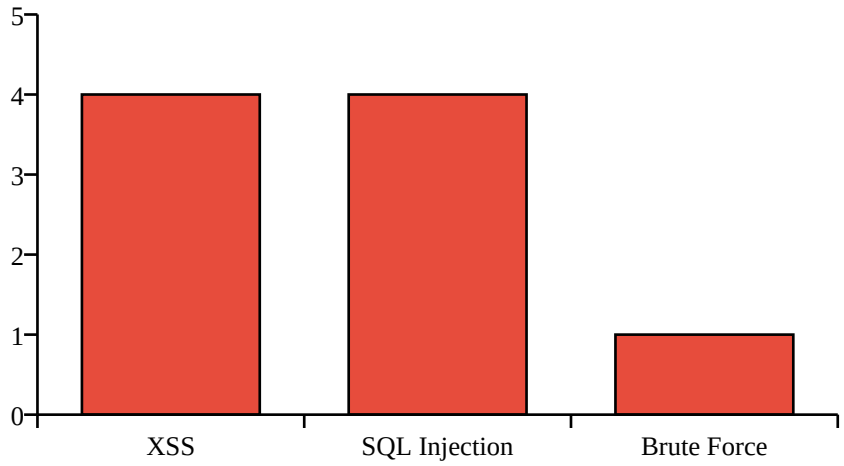
• Florian - Expert en Sécurité Web

• Yoann - Spécialiste en Analyse de Vulnérabilités

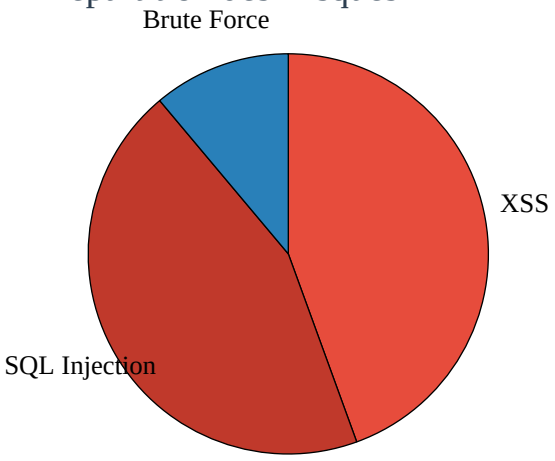
• Quentin - Développeur Full-Stack

Résumé des Vulnérabilités

Résumé des Vulnérabilités Détectées



Répartition des Risques



Type de Vulnérabilité	Nombre Détecté	Niveau de Risque	Impact Potentiel
XSS	4	Élevé	Vol de données, Session Hijacking
SQL Injection	4	Critique	Accès non autorisé à la base de données
Brute Force	1	Moyen	Compromission des comptes

Vulnérabilités XSS Détectées

Description

Les attaques XSS (Cross-Site Scripting) permettent à un attaquant d'injecter du code malveillant dans des pages web vues par d'autres utilisateurs.

URL	Payload	Niveau de Risque	Recommandation
http://127.0.0.1:5000/comment	<script>alert('XSS')</script>	Élevé	Valider et échapper les entrées utilisa
http://127.0.0.1:5000/comment	<img src=x onerror=alert('XSS')>	Élevé	Valider et échapper les entrées utilisa
http://127.0.0.1:5000/comment	<svg/onload=alert('XSS')>	Élevé	Valider et échapper les entrées utilisa
http://127.0.0.1:5000/comment	<iframe src='javascript:alert("XSS")'></iframe>	Élevé	Valider et échapper les entrées utilisa

Vulnérabilités SQL Injection Détectées

Description

Les attaques par injection SQL permettent à un attaquant d'exécuter des commandes SQL malveillantes sur la base de données.

URL	Payload	Niveau de Risque	Recommandation
http://127.0.0.1:5000/login	' OR 1=1 --	Critique	Utiliser des requêtes préparées
http://127.0.0.1:5000/login	' OR 'a'='a' --	Critique	Utiliser des requêtes préparées
http://127.0.0.1:5000/login	' UNION SELECT NULL, NULL --	Critique	Utiliser des requêtes préparées
http://127.0.0.1:5000/login	' UNION SELECT username, password FROM users --	Critique	Utiliser des requêtes préparées

Tests de Brute Force

Description

Les attaques par force brute tentent de deviner les identifiants en essayant toutes les combinaisons possibles.

URL	Payload	Niveau de Risque	Recommandation
http://127.0.0.1:5000/login	[('user', 'password')]	Moyen	Limiter les tentatives de connexion

Recommandations Détaillées

Validation des Entrées

• Mettre en place une validation stricte des entrées utilisateur

• Utiliser des expressions régulières pour valider les formats

• Implémenter une liste blanche de caractères autorisés

Protection contre les Injections SQL

• Utiliser des requêtes préparées pour toutes les opérations SQL

• Éviter la concaténation directe des entrées utilisateur dans les requêtes

• Implémenter un système de logging des requêtes SQL

Sécurité XSS

• Échapper correctement les caractères spéciaux

• Utiliser des en-têtes de sécurité comme Content-Security-Policy

• Implémenter une validation côté serveur

Protection contre le Brute Force

• Limiter le nombre de tentatives de connexion

• Implémenter un délai croissant entre les tentatives

• Utiliser l'authentification à deux facteurs

Sécurité Générale

• Mettre à jour régulièrement tous les composants du système

• Utiliser HTTPS pour toutes les communications

• Implémenter une politique de mots de passe forte

Ce rapport a été généré automatiquement par l'outil de scan de vulnérabilités web

Date de génération : 17/06/2025 11:34:56