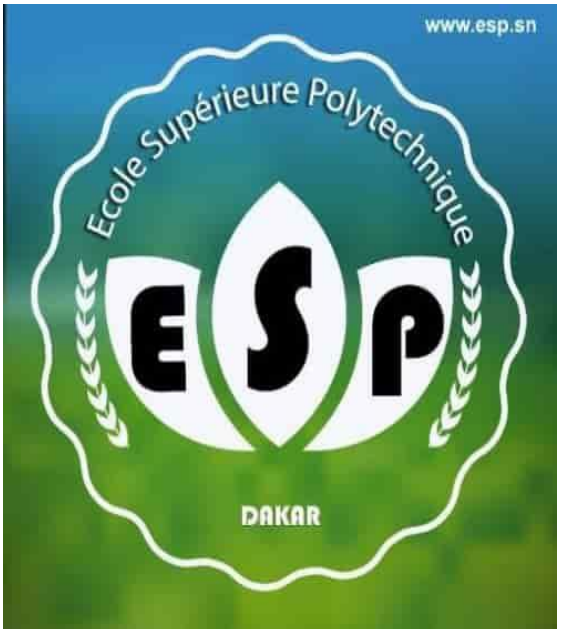
Université Cheikh Anta Diop de Dakar

Ecole Supérieure Polytechnique




Département Génie Informatique

Ingénierie Cryptographique

**Membres du groupes**

Haby DIOP

Mariama Ka

Marième AIDARA

Papa Cheikh GNINGUE

Taamba Bedel Brice THIOMBIANO

Année anniversaire : 2022/2023

# Plan

I. Matching des concepts avec une partie du cours

II. Traiter la catégorie par rapport à elle-même (CVE et CWE associées)

III. Création de notre propre scénario

IV. Outils pour mettre en place les scenarios et les bonnes pratiques

V. Implémentation d’un scénario

VI. Les mesures préventives

## I. Matching des concepts avec une partie du cours

La confirmation de l'identité, de l'authentification et de la session de l'utilisateur sont essentielles pour se protéger des attaques liées à l'authentification. Cependant, Il peut y avoir des faiblesses d'authentification si l'application autorise :

- Des Attaque par force brute : lorsque l'attaquant a la possibilité de tenter toutes les clés une par une pour le décryptage : (chapitre1 _ page 52)
- D'utiliser des mots de passe en texte brut, chiffrés ou faiblement hachés : dus à la mauvaise utilisation de primitives cryptographiques tels que le chiffrement et des fonctions de hachages, dont il est question dans le chapitre1 du cours à la page 23.
- D'autoriser l'authentification par défaut

C'est dû à l'utilisation des mots de passe par défaut, faibles ou bien connus, tels que "Password" ou "admin" ou « passer ». Cela va entrainer la violation des services de sécurités à savoir la confidentialité et l'authentification.

Le but premier de l'utilisation de la cryptographie est de garantir les quatre services fondamentaux de la sécurité des informations :

- **Confidentialité** : C'est un service de sécurité qui préserve l'information d'une personne non autorisée. On parle parfois de vie privée ou de secret. La confidentialité peut être obtenue grâce à de nombreux moyens allant de la sécurisation physique à l'utilisation d'algorithmes mathématiques pour le cryptage des données.

- **L'intégrité des données** : C'est le service de sécurité qui s'occupe d'identifier toute altération des données. Le destinataire d'un message doit pouvoir vérifier que celui-ci n'a pas été modifié en chemin. Un intrus ne doit pas être capable de faire passer un faux message pour un légitime.

- **Authentification** : L'authentification fournit l'identification de l'auteur. Il confirme au destinataire que les données reçues ont été envoyées par un expéditeur identifié et vérifié. Un intrus ne doit pas être capable de se faire passer pour quelqu'un d'autre. Le service d'authentification comporte deux variantes : **L'authentification de message** identifie l'auteur du message sans aucun routeur ou système qui envoie le message et **l'authentification d'entité** est l'assurance que la donnée a été reçue d'une entité spécifique, par exemple un site Web particulier.

- **Non-répudiation** : C'est un service de sécurité qui garantit qu'une entité ne peut pas refuser la propriété d'un engagement antérieur ou d'une action. La non-répudiation est une propriété qui est la plus souhaitable dans les situations où il y a des possibilités de conflit sur l'échange de données.

A. Intégrer des tests de mots de passes faibles, à la création ou utiliser des mots de passe cryptés ou chiffrés :

D'abord,

Les mots de passes faibles : Ce sont les données à protéger pendant la transmission.

Le chiffrement. C'est un processus de transformation d'un message de manière à le rendre incompréhensible. Le résultat de ce processus de chiffrement est appelé texte chiffré ou encore cryptogramme.

