

---

VEILLE TECHNOLOGIQUE

---

# LA SÉCURITÉ DES DONNÉES WEB

---

Matias Brice BTS Services informatiques aux organisations

---



# Sommaire :

• Qu'est-ce que la sécurité des données ?	3
• Pourquoi la sécurité des données est-elle importante ?	3
• Quelles sont les 6 méthodes de piratage informatique les plus courantes ?	4,5
• Quelles sont les institutions qui lutte pour la protection des données sur le web ?	6
• Exemple d'une vulnérabilité des protections des données sur un site web	7,8,9
• Mais comment sécuriser son site contre ces menaces ?	10,11
• Recueillir obligatoirement le consentement aux cookies des internautes	12
• En conclusion	13

# Qu'est-ce que la sécurité des données ?

La sécurité des données concerne aussi bien les pratiques que la technologie permettant de protéger les données précieuses et sensibles des entreprises et des clients, telles que les informations personnelles ou financières.

Pensez aux données précieuses que votre entreprise recueille, stocke et gère. Les informations telles que les données financières ou de paiement, la propriété intellectuelle et les informations personnelles sensibles concernant vos employés et vos clients sont une véritable mine d'or pour les pirates informatiques. La sécurité des données, à savoir les processus et les technologies que vous devez utiliser pour protéger ces données, est un élément capital pour protéger la réputation et la santé financière de votre entreprise.

## Pourquoi la sécurité des données est-elle importante ?

Les données que votre entreprise crée, collecte, stocke et échange constituent un actif précieux. En les protégeant contre la corruption et l'accès non autorisé par des personnes internes ou externes, vous protégez votre entreprise contre les pertes financières, les risques d'atteinte à sa réputation, mais aussi les risques de perte de confiance des consommateurs et de dégradation de la marque. Par ailleurs, la réglementation des pouvoirs publics et du secteur en matière de sécurité des données exige que votre entreprise assure la conformité à ces règles, quel que soit le lieu où vous exercez vos activités.



# Quelles sont les 6 méthodes de piratage informatique les plus courantes ?

## **Le phishing ou hameçonnage :**

Cette méthode de piratage consiste à leurrer l'internaute dans le but de l'inciter à communiquer ses données personnelles et/ou bancaires en se faisant passer pour un tiers de confiance (banque, assurance...).

### **Comment se protéger ?**

- Ne jamais communiquer votre mot de passe
  - Vérifier que votre antivirus est à jour.
  - Pour un achat sur internet, vérifier que le site web est bien sécurisé. L'adresse doit commencer par : « https ».
  - Mail douteux ? N'ouvrez pas la pièce jointe ou le lien qu'il contient.
- 

## **Le rançongiciel :**

De plus en plus répandu, le rançongiciel est un programme malveillant qui crypte les données puis envoie une demande de rançon au propriétaire en échange de la clé permettant de les déchiffrer.

### **Comment se protéger ?**

- Sauvegarder régulièrement vos données.
  - Extensions douteuses d'un fichier ? Si vous avez un doute ne les ouvrez pas.
  - N'ouvrir pas les mails dont la forme ou la provenance vous paraît douteuse.
- 

## **Les logiciels malveillants :**

Caché dans les logiciels de téléchargement ou dans les clés USB, le logiciel malveillant a un seul but : nuire à un système informatique.

### **Comment se protéger ?**

- Installer uniquement les logiciels provenant de sources fiables.
  - Ne connecter jamais une clé USB trouvée par hasard ou reçue dans la boîte aux lettres, elle peut être piégée.
- 

## **La clé USB piégée**

Cette méthode de piratage peut faire des dégâts en quelques secondes. En effet, une clé USB trouvée peut contenir divers éléments pouvant voler ou chiffrer vos données contre rançon.

### **Comment se protéger ?**

C'est très simple, ne connectez jamais une clé USB trouvée !

## Les faux sites internet :

Sites administratifs, boutiques en ligne... les faux sites internet ne manquent pas et sont là pour récupérer les données de paiement ou les mots de passe. Attention, les faux sites internet sont des copies parfaites des sites originaux.

