Faille search_member_sql_inj_error_based

1. Identification de la faille

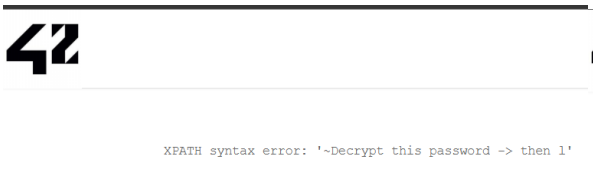
Action : Insertion d'un caractère spécial (guillemet simple ') dans le champ de recherche "Member ID".
Observation : Le serveur a renvoyé une erreur de syntaxe MariaDB, confirmant que l'entrée utilisateur est directement interprétée par la base de données sans nettoyage préalable.

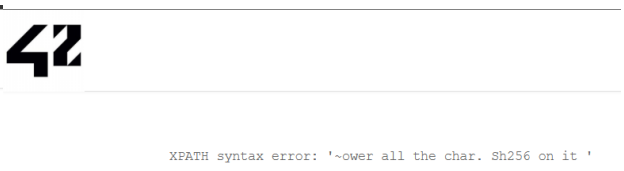
2. Exploitation et Contournement

Technique : Utilisation de la fonction extractvalue() pour forcer l'affichage des résultats de requêtes SQL directement dans les messages d'erreur XPATH du serveur.
Contournement de protection : Le serveur échappait les guillemets (affichage de \'USERS\'), empêchant l'utilisation de chaînes de caractères classiques.
L'utilisation de l'encodage hexadécimal (ex: 0x7573657273 pour users) a permis de contourner cette restriction.

3. Extraction des données

Données récupérées :
Un hash MD5 : 5ff9d0165b4f92b14994e5c685cdce28.
Une instruction dans la colonne comment : "Decrypt this password -> then lower all the char. Sh256 on it".





XPATH syntax error: '~8~'

XPATH syntax error: '~5ff9d0165b4f92b14994e5c685cdce2'

Résolution du Flag

Étape 1 : Le décodage du hash MD5 révèle le mot de passe : FortyTwo.
Étape 2 : Passage en minuscules comme demandé : fortytwo.
Étape 3 : Le hachage SHA256 de fortytwo correspond au premier flag de la liste fournie:
10a16d834f9b1e4068b25c4c46fe0284e99e44dceaf08098fc83925ba6310ff5

5. Remédiation
Solution : Implémenter des requêtes préparées (Prepared Statements).
Cela permet de séparer les données utilisateur de la requête SQL, rendant l'injection de commandes impossible.