Le texte chiffré. C'est la version brouillée du texte en clair produit par le chiffrement. Le texte chiffré n'est pas protégé. Il circule sur le canal public et il peut être intercepté ou compromis par quiconque qui a accès au canal de communication.

Le déchiffrement. C'est le processus de reconstruction du texte en clair à partir du texte chiffré.

L'algorithme cryptographique. C'est une fonction mathématique utilisée pour le chiffrement et le déchiffrement.

La clé de chiffrement. C'est une valeur qui est connue de l'expéditeur. L'expéditeur entre la clé de chiffrement dans l'algorithme de chiffrement avec le texte en clair afin de calculer le texte chiffré, on constate deux types de chiffrement :

- Le chiffrement symétrique où les mêmes clés sont utilisées pour crypter et déchiffrer les informations.
- Le chiffrement asymétrique dans lequel différentes clés sont utilisées pour crypter et déchiffrer les informations.

B) Utiliser des fonctions de hachages

Les fonctions de hachage peuvent être divisées en deux classes :

- Les fonctions de hachage sans clé, dont la spécification requiert un seul paramètre d'entrée (un message) ;
- Les fonctions de hachage à clé, dont la spécification requiert deux entrées distinctes, un message et une clé secrète.

Une fonction de hachage est une fonction h qui a, au minimum, les deux propriétés suivantes :

- Compression : h applique une entrée x de longueur de bit finie arbitraire, à une sortie h(x) de longueur de bit fixe n.
- Facilité de calcul : étant données h et une entrée x, h(x) est facile à calculer.

Exemples : SHA-512, etc.

Maintenant pour s'en prémunir il faut :

Implémentez l'authentification multifacteur pour éviter les attaques automatisées, le bourrage des informations d'identification, la force brute et la réutilisation des informations d'identification volées.

L'authentification multifacteur (MFA) est une méthode d'authentification dans laquelle l'utilisateur doit fournir au minimum deux facteurs de vérification pour accéder à une ressource de type application, compte en ligne ou VPN.

Intégrer des tests de mots de passes faibles, à la création ou au changement. Soit le comparer ce mot de passe avec une liste de mots de passe les plus faibles ou bien éviter D'utiliser des mots de passe en texte brut, chiffrés ou faiblement hachés.

Utiliser des fonctions de hachages afin de rendre incompréhensible le mot de passe même s'il est découvert par un attaquant. Il existe 2 types de fonctions de hachages à savoir : les fonctions de hachage sans clé, dont la spécification requiert un seul paramètre d'entrée (un message); et les fonctions de hachage à clé, dont la spécification requiert deux entrées distinctes, un message et une clé secrète.

### B. Traiter la catégorie par rapport à elle-même (CVE et CWE associées)

Cette vulnérabilité présente plusieurs échecs d'authentification dues à deux causes :

1. L'utilisateur n'est pas autorisé à lire le modèle de connexion par mot de passe à usage unique.
2. L'ordinateur de l'utilisateur ne peut pas accéder au contrôleur de domaine en raison de problèmes réseau.

Quelques CWEs et CVEs associées à cette vulnérabilité :

- **CWE-297 : Validation incorrecte du certificat avec incompatibilité d'hôte**

Le logiciel communique avec un hôte qui fournit un certificat, mais le logiciel ne garantit pas correctement que le certificat est réellement associé à cet hôte.

Même si un certificat est bien formé, signé et suit la chaîne de confiance, il peut simplement s'agir d'un certificat valide pour un site différent de celui avec lequel le logiciel interagit. Si les

données spécifiques à l'hôte du certificat ne sont pas correctement vérifiées, telles que le nom commun (CN) dans l'objet ou l'extension SAN (Subject Alternative Name) d'un certificat X.509, il peut être possible qu'une attaque de redirection ou d'usurpation d'identité permette à un hôte malveillant disposant d'un certificat valide de fournir des données, usurpant ainsi l'identité d'un hôte approuvé. Afin de garantir l'intégrité des données, le certificat doit être valide et il doit se rapporter au site auquel vous accédez.

Même si le logiciel tente de vérifier le nom d'hôte, il est toujours possible de vérifier incorrectement le nom d'hôte. Par exemple, les attaquants pourraient créer un certificat dont le nom commence par un nom approuvé suivi d'un octet NUL, ce qui pourrait entraîner certaines comparaisons basées sur des chaînes pour n'examiner que la partie contenant le nom approuvé.