**Comment se protéger ?** Pour éviter de se faire avoir par de faux sites internet, ne saisissez jamais vos données de paiement ou mots de passe sur les sites ne comportant pas un nom commençant par « https ».

## Le vol de mot de passe

Cette méthode piratage consiste à récupérer les mots de passe des victimes. Pour ce faire, les pirates utilisent des logiciels destinés à essayer le maximum de combinaisons possibles dans le but de trouver votre mot de passe. Pour cela ils utilisent les données relevées sur les réseaux sociaux.

**Comment se protéger ?** Lorsque vous créez votre mot de passe, respectez quelques règles :

- Créer un mot de passe complexe : lettres, majuscules, caractères spéciaux et chiffres.
- Eviter d'utiliser les dates de naissance, numéros de téléphone... ou d'autres éléments personnels.
- Varier les mots de passes sur les différents sites.

En plus de ces mesures de prévention spécifiques à chaque méthode de piratage, il est conseillé aux entreprises de faire **appel à un expert en sécurité informatique** qui garantira la **sécurité du Système d'Information de l'entreprise**.

Référencé sur la plateforme [cybermailveillance.gouv.fr](https://cybermailveillance.gouv.fr), Axess accompagne les entreprises et administration dans la mise en place de mesures visant à prévenir les attaques. Ils interviennent en amont et/ou à la suite des cyberattaques pour récupérer vos données.



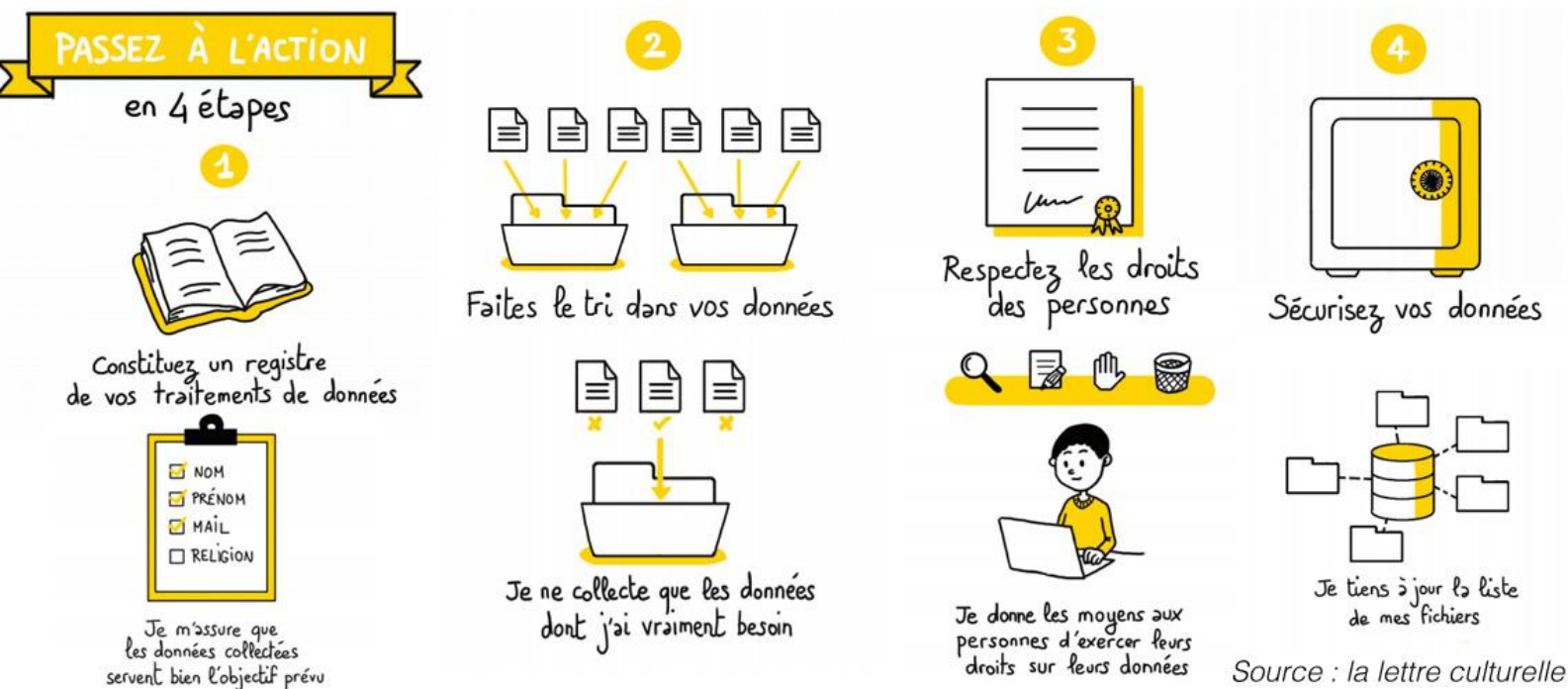
# Quelles sont les institutions qui luttent pour la protection des données sur le web ?

