

Jérémie SCHEMITH

Ayoub BOUASRIA

Simon VILLECHENAUD

Valentine GILLES

**Atelier 3 :**

**VULNÉRABILITÉS RÉSEAU**



8INF968 – Atelier pratique cybersécurité I

# Table des matières

[**Table des matières 2**](#_n7efmlo5o77a)

[**I. Présentation 3**](#_dq8svldr4i4m)

[a. Introduction 3](#_7obqmmxmhuro)

[b. Environnement 3](#_72640z2tub3t)

[1. Architecture Globale 3](#_efyubrjujrjd)

[2. Configuration du Réseau 4](#_pjgyk8tvegv3)

[3. Points d'Intérêt 4](#_r9o66n2b5hxt)

[c. Scénario 5](#_t2hwzhjgblsu)

[a. Phase d'Exploration 5](#_e58civ5ryfr2)

[b. Phase d'Exploitation 5](#_pj35lzgzta02)

[c. Phase de Phishing 5](#_95y4cxm1j113)

[d. Phase d'Escalade 5](#_yonnu3t7xogq)

[e. Modification du Script 5](#_df5thmeck2wc)

[**II. Exploitation des failles 6**](#_e45zf2jjzsd8)

[a. Brute Force de session 6](#_9ze3gz6ogym2)

[b. Injection SQL 6](#_y7ceiu5s4xmy)

[c. Phishing 9](#_dpqdjcduech6)

[d. Mauvaise Configuration 13](#_sbmcsgf9eks8)

[**III. Correction des failles 14**](#_qsvki2o5a0tr)

[a. Brute Force 15](#_ta61vmoew2zi)

[b. Injection SQL 15](#_57gwdjmget36)

[c. Phishing 15](#_60ihutdp1ndl)

[d. Mauvaise configuration : Accès anormaux 15](#_ak0aqpuy5noi)

[**Conclusion 16**](#_x9d2h9w8x31y)

# Présentation

## Introduction

Dans un paysage informatique en constante évolution, la sécurité des systèmes d'information est devenue une préoccupation majeure pour les organisations. La simulation d'attaques et l'évaluation proactive des infrastructures sont des éléments essentiels pour garantir la robustesse des défenses cybernétiques.

Le présent rapport se concentre sur une simulation d'attaque ciblant un environnement réseau complexe composé de deux machines Windows 10, d'un serveur Windows, d'un routeur PFsense, d'une machine Linux sous Debian et d'un serveur DNS intégré. Cette infrastructure est configurée autour d'un Active Directory (AD) centralisé, servant de pilier pour l'authentification des utilisateurs, avec le protocole LDAP facilitant l'intégration de différentes plates-formes au domaine AD.

La présence d'un site web hébergé sur la machine Linux, accessible via l'URL linux.ad.atelier3.com, ajoute une dimension critique à la sécurité de l'environnement. Cette simulation vise à identifier les vulnérabilités potentielles, évaluer la résilience du réseau face aux attaques, et formuler des recommandations visant à renforcer la posture de sécurité globale.

Le rapport se divise en plusieurs sections, débutant par une analyse détaillée de l'environnement réseau, suivi d'une simulation d'attaque, et concluant par des recommandations spécifiques pour améliorer la sécurité du système. L'objectif ultime est de fournir une vision holistique des risques potentiels, de renforcer les défenses existantes, et de préparer l'infrastructure à faire face aux menaces émergentes.

Sans plus tarder, plongeons dans l'examen minutieux de l'architecture réseau, mettant en lumière les composants clés et les points d'intérêt qui seront soumis à une évaluation approfondie au cours de cette simulation d'attaque.

## Environnement

### Architecture Globale

L'infrastructure ciblée dans le cadre de cette simulation d'attaque comprend un réseau complexe reposant sur les éléments suivants :

* Deux machines Windows (Windows 10) : Utilisateurs authentifiés via Active Directory.
* Serveur Windows (Windows Server) :
  + Fonctions principales d'Active Directory, serveur d'authentification LDAP.
  + Serveur DNS : Gère la résolution des noms de domaine au sein du réseau.
* Routeur PFsense : Assure la gestion des flux de données entre les réseaux locaux et externes.
* Machine Linux (Debian) :
  + Héberge un site web accessible via l'URL linux.ad.atelier3.com.
  + Également intégrée au domaine Active Directory via LDAP.

### Configuration du Réseau

* Active Directory (AD) :
  + Utilisé comme système central d'authentification pour toutes les machines du réseau.
  + Les deux machines Windows et le serveur Windows sont membres du domaine AD.
* LDAP (Lightweight Directory Access Protocol) :
  + Mis en place sur le serveur Windows pour faciliter l'authentification des utilisateurs.
  + Utilisé pour l'intégration de la machine Linux au domaine AD.
* DNS (Domain Name System) :
  + Géré par le serveur Windows, responsable de la résolution des noms de domaine au sein du réseau.
  + Point crucial pour la connectivité et l'acheminement du trafic réseau.
* Pfsense :
  + Fonctionne comme un routeur permettant le contrôle du trafic réseau.
  + Règles de pare-feu configurées pour réguler le trafic entre les différentes machines du réseau.
* Machine Linux (Debian) :
  + Héberge un site web accessible via linux.ad.atelier3.com.
  + Intégration au domaine AD pour une authentification centralisée.

### Points d'Intérêt

* Site Web (React):
  + L'URL linux.ad.atelier3.com est une surface d'attaque potentielle.
  + La machine Linux, bien qu'étant dans le domaine AD, peut représenter un point d'entrée vulnérable.
* LDAP et Authentification :
  + Le protocole LDAP utilisé pour l'authentification pourrait être ciblé.
  + Une compromission réussie pourrait compromettre l'ensemble de l'infrastructure.
* Serveur DNS :
  + Un point critique pour la résolution des noms de domaine.
  + Une compromission pourrait entraîner des attaques de redirection ou d'empoisonnement DNS.

## Scénario

Le réseau sous investigation est représentatif d'un environnement d'entreprise typique, pris en charge par un administrateur réseau dédié. La configuration inclut un service d'annuaire LDAP, spécifiquement Active Directory, déployé sur l'ensemble des machines. Malheureusement, malgré l'automatisation de certaines tâches par l'administrateur réseau, les bonnes pratiques de sécurité n'ont pas été pleinement prises en compte. De plus, la vigilance des utilisateurs face aux menaces de phishing par courrier électronique n'est pas uniforme.

### Phase d'Exploration

L'attaque débute par la recherche d'une surface d'attaque potentielle. Le site web de l'entreprise, accessible depuis l'internet, est identifié comme une cible. Les attaquants décident d'utiliser une approche de force brute pour compromettre des identifiants d'accès au site web.

### Phase d'Exploitation

Après avoir réussi à obtenir des identifiants via une attaque de force brute, les attaquants exploitent une vulnérabilité sur le site web en utilisant une injection SQL. Cette méthode leur permet d'extraire des informations sensibles du serveur, y compris une adresse e-mail associée à un utilisateur du service LDAP (Active Directory).

### Phase de Phishing

Forts de l'adresse e-mail obtenue, les attaquants lancent une campagne de phishing visant l'utilisateur associé au compte LDAP compromis. L'objectif de la tentative de phishing est de tromper l'utilisateur afin qu'il divulgue ses identifiants LDAP, en exploitant la confiance liée à une communication apparemment légitime.

### Phase d'Escalade

Une fois en possession des identifiants LDAP de l'utilisateur compromis, les attaquants exploitent cette victoire pour se connecter au domaine. À ce stade, une analyse attentive du réseau révèle l'exécution régulière d'un script via le Task Scheduler, orchestré par l'administrateur du domaine.

### Modification du Script

Profitant de l'accès au domaine, les attaquants prennent le contrôle du script en cours d'exécution dans le Task Scheduler. Cela leur offre la possibilité de modifier le script pour des activités malveillantes, ainsi que de lire son contenu pour identifier toute information sensible qui pourrait être exploitable à leur avantage.