Cette faiblesse peut se produire même lorsque le logiciel utilise l'épinglage de certificat, si le logiciel ne vérifie pas le nom d'hôte au moment où un certificat est épinglé.

| | |
|---|---|
| CVE-2012-5804 | Le module E-commerce ne vérifie pas le nom d'hôte lors de la connexion au site de paiement. |
| CVE-2003-0355 | Le navigateur Web ne valide pas le nom commun, ce qui permet l'usurpation d'identité des sites https. |

- **CWE-287 : Authentification incorrecte**

Lorsqu'un acteur prétend avoir une identité donnée, le logiciel ne prouve pas ou ne prouve pas suffisamment que la revendication est correcte.

| | |
|---|---|
| CVE-2009-2382 | Le script admin permet de contourner l'authentification en définissant une valeur de cookie sur « LOGGEDIN ». |
| CVE-2009-3232 | Le script de mise à jour de l'authentification ne gère pas correctement lorsque l'administrateur ne sélectionne aucun module d'authentification, ce qui permet le contournement de l'authentification. |

- **CWE-384 : Fixation de session**

L'authentification d'un utilisateur ou l'établissement d'une nouvelle session utilisateur sans invalider aucun identificateur de session existant donne à un attaquant la possibilité de voler des sessions authentifiées.

Un tel scénario est couramment observé lorsque :

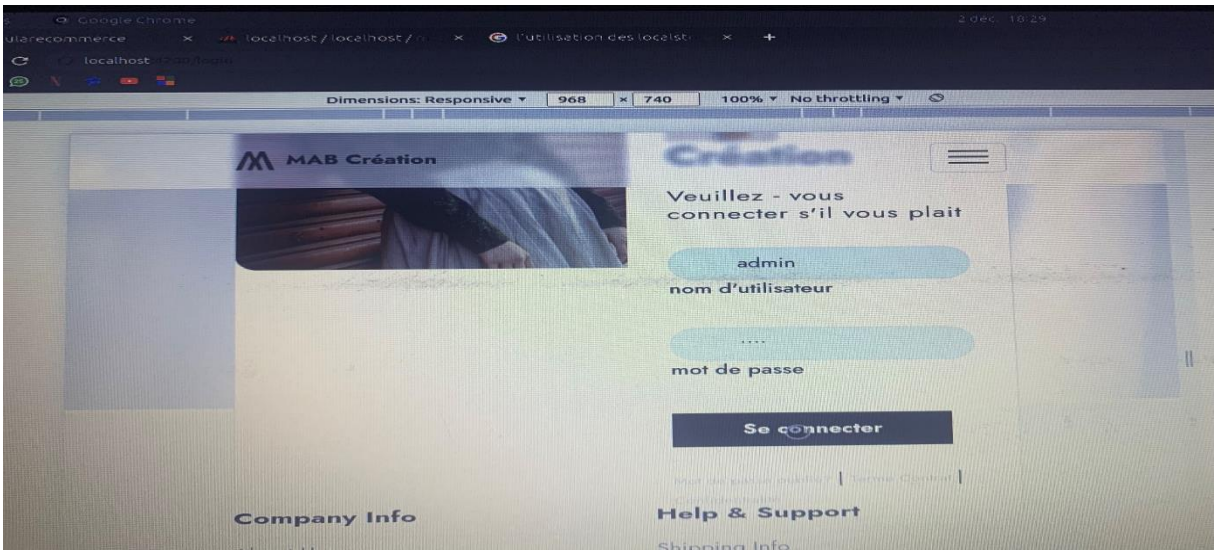
- Une application Web authentifie un utilisateur sans invalider au préalable la session existante, continuant ainsi à utiliser la session déjà associée à l'utilisateur.
- Un attaquant est capable d'imposer un identificateur de session connu à un utilisateur afin que, une fois l'utilisateur authentifié, l'attaquant ait accès à la session authentifiée.
- L'application ou le conteneur utilise des identificateurs de session prévisibles. Dans l'exploit générique des vulnérabilités de fixation de session, un attaquant crée une nouvelle session sur une application Web et enregistre l'identificateur de session associé. L'attaquant amène ensuite la victime à s'associer, et éventuellement à s'authentifier, auprès du serveur à l'aide de cet identificateur de session, ce qui lui permet d'accéder au compte de l'utilisateur via la session active.

### C. Création de notre propre scénario

**Scénario :** l'utilisation des localStorages

Le localStorage est une méthode de stockage de données sur le navigateur créé pour pallier aux deux problèmes majeurs des cookies : le faible espace de stockage ainsi que le manque de réelles API pour y accéder en JavaScript. En effet lors de l'authentification, le localStorage enregistre le login et le mot de passe entré au niveau du navigateur. un attaquant porrait les réutilisait et avoir les même accès en retrouvant les informations dans : outils de développement –>Applications – >local Storage- http://Localhost:port d'écoute