Au niveau national nous avons la CNIL :

La Commission Nationale de l'Informatique et des Libertés (**CNIL**) a été créée par la loi Informatique et Libertés du 6 janvier 1978. Elle est chargée de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papiers, aussi bien publics que privés.

Au niveau européen nous avons la RGPD :

La RGPD, ou Règlement Général sur la Protection des Données, ou General Data Protection Régulation est un règlement européen permettant d'encadrer davantage les responsables de traitement ainsi que les sous-traitants des données au sein de l'Union Européenne sur l'utilisation des données des personnes physiques.



# Exemple d'une vulnérabilité des protections des données sur un site web

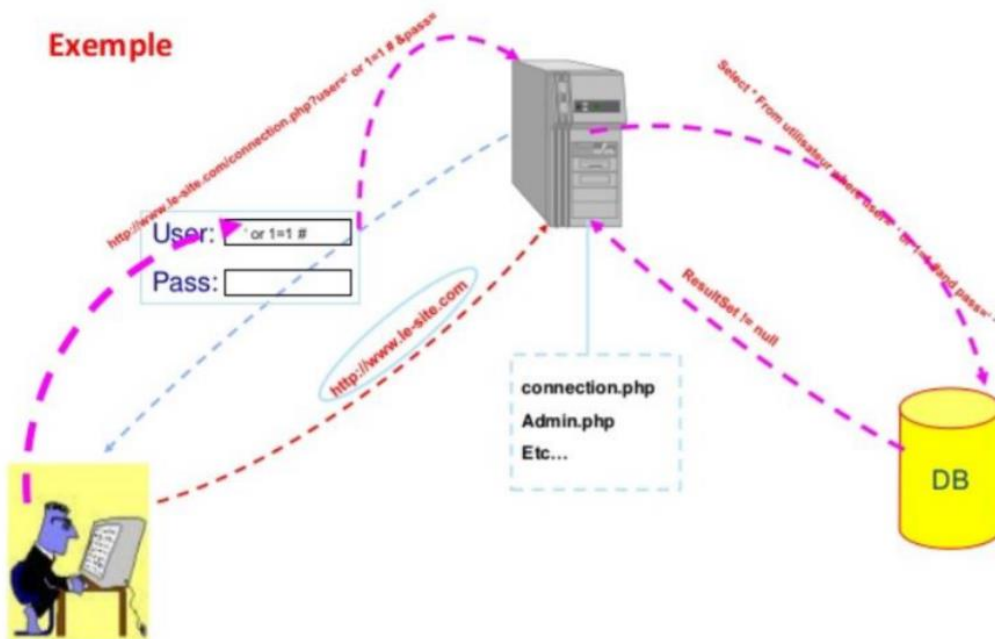
**L'injection SQL** : C'est un type d'exploitation d'une faille de sécurité d'une application interagissant avec une base de données. L'attaquant détourne les requêtes en y injectant une chaîne non prévue par le développeur et pouvant compromettre la sécurité du système.

```
1 <?php
2
3 // On récupère les variables envoyées par le formulaire
4 $login = $_POST['login'];
5 $password = $_POST['password'];
6
7 // Connexion à la BDD en PDO
8 try { $bdd = new PDO('mysql:host=localhost;dbname=bdd','root',''); }
9 catch (Exception $e) { die('Erreur : ' . $e->getMessage()) or die(print_r($bdd->errorInfo())); }
10
11 // Requête SQL
12 $req = $bdd->query("SELECT * FROM utilisateurs WHERE login='$login' AND
13 password='$password'");
14 ?>
```