# Exploitation des failles

Les entreprises les plus touchées par les cyberattaques sont les petites entreprises, car beaucoup moins bien protégées que les grandes entreprises. Nous allons donc simuler une petite entreprise, concurrente à Spotify et Deezer, nommée Spotizer (oui le nom était facile à trouver) et tenter d’obtenir les accès root de leur système d’exploitation.

## Brute Force de session

Le brute force de session consiste à tenter de deviner la bonne combinaison nom d’utilisateur/mot de passe d’une session, de manière automatisée en essayant toutes les combinaisons possibles, pour en obtenir les accès.

Pour gagner du temps, il existe quelques outils qui permettent de faciliter la découverte de ces combinaisons. En effet, certains noms d’utilisateurs et mots de passe sont très fréquemment utilisés. On peut retrouver un [exemple sur github](https://github.com/insidetrust/statistically-likely-usernames). Etant donné que ces noms d’utilisateurs sont des noms américains et que notre entreprise est française, nous avons demandé à chatGPT de nous générer un document similaire mais [avec des noms d’utilisateur français](https://gitlab.com/VillechenaudSimon/uqac-cyber-project-3/-/blob/main/bruteforce/brute_usernames?ref_type=heads). Nous avons aussi trouvé un [top 5000 de mots de passe](https://github.com/tarraschk/richelieu) couramment utilisés par les utilisateurs français.

La prochaine étape consiste alors à trouver un couple nom d’utilisateur/mot de passe pour parvenir à entrer dans le site.

Nous avons alors créé un [script](https://gitlab.com/VillechenaudSimon/uqac-cyber-project-3/-/blob/main/bruteforce/bruteforce.sh?ref_type=heads) capable de faire ceci.

En lançant le script, nous avons pu trouver un couple nom d’utilisateur/mot de passe :

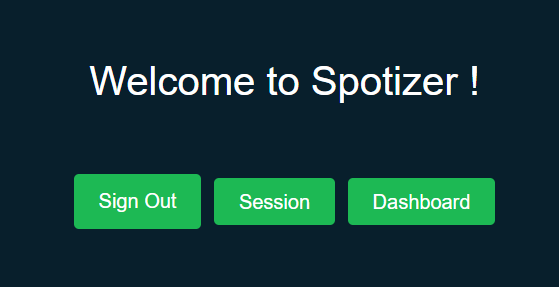
nom d’utilisateur : sleroy

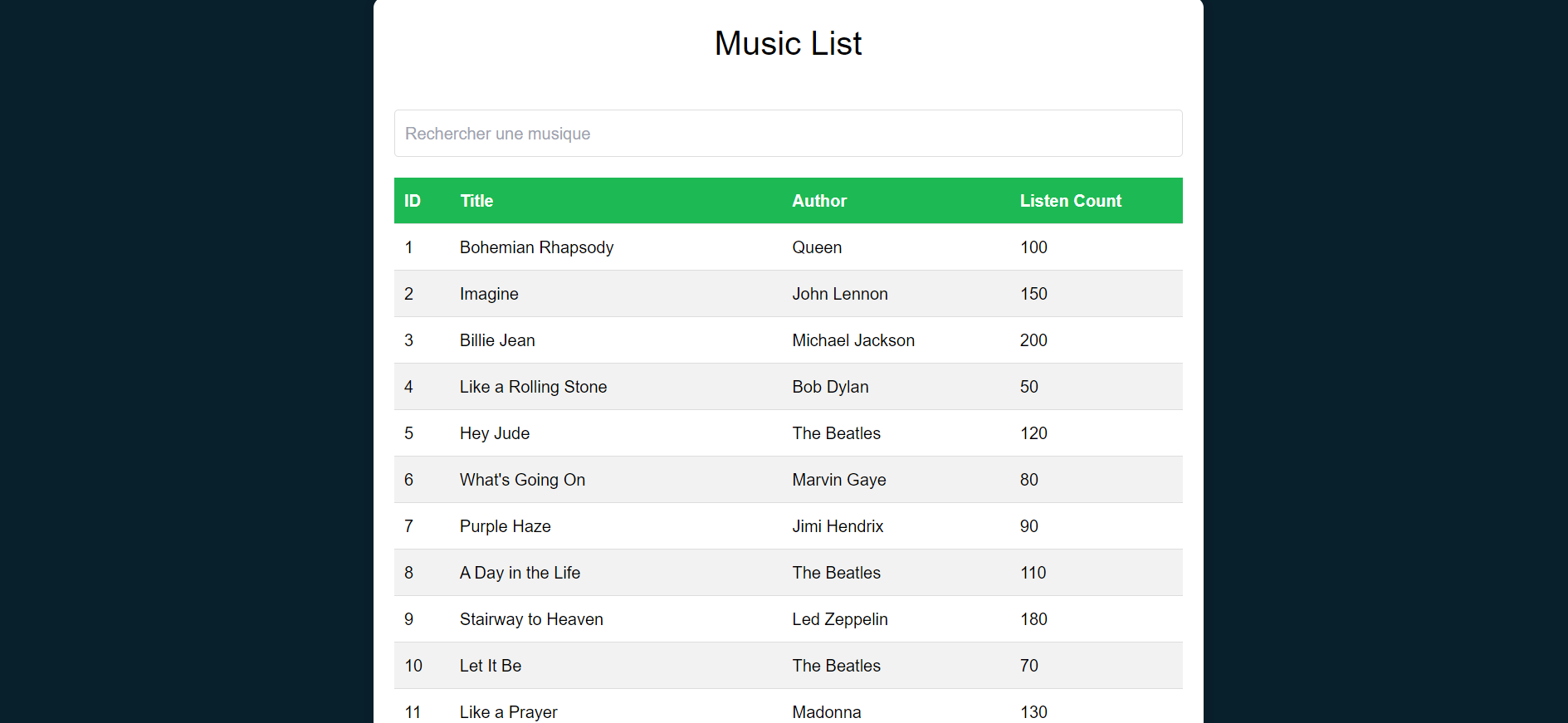
mot de passe : L58jkdjP!m

On peut alors entrer sur le site web.