**Illustration** :



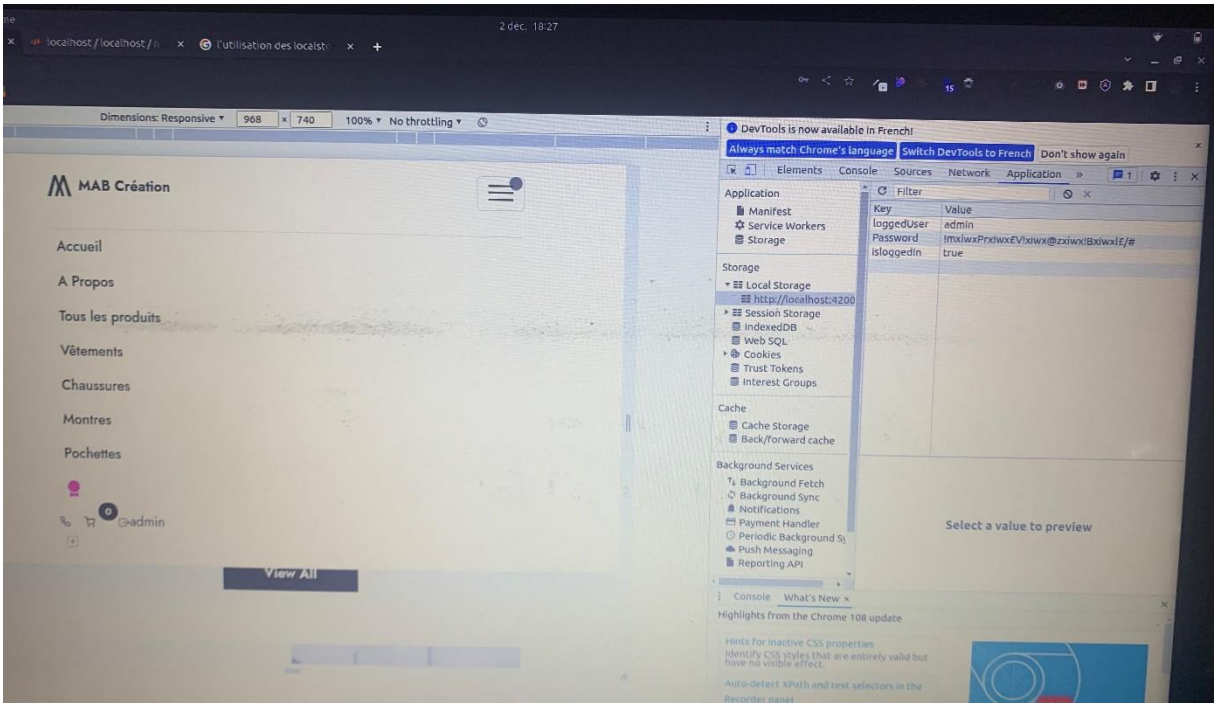

Voici la page d'authentification présentée à l'utilisateur pour qu'il puisse pouvoir avoir accès sur son interface utilisateur.

Cependant, l'utilisateur doit garder sa session lors de sa connexion sur ce site pour ne pas avoir à se reconnecter à chaque fois que le navigateur se rafraîchit. Pour ce faire, nous allons utiliser

des modes de stockages locaux appelés LocalStorage. Voici un extrait du code qui montre la faille ci-dessus,

```
signIn(user :User){
  this.loggedUser = user.username;
  this.passwordUser = user.password;
  this.isloggedIn = true;
  this.roles = user.roles;
  localStorage.setItem('loggedUser',this.loggedUser);
  localStorage.setItem('passwordUser',this.passwordUser);
  localStorage.setItem('isloggedIn',String(this.isloggedIn));
}
```

Voici un extrait du code de l'authentification dans lequel on remarque localStorage ou on garde le nom d'utilisateur et le mot de passe en local. Maintenant on revient dans le site, on se déconnecte pour visualiser les outils de développement afin de voir les identifiants stockés en local.




**Nous voici dans** outils de développement –>Applications – >local Storage ou on voit le login et mot de passe entrés. Une fois déconnecté, le mot de passe reste dans le navigateur, ce qui constitue un risque énorme.

Les mesures préventives :

On n'a pas besoins de sauvegarder en même temps le mot de passe. Juste le username suffit pour garder un localStorage.