La requête va aller chercher dans la table "utilisateurs" une entrée où le pseudo est égal à \$pseudo et où le mot de passe est égal à \$password. La faiblesse de ce code se trouve dans le fait que l'on peut envoyer n'importe quoi par le biais du formulaire, y compris des morceaux de code. Par exemple, imaginez qu'un utilisateur décide de mettre en login "jean' #" et laisser le password vide (le symbole # permet de faire un commentaire en PHP). Notre requête deviendrait donc :

```
1 <?php
2
3 $req = $bdd->query("SELECT * FROM utilisateurs WHERE login='jean' # AND
4 password=''");
5
6 // Qui sera interprété de la façon suivante
7 $req = $bdd->query("SELECT * FROM utilisateurs WHERE login='jean'");
8
9 ?>
```

Tout ce qui suit ce symbole est donc considéré par PHP comme un commentaire et n'est pas pris en compte dans la requête SQL. Pour faire simple, grâce à cette injection l'utilisateur va pouvoir se connecter à n'importe quel compte sans connaître son mot de passe.



**Violation de gestion d'authentification et de session :** La portée de ces failles est importante. En effet, lorsqu'il est possible de contourner les mécanismes d'authentification ou la gestion de sessions d'un site, il devient possible d'avoir accès à des zones sensibles, au compte d'un autre utilisateur, des informations personnels ou tout simplement au compte administrateur. La protection des données et dans ce cas la non protégé.

Il y'a aussi d'autres techniques tel que le :

**Cross site Scripting (XSS) :** Il s'agit d'un type de faille de sécurité sur les sites web. Cette faille repère l'endroit où des sites web dynamique (forum, blog ...) récupère des données entrées par un utilisateur sans les avoir filtrés au préalable. Il existe en fait deux types de XSS :

**Le XSS réfléchi (non permanent) :** Cette faille est la plus simple des deux. Elle est appelée non permanente car elle n'est pas enregistrée dans un fichier ou dans une base de données. Elle est donc éphémère. L'exemple le plus couramment utilisé pour illustrer cette faille est la connexion à un espace membre.

• **Le XSS stocké (permanent) :** La faille permanente est la faille XSS la plus sérieuse car le script est sauvegardé dans un fichier ou une base de données. Il sera donc affiché à chaque ouverture du site. On prendra ici l'exemple d'un livre d'or dans lequel les utilisateurs peuvent poster un commentaire.

Nous allons nous pencher sur le XSS réfléchi que je vais vous présenter :



```
1 <?php
2
3     echo "Bonjour " . $_POST['pseudo'] . " !"
4
5 ?>
6
7 <html>
8     <form method="post" action="connexion.php">
9         <input type="texte" name="pseudo" />
10        <input type="submit" value="Connexion" />
11    </form>
12</html>
```

Dans la photo de code ci-dessus, la page de connexion se contente de dire bonjour suivi du pseudo de l'utilisateur. Mais si l'utilisateur a envie de s'amuser un petit peu, et décide de trouver un pseudo plus "fun". Par exemple, que se passerait-il s'il décidait d'entrer **Vincent** dans la zone de texte et de valider ? Eh bien il obtiendrait : Bonjour Vincent (Vincent en gras).