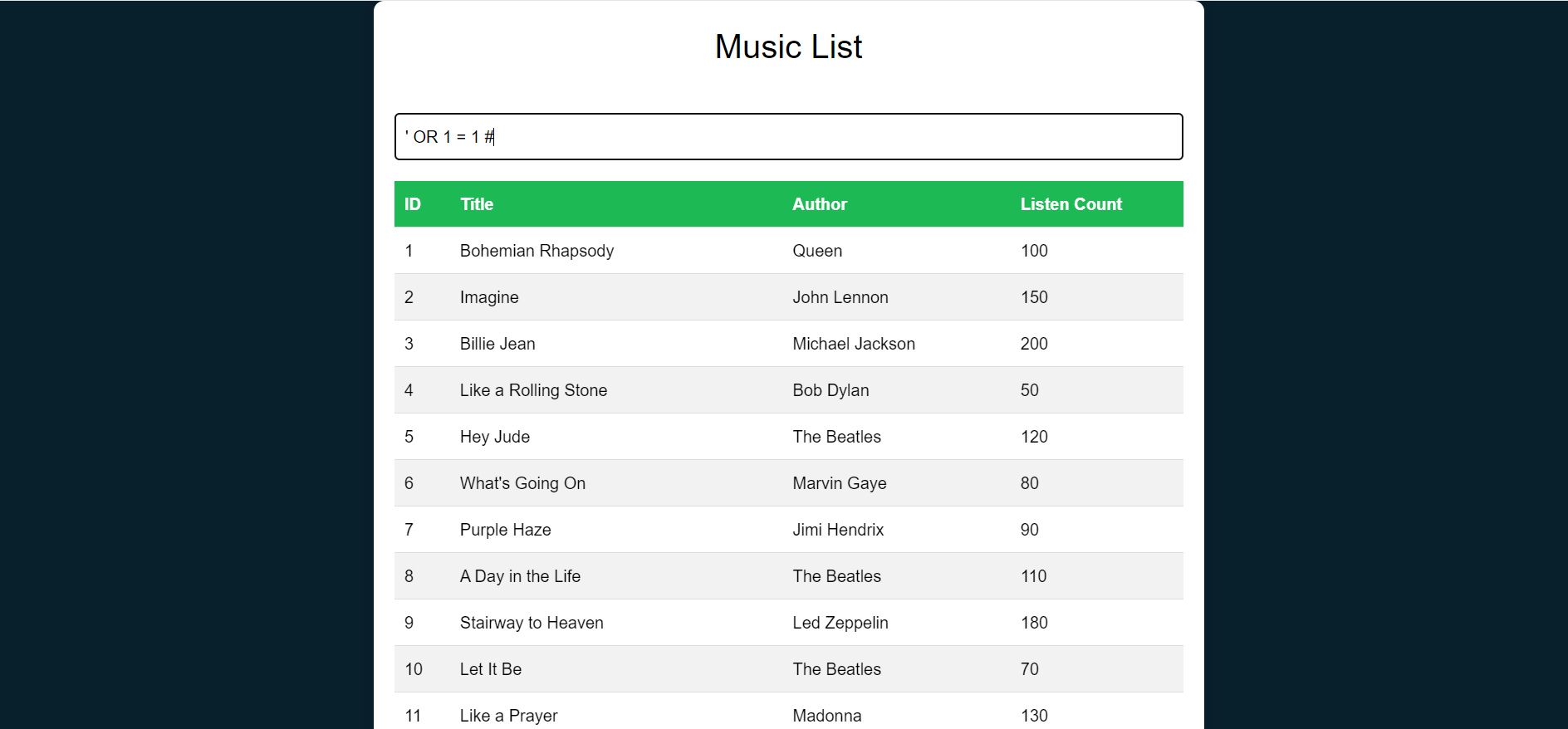
## Injection SQL

Une fois qu’on est connecté en tant que ‘sleroy’ sur le site web on voit qu’un bouton nous permettant d’aller sur une page nommée “dashboard” est apparu.

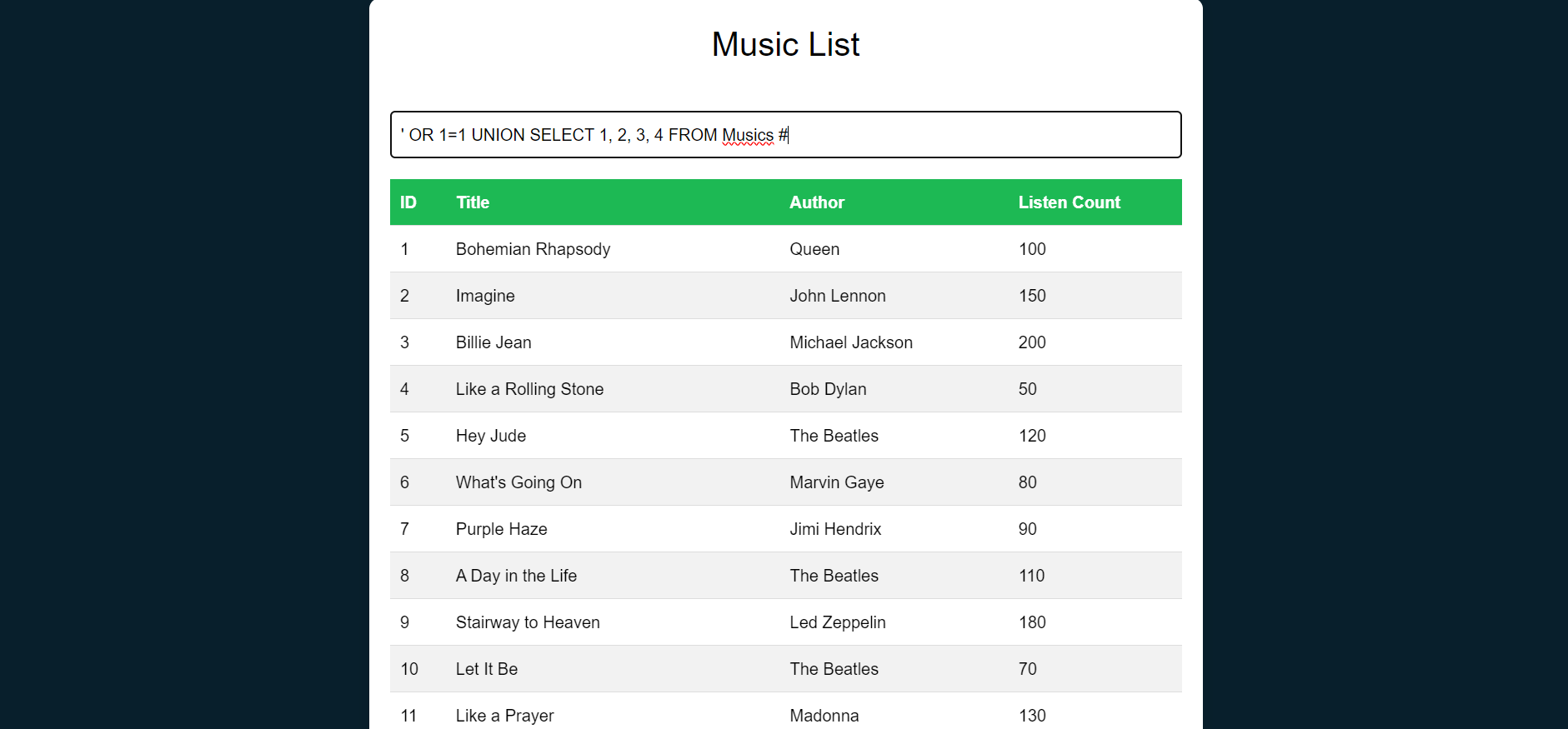




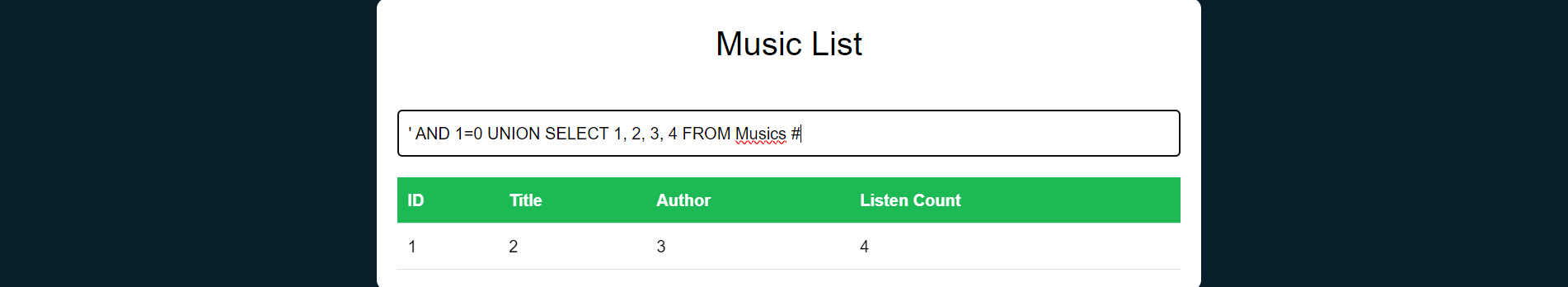
Sur cette page, nous avons accès à une barre de recherche nous permettant de filtrer la liste des musiques affichées en fonction du nom. En entrant ' OR 1=1 # dans la barre de recherche, on observe que l’ensemble des musiques reste affiché ce qui laisse penser que cette page est vulnérable aux attaques via injection SQL.



