Rapport de l'analyse

Tableau récapitulatif

IP	Niveau de vulnérabilité	Nombre total de failles	RCE	SQLi	Insecure_ Authentication	Local_File_Inclusion	Remote_ File_Inclusion	XSS
192.168.56.1	0	0	0	0	0	0	0	0
192.168.56.100	0	0	0	0	0	0	0	0
192.168.56.102	10	5	1	2	0	1	0	1
192.168.56.103	4	1	0	0	1	0	0	0

SQLi

Les SQLi, aussi appelées 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 mots de passe et les noms d'utilisateurs. Voici une ressource pour vous protéger contre les injections sql.
https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

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 utilisés.

XSS

Les failles XSS sont des failles liées aux différents points d'entrée du site web, par 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 interprété par les navigateurs des autres utilisateurs qui visiteront la page. Ce type d'attaques peut permettre de voler les cookies, si une personne vole un cookie d'un administrateur il peut élever ses privilèges et accéder à des informations sensibles. Il peux aussi par exemple rediriger les utilisateurs sur une page malveillante. Voici une ressource pour vous protéger contre les XSS
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html#defense-against-xss