Ou bien au moment de la déconnexion, supprimer en même temps que le login ; le mot de passe sauvegardé en faisant :

- localStorage.removeItem('loggedUser');
- localStorage.removeItem('loggedPassword');

**D. Outils pour mettre en place les scenarios et les bonnes pratiques**

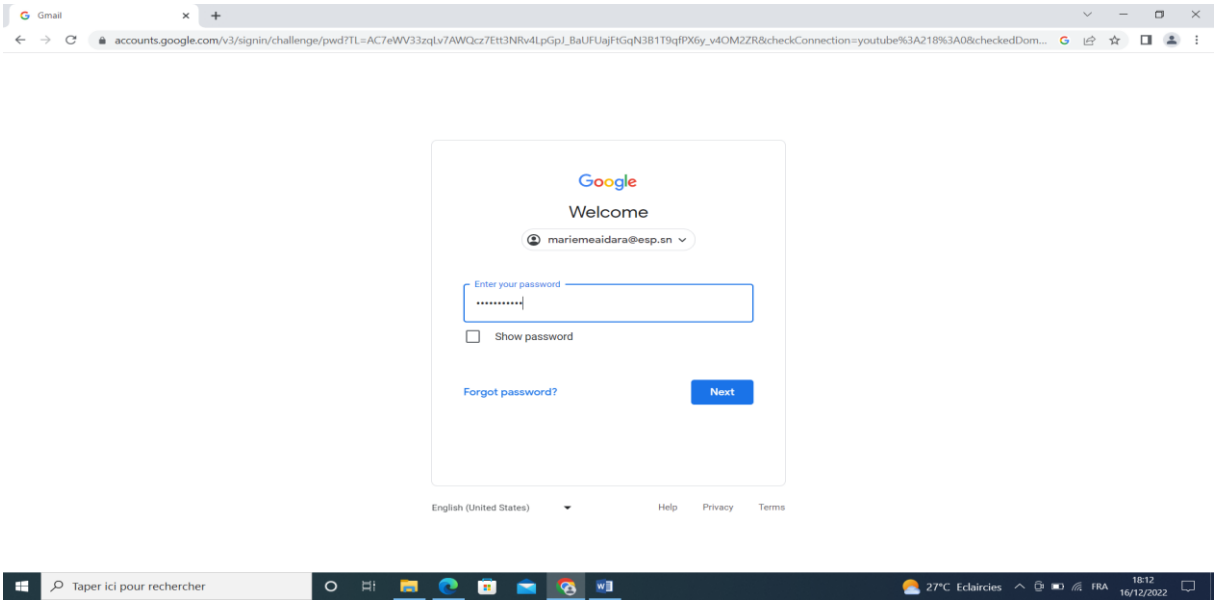
- Outils pour le propre scénario implémenté
  - **La technologie** Angular
  - **Les fonctions** LocalStorages
  - **Le langage** Type Script