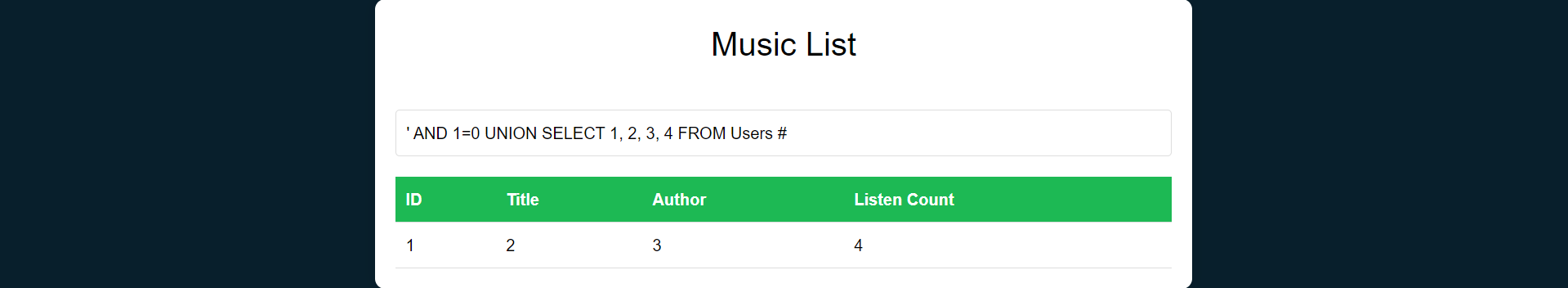
Nous allons donc essayer d’extraire des informations contenues dans la base de données via cette faille. On remarque que 4 champs sont affichées dans la table qui liste les musiques ainsi on essaye d’entrer ' OR 1=1 UNION SELECT 1, 2, 3, 4 FROM Musics # dans la barre de recherche en supposant l'existence d’une hypothétique table nommée ‘Musics’ (ce qui est probable vu que c’est ce que nous liste le site). L’idée derrière cette tentative est de trouver le nombre de champs qui sont initialement sélectionnés par la requête afin de pouvoir faire un union dessus pour pouvoir afficher des informations provenant d’autres tables que Musics dans le tableau. En effet, on remarque qu’une nouvelle ligne contenant les valeurs 1, 2, 3 et 4 est apparue à la fin du tableau.



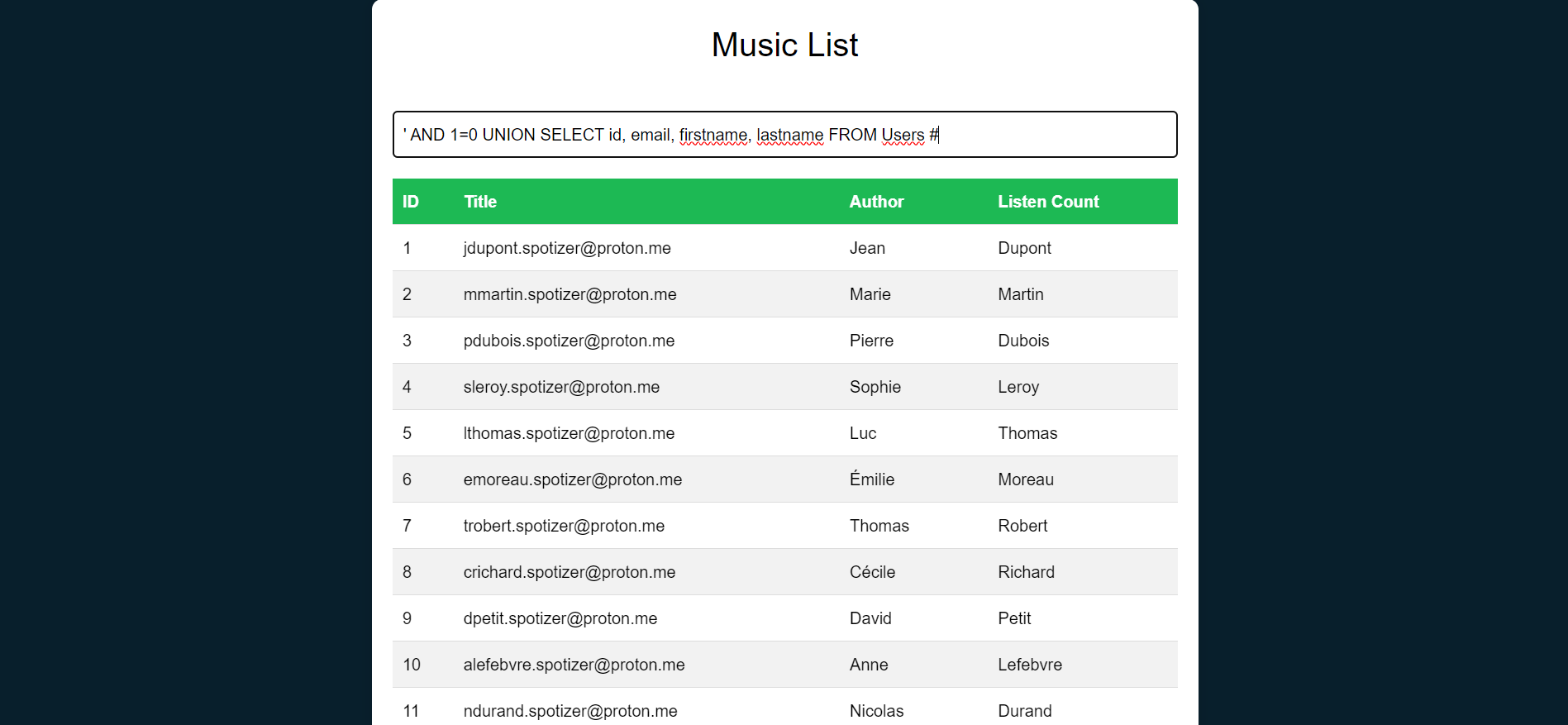
On en conclut que la requête initiale sélectionne 4 champs de la table Musics. Notez que si la requête avait échoué et qu’aucun résultat ne s’était affiché dans le tableau il aurait été possible de réessayer avec d’autres nombres de colonne et d’autres noms de table pour ‘Musics’. Afin de nettoyer un peu l’affichage pour mettre l’accent sur les informations que l’on ajoute à la table, on change la chaîne de caractères utilisée par la suivante : ' AND 1=0 UNION SELECT 1, 2, 3, 4 FROM Musics # afin de n’afficher que le résultat de la seconde requête de la clause union (étant donné que 1=0 est tout le temps faux).

