Rapport de l'analyse

Tableaux récapitulatif

IP	Niveau de vulnérabilité	Nombre total de failles	RCE	SQLi	XSS
127.0.0.1	5	10	1	1	0

SQLi

Les SQLi, aussi appelé injection SQL est un type de faille qui a pour but interagir avec une base de données, pour cela on injecte un morceau malveillant de requête SQL dans une requête SQL qui va par exemple vérifier un mot de passe. Ce type de faille peux permettre par exemple de récupérer tous les mot de passe et les nom d'utilisateurs.Voici une ressource pour vous protéger contre les injections sql https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

XSS

Les failles XSS sont des failles liées aux différents point d'entrés du site web, per exemple en laissant un commentaire l'utilisateur peux tenter d'injecter du code malveillant, si votre serveur ne vérifie pas ce que rentre l'utilisateur il va renvoyer le code qui va être interpréter par les navigateurs des autres utilisateur qui visiterons la page. Ce type d'attaques peux permettre de voler les cookies, si un personne vole un cookie d'un administrateur il peux élever ses privilèges et accéder à des informations sensible. Il peux aussi par exemple rediriger les utilisateurs sur un page malveillantes. Voici une ressouce pour vous protéger contre les XSS https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html#defense-against-xss

RCE

RCE ou remonte commande injection, ce sont des failles qui permettent à l'utilisateur d'exécuter des commandes, pour éviter ce type de faille il faut vérifier les requêtes de l'utilisateur, par exemple en vérifiant les symboles utilisées.