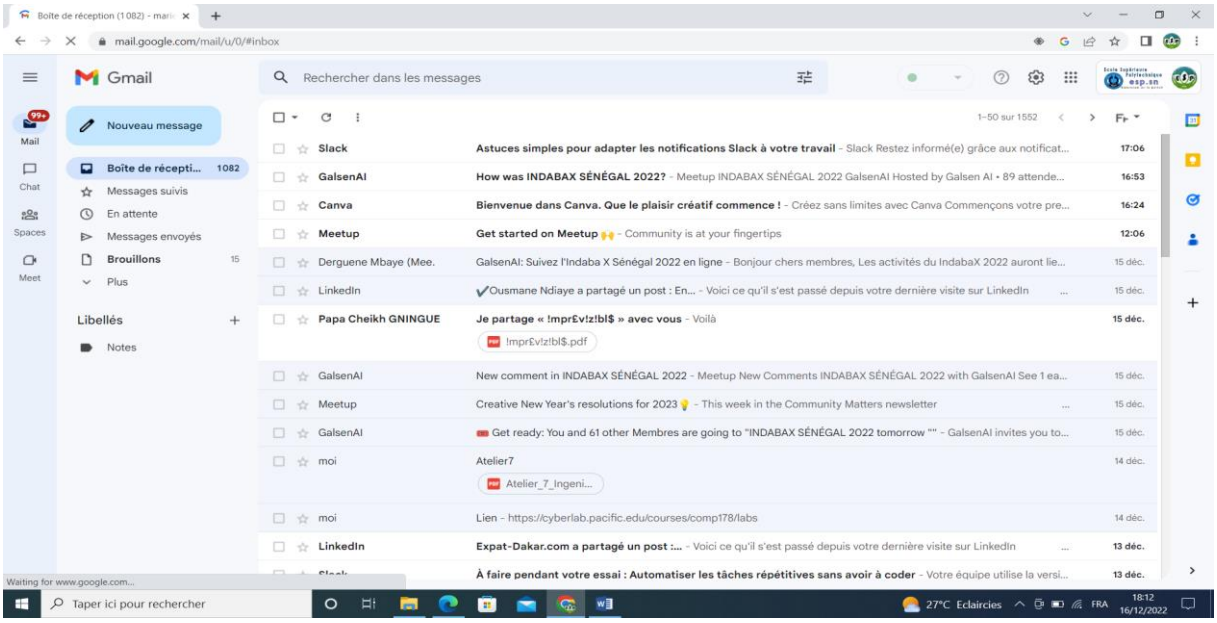
**E. Implémentation des scénarios**

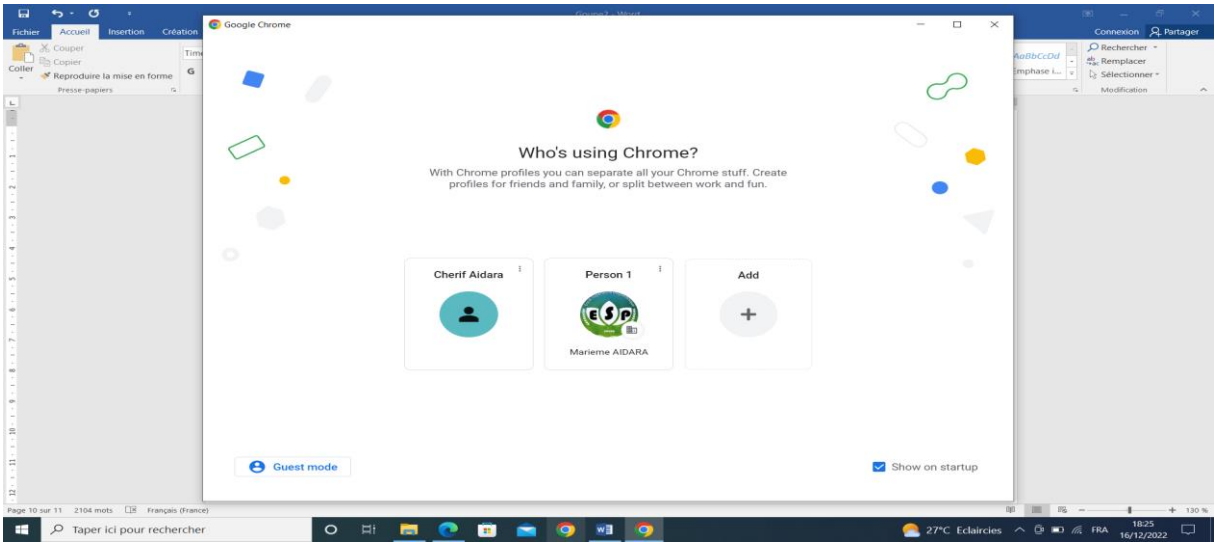
**Scénario 3** : Les timeouts de session d'application ne sont pas paramétrés correctement. Un utilisateur utilise un ordinateur public pour accéder à une application. À la place de se déconnecter correctement, l'utilisateur ferme le navigateur et quitte l'ordinateur. Un attaquant utilise ensuite le même navigateur quelque temps après et l'utilisateur est toujours authentifié.