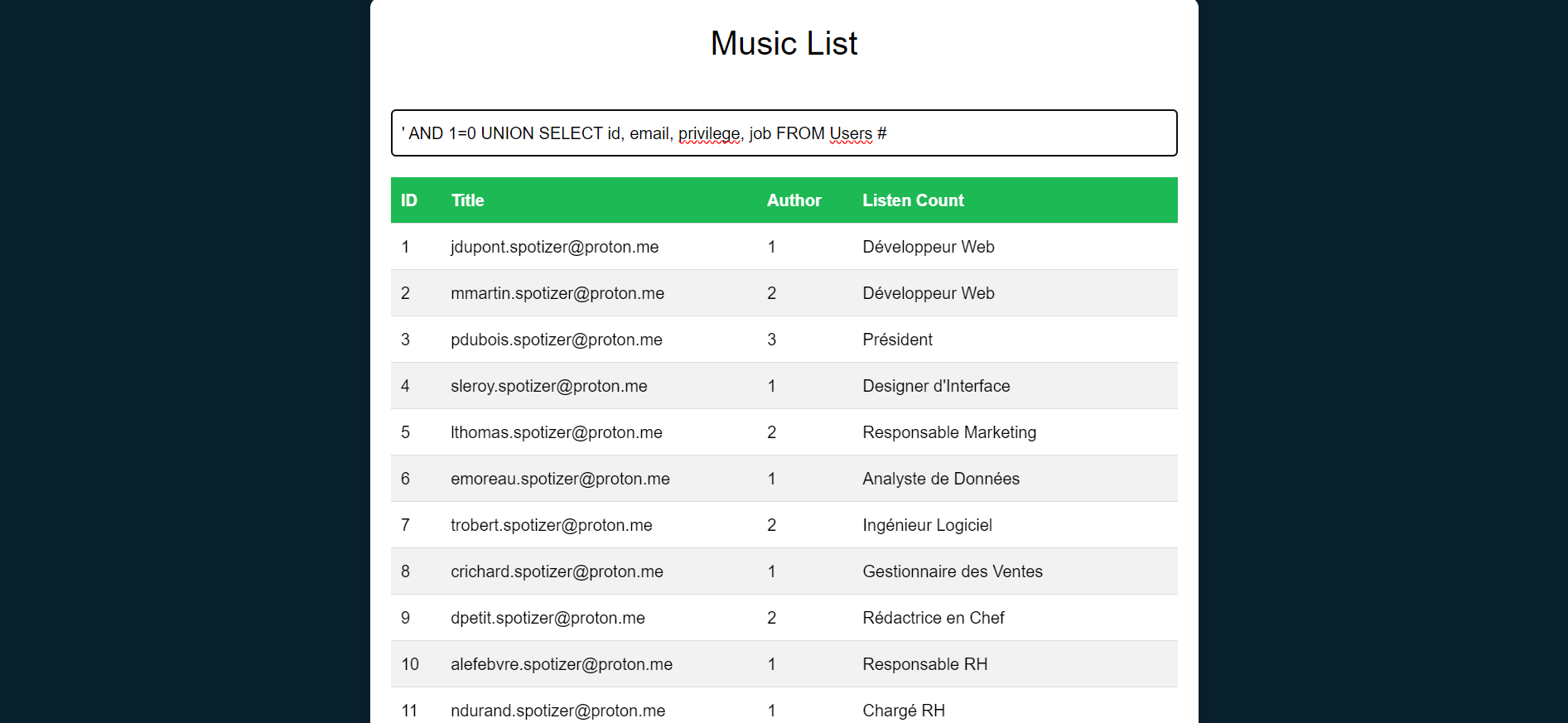


On va maintenant chercher les noms des tables qui existent dans la base de données en changeant le ‘Musics’ avec notre guess. Si le résultat est toujours ‘1 2 3 4’ alors la table existe, si rien ne s’affiche alors la table n’existe pas. Ainsi, en procédant par tâtonnement, on fini par trouver l’existence d’une table ‘Users’ : ' AND 1=0 UNION SELECT 1, 2, 3, 4 FROM Users #



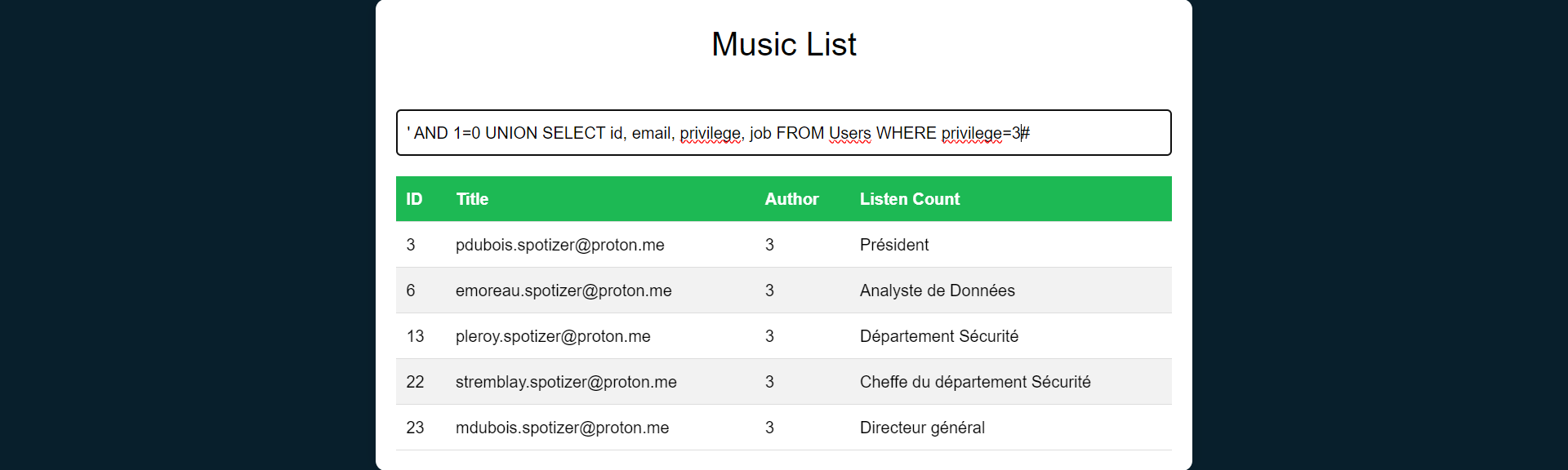
Maintenant qu’on a trouvé une table intéressante, on va encore procéder par tâtonnement pour identifier les colonnes de cette table en testant des noms communs pour ce genre de table (id, userId, name, username, firstname, lastname, age, email etc..). Ainsi, on obtient avec l’injection de ' AND 1=0 UNION SELECT id, email, firstname, lastname FROM Users # le résultat illustré dans la figure TODO: num. En analysant les emails de cette dernière requête on se rend compte que les emails correspondent à des emails de Spotizer et que la table Users est juste mal nommée puisque nous avons en réalité obtenu des informations personnelles concernant l’ensemble des employés de l’entreprise. Également, avec l’injection de ' AND 1=0 UNION SELECT id, email, privilege, job FROM Users # on obtient d’autres informations concernant ces employés notamment leur position dans l’entreprise et le niveau de privilèges que cela leur procure dans le système informatique.





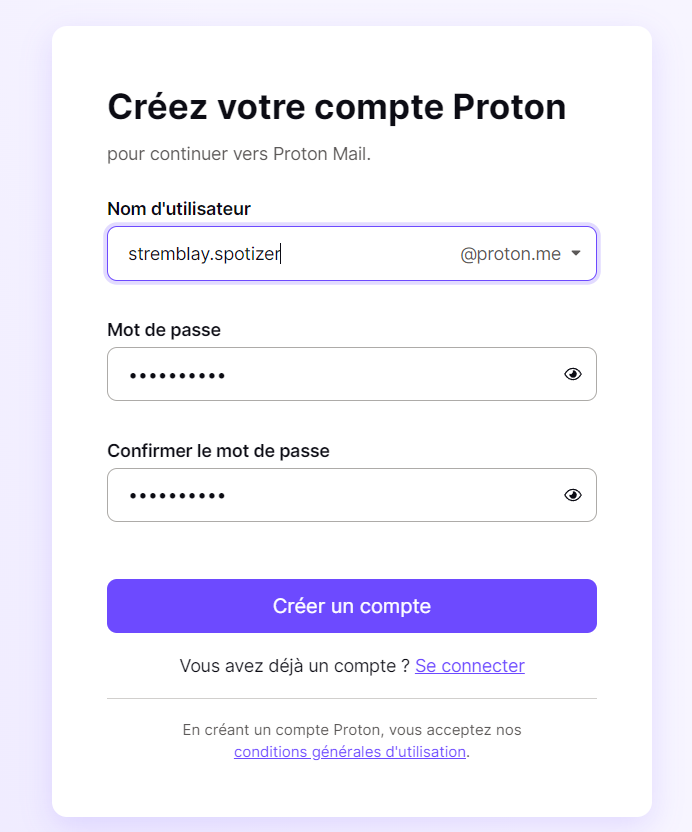
## Phishing

Maintenant que nous avons obtenu les informations sur les employés de l’entreprise, on peut s’en servir pour continuer notre intrusion. Comme nous avons pu le remarquer, la personne dont nous possédons les accès à des accès de niveau 1. Mais certaines personnes ont des accès de niveau 3, ce qui laisse entendre que ce serait des accès haut niveau, étant donné que c’est le niveau que possède le chef du département sécurité. Cependant, cela ne signifie pas que ce sont des accès administrateur non plus. On ne le saura qu’une fois qu’on l’aura.



Nous allons donc tenter d’obtenir ces accès en poussant les utilisateurs à nous donner eux même leurs codes d’authentification.

Logiquement, la personne la plus à même de demander aux utilisateurs de changer leurs accès est la cheffe du département de sécurité. On va donc créer un mail similaire au sien, en changeant par exemple le “L” en “i” majuscule. On y voit que du feu !



On va ensuite créer un joli mail, expliquant aux utilisateurs qu’il est nécessaire de changer leur mot de passe. Voici donc le mail que nous allons envoyer à tous les utilisateurs de niveau 3 :

*“Objet : Action requise : Réinitialisation de votre mot de passe Spotizer*

*Chers employés de Spotizer,*

*Nous prenons la sécurité de vos comptes et de nos systèmes très au sérieux chez Spotizer. Malheureusement, nous avons récemment détecté une tentative d'accès non autorisé à nos systèmes, ce qui a compromis la sécurité de certains comptes utilisateur, y compris le vôtre.*

*Par mesure de précaution, nous vous demandons de réinitialiser votre mot de passe immédiatement. Voici comment procéder :*

*1. Accédez à la page de réinitialisation du mot de passe de Spotizer en utilisant le lien suivant : [lien]*

*2. Suivez les instructions fournies sur la page pour réinitialiser votre mot de passe. Assurez-vous de choisir un mot de passe fort et unique que vous n'avez pas utilisé ailleurs.*

*La sécurité de vos informations personnelles et de notre entreprise est notre priorité absolue. Nous nous excusons pour tout inconvénient que cela pourrait causer et vous remercions de votre coopération pour maintenir un environnement en ligne sécurisé.*