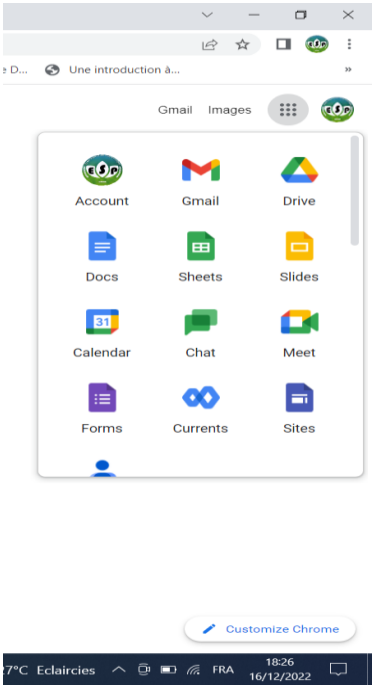
**Illustration**

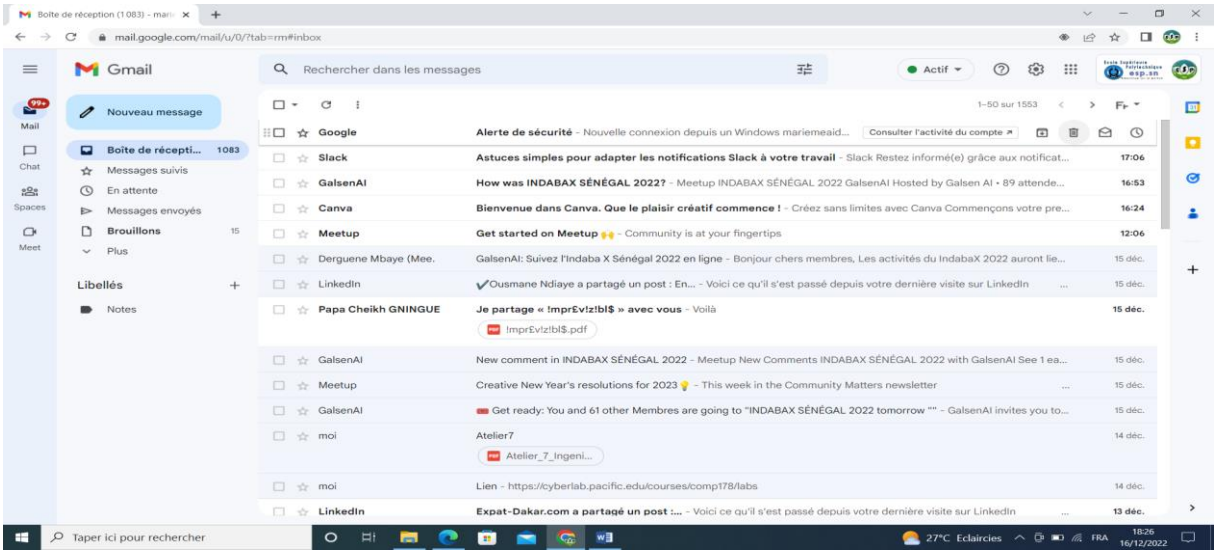
Pour illustrer ce scénario, nous allons prendre les applications telles que Facebook et Gmail. Après s'être connecté sur ces dernières via un navigateur. Lorsqu'on ferme l'application sans se déconnecter, il est tout à fait possible de recharger la page sans pour autant se reconnecter même après plusieurs jours d'inactivité. Cela entraine que toute personne utilisant ce même navigateur peut avoir accès à notre compte. De plus, si la personne connectée à enregistrer ses identifiants (username et mot de passe), il est possible de les récupérer via les paramètres du navigateur et de les utiliser pour nuire, sachant qu'une personne peut utiliser les mêmes identifiants pour plusieurs applications.


Gmail
accounts.google.com/v3/signin/challenge/pwd?TL=AC7eWV33zqLv7AWQcz7Ett3NRv4LpGpJ_BaUFUajFtGqN3B1T9qfPX6y_v4OM2ZR&checkConnection=youtube%3A218%3A0&checkedDom...
Google
Welcome
mariemeaidara@esp.sn
Enter your password
Show password
Forgot password?
Next
English (United States)
Help
Privacy
Terms
Taper ici pour rechercher
27°C Eclaircies
FRA
18:12
16/12/2022


Boîte de réception (1 082) - mari
mail.google.com/mail/u/0/#inbox
Gmail
Rechercher dans les messages
Nouveau message
Boîte de récepti... 1082
Messages suivis
En attente
Messages envoyés
Brouillons 15
Plus
Libellés
Notes
1–50 sur 1552
Slack Astuces simples pour adapter les notifications Slack à votre travail - Slack Restez informé(e) grâce aux notificat... 17:06
GalsenAI How was INDABAX SÉNÉGAL 2022? - Meetup INDABAX SÉNÉGAL 2022 GalsenAI Hosted by Galsen AI • 89 attende... 16:53
Canva Bienvenue dans Canva. Que le plaisir créatif commence ! - Créez sans limites avec Canva Commençons votre pre... 16:24
Meetup Get started on Meetup - Community is at your fingertips 12:06
Derguene Mbaye (Mee. GalsenAI: Suivez l'Indaba X Sénégal 2022 en ligne - Bonjour chers membres, Les activités du IndabaX 2022 auront lie... 15 déc.
LinkedIn Ousmane Ndiaye a partagé un post : En... - Voici ce qu'il s'est passé depuis votre dernière visite sur LinkedIn 15 déc.
Papa Cheikh GNINGUE Je partage « !mprEv!z!bl$ » avec vous - Voilà !mprEv!z!bl$.pdf 15 déc.
GalsenAI New comment in INDABAX SÉNÉGAL 2022 - Meetup New Comments INDABAX SÉNÉGAL 2022 with GalsenAI See 1 ea... 15 déc.
Meetup Creative New Year's resolutions for 2023 - This week in the Community Matters newsletter 15 déc.
GalsenAI Get ready: You and 61 other Membres are going to "INDABAX SÉNÉGAL 2022 tomorrow "" - GalsenAI invites you to... 15 déc.
moi Atelier7 Atelier_7_Ingeni... 14 déc.
moi Lien - https://cyberlab.pacific.edu/courses/comp178/labs 14 déc.
LinkedIn Expat-Dakar.com a partagé un post :... - Voici ce qu'il s'est passé depuis votre dernière visite sur LinkedIn 13 déc.
À faire pendant votre essai : Automatiser les tâches répétitives sans avoir à coder - Votre équipe utilise la versi... 13 déc.
Waiting for www.google.com...
Taper ici pour rechercher
27°C Eclaircies
FRA
18:12
16/12/2022