*Merci pour votre compréhension et votre vigilance.*

*Cordialement,*

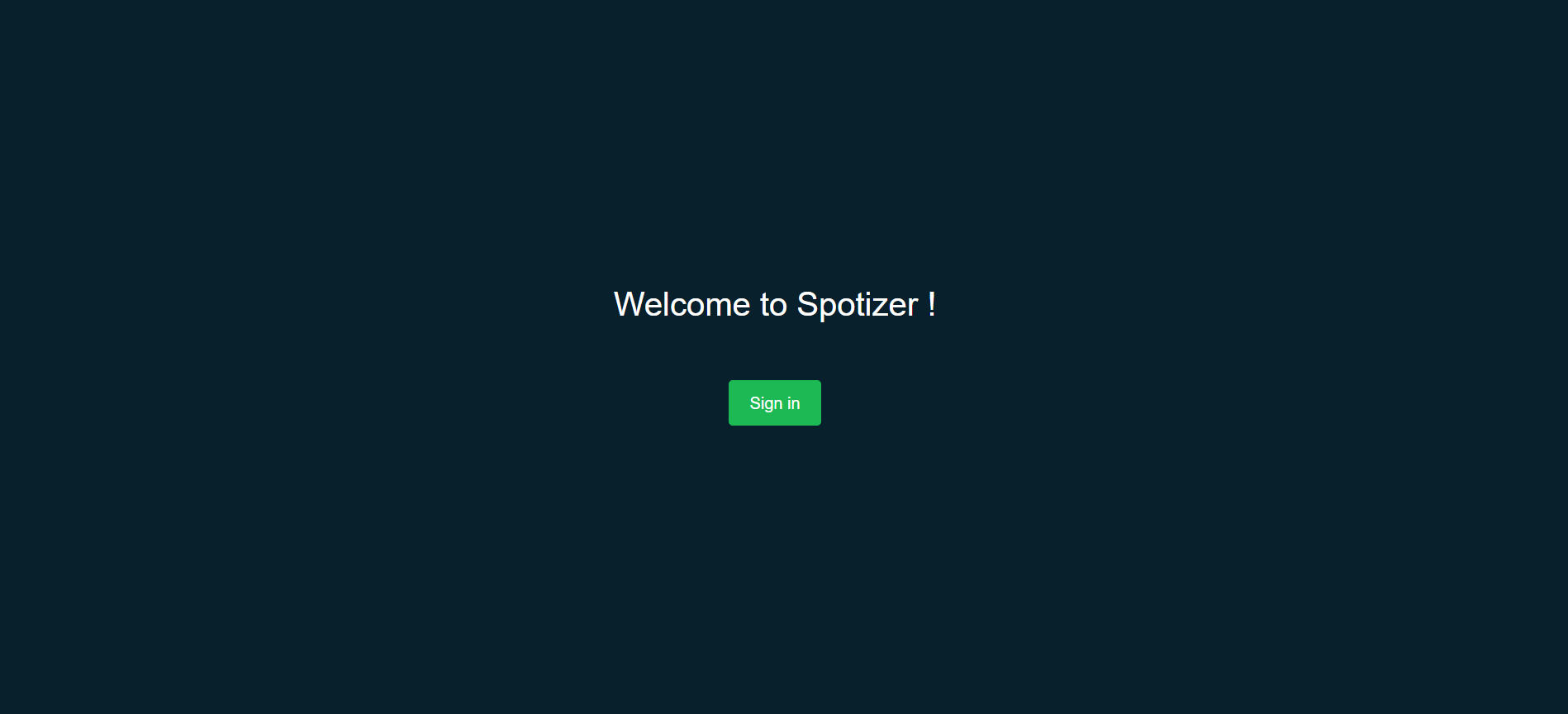
*Sylvie Tremblay*

*Cheffe du département Sécurité*

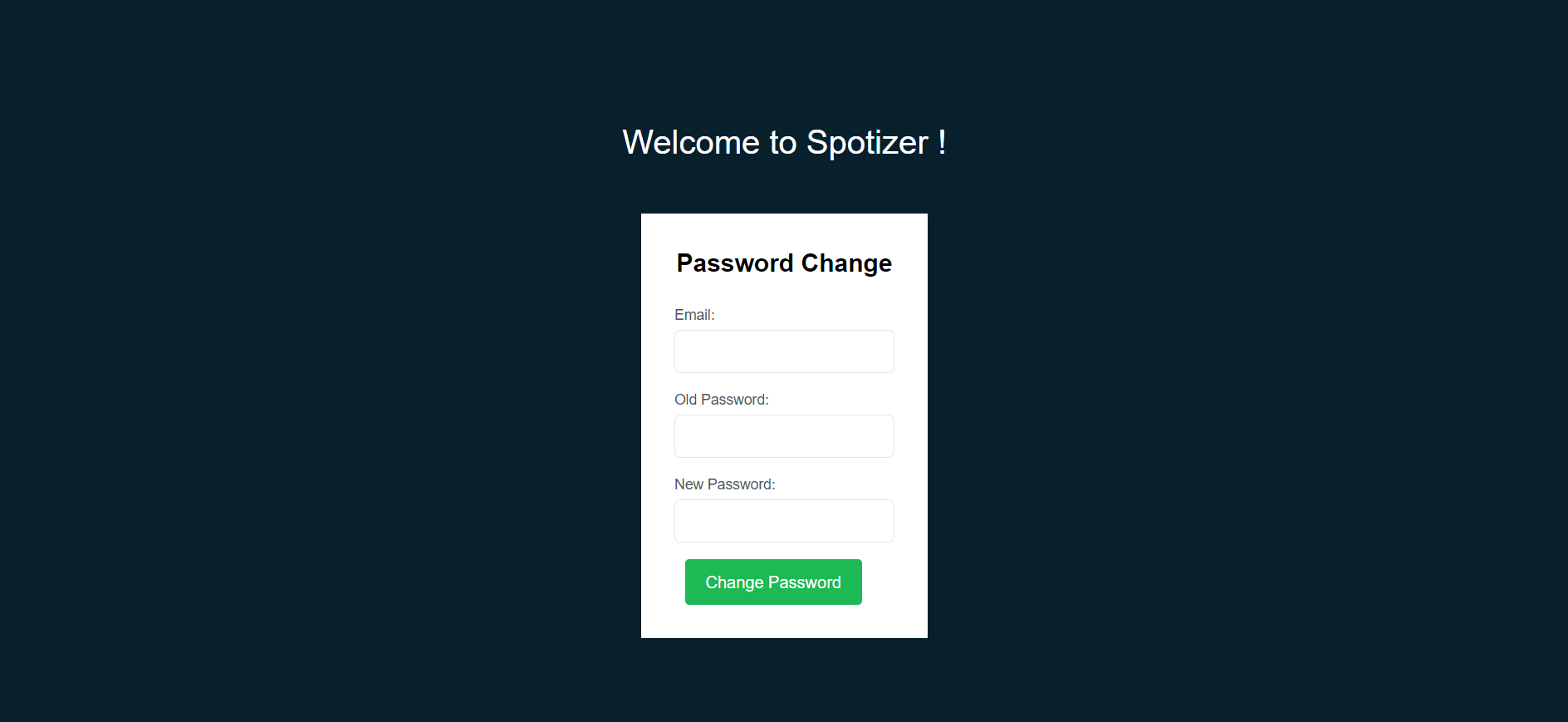
*Spotizer”*

Mais pour récupérer ce mot de passe, il faut bien évidemment une page web cohérente, capable de tromper l’utilisateur. Dans l’idéal, il serait judicieux de prendre un nom de domaine qui ressemble au nom de domaine de l’entreprise afin de gagner en crédibilité. Comme c’est payant, nous n’irons pas jusque là pour notre simulation. Cependant, nous allons prendre soin de recopier la charte graphique du site pour plus de cohérence.

Leur site :



Notre site :

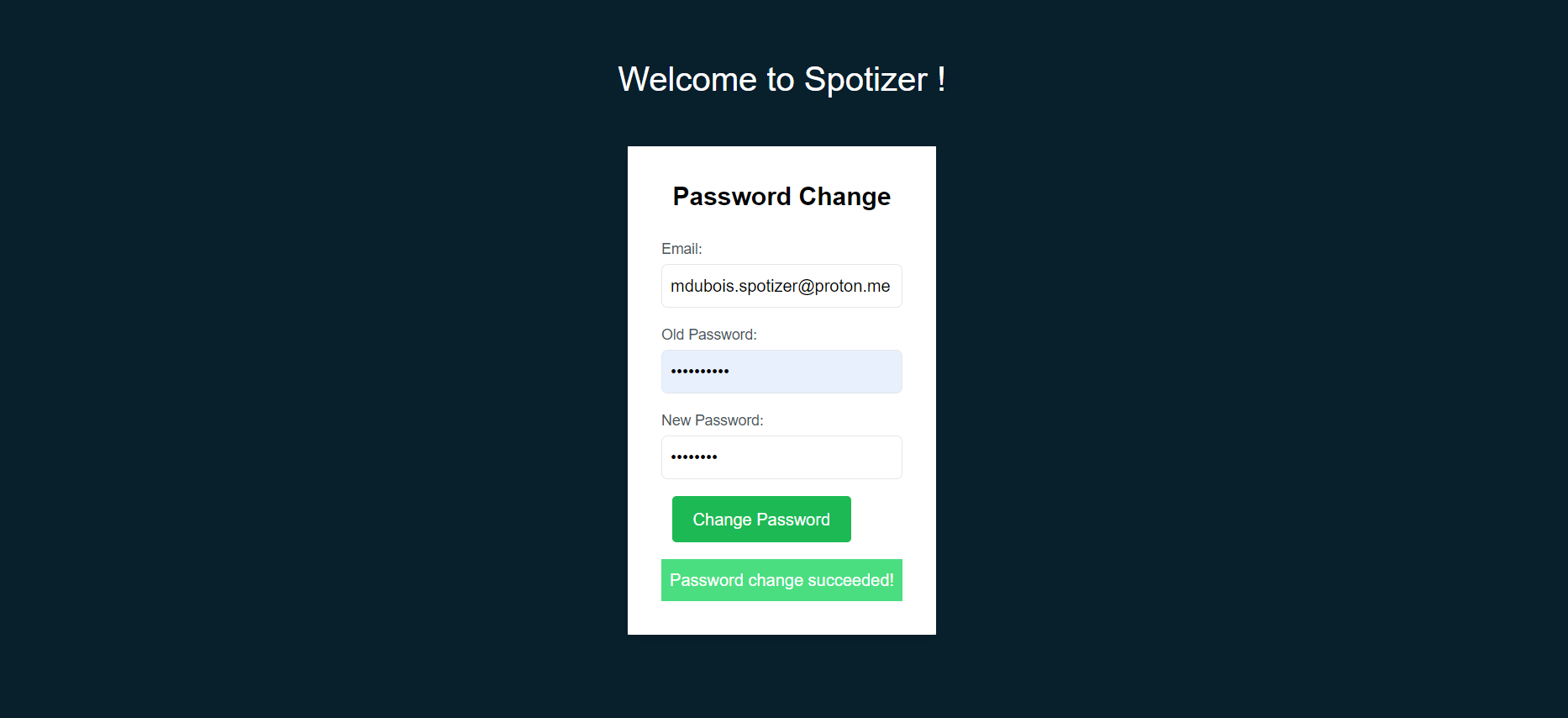


Ensuite, si on a de la chance, quelqu’un tombera dans le panneau. Nous allons estimer que nous avons de la chance et que c’est le cas.

En regardant quelques heures plus tard dans les logs de notre serveur, nous avons pu obtenir les identifiants d’un compte :



Voici ce qu’a vu notre ami Marc au moment de changer son mot de passe.



Techniquement, nous pourrions créer un script capable de changer son mot de passe sur le vrai site depuis notre interface. Ainsi, il n’y verrait que du feu. Mais cela n’a pas été mis en place dans notre simulation, alors, nous changeons le mot de passe à la main pour ne pas éveiller ses soupçons. Nous avons maintenant les accès du compte LDAP d’un utilisateur de niveau 3 !

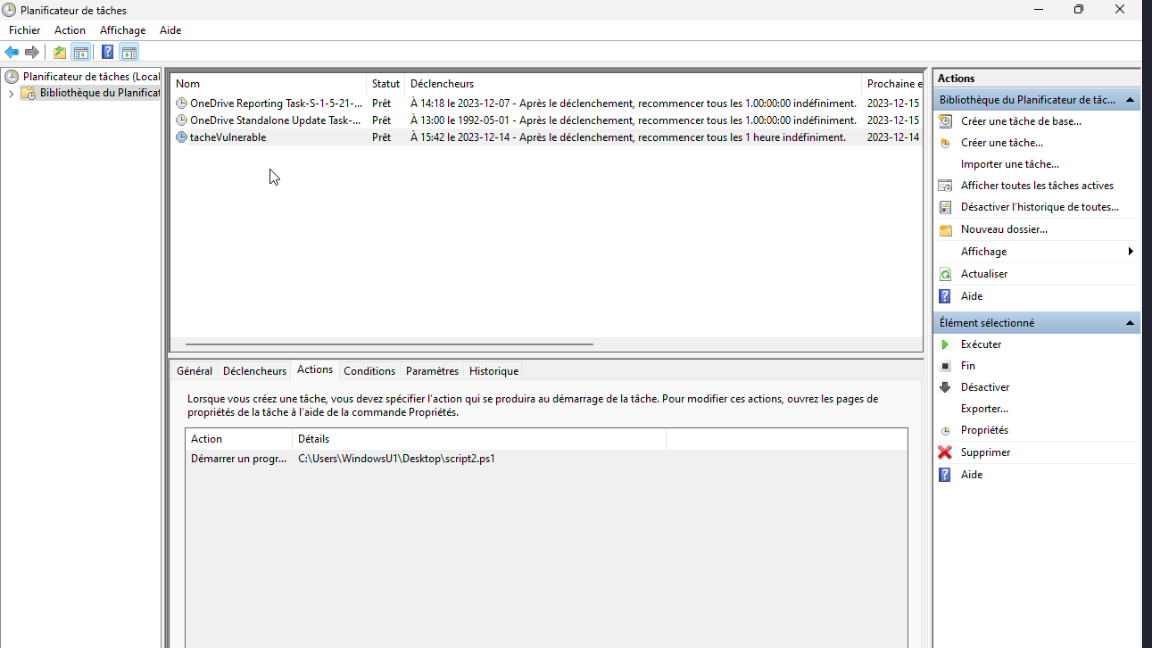
## Mauvaise Configuration

Suite à la compromission du compte de Marc DUBOIS, nous avons pu acquérir un accès en tant qu'utilisateur compromis sur une machine Windows. Après quelques tests, nous avons pu nous rendre compte que Marc n’avait pas les accès administrateur, bien que ses accès soient plus élevés que la plupart des autres employés. Nous allons donc devoir continuer à chercher comment obtenir ces accès.

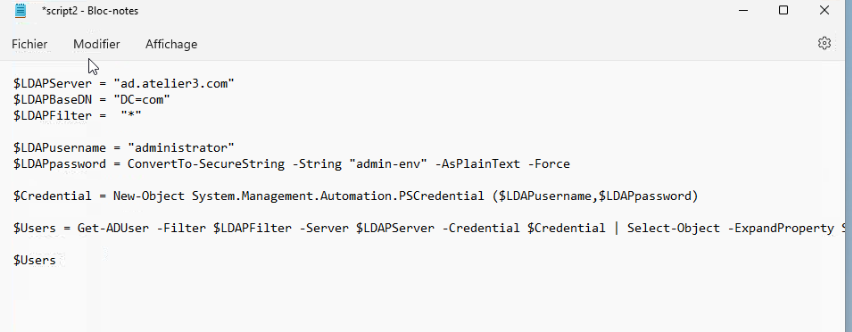
À ce stade, l'utilisation d'outils tels que [WinPeas](https://github.com/carlospolop/PEASS-ng/blob/master/winPEAS) peut être employée pour détecter d'éventuelles anomalies sur le système compromis.

L'utilisation de WinPeas offre une visibilité approfondie sur la configuration du système, identifiant les vulnérabilités potentielles, les privilèges élevés, et d'autres points de faiblesse qui pourraient être exploités par les attaquants.

Au cours de la simulation d'attaque, une observation attentive du système a révélé la présence d'un script s'exécutant de manière régulière via le Task Scheduler. Cette tâche automatisée, initialement configurée par l'administrateur du domaine, avait pour but d'automatiser certaines opérations au sein du réseau.



Contenu du script :



En examinant le script, il est devenu évident que son objectif principal était de récupérer l'ensemble des utilisateurs du domaine. Cette fonctionnalité, bien que potentiellement utile à des fins d'automatisation, introduit un risque considérable, car elle pourrait être exploitée de manière malveillante pour des actions non autorisées.

Une analyse approfondie du script en question a mis en lumière une série de lacunes graves en termes de sécurité. Tout d'abord, les identifiants de l'administrateur du domaine étaient stockés en clair dans le script, créant une vulnérabilité majeure. La présence de ces informations sensibles dans un fichier accessible aux attaquants représente un risque sérieux pour la sécurité du réseau.

La mauvaise configuration de ce script présente plusieurs risques majeurs pour la sécurité du réseau :

* **Exposition des Identifiants Administrateur** : Les identifiants de l'administrateur du domaine étant stockés en clair, un accès non autorisé à ce script permettrait à un attaquant de compromettre les droits administratifs du réseau.
* **Collecte de Données Sensibles :** La fonction de récupération de l'ensemble des utilisateurs du domaine peut être exploitée pour collecter des données sensibles sur les utilisateurs, potentiellement exposant des informations confidentielles.

# Correction des failles

Notre projet a mis en évidence plusieurs failles de sécurité importantes, y compris des attaques par bruteforce, des injections SQL, des tentatives de phishing, et des problèmes liés à des configurations inadéquates. Voici les mesures correctives recommandées pour chaque type de vulnérabilité identifiée :

## Brute Force

Pour contrer les attaques par brute force, nous recommandons de mettre en place une politique de mots de passe robustes, incluant des exigences de complexité (caractères spéciaux, lettres majuscules et minuscules, des chiffres, etc.) et de renouvellements réguliers. Attention, renouveler régulièrement les mots de passe peut mener à une baisse de leur efficacité s' ils sont choisis dans le but d’être facilement retenu, c’est pourquoi cette dernière recommandation est surtout efficace lorsqu’un gestionnaire de mots de passe est utilisé. Il est aussi conseillé de bloquer les possibilités d’authentification après plusieurs tentatives infructueuses, avec un temps d’attente obligatoire par exemple. Enfin, l'utilisation de systèmes de détection d'intrusion (IDS) pour surveiller les tentatives de connexion suspectes peut être d’une grande aide : il est possible de d’ignorer les requêtes provenant d’une certaine adresse IP si cette dernière est à l’origine d’un trop grand nombre de tentatives.

## Injection SQL

Afin de prévenir les injections SQL, il est crucial de valider et de nettoyer toutes les entrées utilisateur dans les applications web. L'utilisation de requêtes préparées et l'adoption de principes de programmation sécurisée sont des stratégies efficaces pour mitiger ce risque. Par exemple, il faut assainir les données présentes dans les champs d’entrées en filtrant les caractères spéciaux qui n’ont pas de sens à être utilisés dans le contexte. Cependant, la solution la plus efficace reste d’utiliser des librairies de construction de requêtes ou des librairies qui fournissent un ORM (Object-Relational Mapping). Ainsi, la responsabilité d’éviter la présence de faille SQLI leur est transférée, il suffit donc de choisir une librairie sécurisée et de confiance.

## Phishing

Pour le phishing, la sensibilisation et la formation continue des employés sont fondamentales. Précisément, il faut inciter les employés à vérifier la validité de quelques paramètres comme l’URL vers laquelle ils sont redirigés (noms de domaine identiques à l’officiel). De plus, l'implémentation de solutions de filtrage d'email et l'adoption de protocoles d'authentification des emails tels que SPF, DKIM et DMARC peuvent réduire significativement le risque d'attaques de phishing réussies.

## Mauvaise configuration : Accès anormaux

Les problèmes liés à une mauvaise configuration peuvent être résolus en effectuant des audits de configuration réguliers et en suivant les meilleures pratiques de sécurité, telles que le principe du moindre privilège et la sécurisation des interfaces de gestion.

# Conclusion

Cet atelier de cybersécurité a mis en évidence la complexité et l'importance vitale de protéger les systèmes d'information contre une gamme croissante de menaces. À travers l'analyse et la correction de diverses vulnérabilités, allant des attaques par bruteforce et injections SQL aux risques liés au phishing et aux configurations inadéquates, nous avons acquis une compréhension approfondie des défis de la sécurité informatique dans le monde moderne.

La mise en œuvre des mesures correctives proposées démontre notre engagement à maintenir une posture de sécurité proactive. De plus, la sensibilisation et la formation des employés sur les risques de cybersécurité sont des éléments clés pour renforcer la défense globale de l'organisation.