Google Chrome
Who's using Chrome?
With Chrome profiles you can separate all your Chrome stuff. Create profiles for friends and family, or split between work and fun.
Cherif Aidara
Person 1
Marieme AIDARA
Add
Guest mode
Show on startup
Taper ici pour rechercher
27°C Eclaircies
FRA
18:25
16/12/2022


Une introduction à...
Gmail
Images
Account
Gmail
Drive
Docs
Sheets
Slides
Calendar
Chat
Meet
Forms
Currents
Sites
Customize Chrome
27°C Eclaircies
FRA
18:26
16/12/2022


mail.google.com/mail/u/0/?tab=rm#inbox
Gmail
Rechercher dans les messages
Nouveau message
Boîte de réception 1083
Messages suivis
En attente
Messages envoyés
Brouillons 15
Plus
Libellés
Notes
Google
Alerte de sécurité - Nouvelle connexion depuis un Windows mariemeaid...
Slack
Astuces simples pour adapter les notifications Slack à votre travail - Slack Restez informé(e) grâce aux notificat... 17:06
GalsenAI
How was INDABAX SÉNÉGAL 2022? - Meetup INDABAX SÉNÉGAL 2022 GalsenAI Hosted by Galsen AI • 89 attende... 16:53
Canva
Bienvenue dans Canva. Que le plaisir créatif commence ! - Créez sans limites avec Canva Commençons votre pre... 16:24
Meetup
Get started on Meetup - Community is at your fingertips 12:06
Derguene Mbaye (Mee.
GalsenAI: Suivez l'Indaba X Sénégal 2022 en ligne - Bonjour chers membres, Les activités du IndabaX 2022 auront lie... 15 déc.
LinkedIn
Ousmane Ndiaye a partagé un post : En... - Voici ce qu'il s'est passé depuis votre dernière visite sur LinkedIn 15 déc.
Papa Cheikh GNINGUE
Je partage « !mprÉv!z!bl$ » avec vous - Voilà
!mprÉv!z!bl$.pdf 15 déc.
GalsenAI
New comment in INDABAX SÉNÉGAL 2022 - Meetup New Comments INDABAX SÉNÉGAL 2022 with GalsenAI See 1 ea... 15 déc.
Meetup
Creative New Year's resolutions for 2023 - This week in the Community Matters newsletter 15 déc.
GalsenAI
Get ready: You and 61 other Membres are going to "INDABAX SÉNÉGAL 2022 tomorrow "" - GalsenAI invites you to... 15 déc.
moi
Atelier7
Atelier_7_Ingeni... 14 déc.
moi
Lien - https://cyberlab.pacific.edu/courses/comp178/labs 14 déc.
LinkedIn
Expat-Dakar.com a partagé un post :... - Voici ce qu'il s'est passé depuis votre dernière visite sur LinkedIn 13 déc.
Taper ici pour rechercher
27°C Eclaircies
FRA
18:26
16/12/2022

L’outil utilisé pour implémenter ce scénario est gmail. Nous pouvons remarquer sur les images ci-dessus qu’après s’être connecté à 18h12 et avoir quitté l’application sans être déconnecté, toute personne inconnu peut se reconnecter au compte tout simplement en choisissant le compte email hôte lors de l’ouverture de chrome puis en réouvrant gmail.

### F. Les mesures préventives

- Lorsque cela est possible, implémentez l'authentification multifacteur pour éviter les attaques automatisées, le bourrage des informations d'identification, la force brute et la réutilisation des informations d'identification volées ;
- Ne pas livrer ou déployer avec des informations d'identification par défaut, en particulier pour les utilisateurs avec privilèges ;
- Intégrer des tests de mots de passes faibles, à la création ou au changement. Comparer ce mot de passe avec la liste des 10000 mots de passe les plus faibles ;
- Respecter la longueur, la complexité et la rotation des mots de passe par rapport aux directives du National Institute of Standards and Technology (NIST) 800-63 B à la section 5.1.1 ou autres directives modernes ;
- Assurez-vous que l'inscription, la récupération des informations d'identification et les chemins d'accès aux API sont durcis contre les attaques d'énumération de compte en utilisant le même message pour tous les résultats ;
- Limitez ou retardez de plus en plus les tentatives de connexion échouées, mais veillez à ne pas créer un scénario de déni de service. Enregistrer tous les échecs et alerter les administrateurs lors du bourrage des informations d'identification, de brute force ou d'autres attaques détectées
- Utilisez un gestionnaire de session intégré et sécurisé côté serveur qui génère un nouvel identifiant de session aléatoire avec une entropie élevée après la connexion. Les identifiants de session ne doivent pas se trouver dans l'URL, ils doivent être stockés de manière sécurisée et être invalidés après la déconnexion, une inactivité et une certaine durée.