# Mais comment sécuriser son site contre ces menaces ?

**L'injection SQL :** Comme vous avez pu le remarquer, les injections SQL bien utilisées peuvent être redoutables ! Mais heureusement pour nous, il est très simple de s'en protéger (surtout avec PDO (PHP Data Objects)). Il suffit d'utiliser des requêtes préparées. Notre requête devient donc :

```
1 <?php
2
3 // On récupère les variables envoyées par le formulaire
4 $login = $_POST['login'];
5 $password = $_POST['password'];
6
7 // Connexion à la BDD en PDO
8 try { $bdd = new PDO('mysql:host=localhost;dbname=bdd','root',''); }
9 catch (Exception $e) { die('Erreur : ' . $e->getMessage()) or die(print_r($bdd->errorInfo())); }
10
11 // Requête SQL sécurisée
12 $req = $bdd->prepare("SELECT * FROM utilisateurs WHERE login= ? AND password= ?");
13 $req->execute(array($login, $password));
14
15 ?>
```

Une requête préparée ou requête paramétrable est utilisée pour exécuter la même requête plusieurs fois, avec une grande efficacité. L'exécution d'une requête préparée se déroule en deux étapes : la préparation et l'exécution. Lors de la préparation, un Template de requête est envoyé au serveur de base de données. Le serveur effectue une vérification de la syntaxe, et initialise les ressources internes du serveur pour une utilisation ultérieure. Le serveur MySQL supporte le mode anonyme, avec des marqueurs de position utilisant le caractère « ? ». Une telle séparation est souvent considérée comme la seule fonctionnalité pour se protéger des injections SQL

**Cross site Scripting (XSS) :** La solution la plus adaptée contre cette faille est d'utiliser la fonction `htmlspecialchars()`. Cette fonction permet de filtrer les symboles du type <, & ou encore ", en les remplaçant par leur équivalent en HTML. Par exemple : Le symbole & devient &amp;

Reprenons le code du début et modifions tout cela :

```
1 <?php
2
3     $pseudo = htmlspecialchars($_POST['pseudo']);
4     echo "Bonjour ".$pseudo." !"
5
6 ?>
```

Maintenant réessayons d'envoyer <strong>Vincent</strong> et on obtient du texte brut. **Bonjour <strong>Vincent</strong> !**

Alors oui, aucun script ne peut être à 100% sécurisé et s'il l'est aujourd'hui, il ne le sera pas **forcément demain**. De nouvelles failles voient le jour constamment. Cela peut provenir de vos propres scripts mais aussi d'un serveur mal configuré. Mais si c'est petites aides peuvent être appliqués à chaque sites ça réduirait grandement le risque des données fuites, même si on le sait que il existe encore des milliers et des milliers d'autres failles dans le monde.

```
<!DOCTYPE html>
<html lang="fr">
  <head>
    <meta charset="utf-8">
    <title>Formulaire</title>
    <script>

function verifFormulaire(form)
{
  if (form.prenom.value.length > 20)
  {
    alert("Le prénom ne peut pas dépasser20 caractères");

    // mise à vide du champ du prénom
    form.prenom.value = "";
    // mise du focus (curseur) sur le prenom
    form.prenom.focus();
  }
  else
  {
    // exécution du script PHP de traitement avec envoi de la donnée
    form.submit();
  }
}
</script>

</head>
<body>


<form method="post" action="affichPrenom.php">
  Quel est votre prénom ?
  <input type="text" name="prenom" />
  <br /><br />
  <input type="button" value="Affichage" onClick="verifFormulaire(form);" />

</form>
</body>
</html>
```

Dans ce cas on va venir bloquer les connexions utilisant un grand nombres de caractères dans ce cas on va limiter à 20 caractères ce qui empêchera quelques connexion avec des commandes du style : <script>alert("toto");</script>.

On ce verras alors afficher un message alerte avec le javascript : Le prénom ne peut pas dépasser 20 caractères.

# RECUEILLIR OBLIGATOIREMENT LE CONSENTEMENT AUX COOKIES DES INTERNAUTES

 **Vos données, votre choix.** ×

Sur nos sites et nos applications, nous recueillons à chacune de vos visites des données vous concernant. Ces données nous permettent de vous proposer les offres et services les plus pertinents pour vous, et de vous adresser, en direct ou via des partenaires, des communications et publicités personnalisées et de mesurer leur efficacité. Elles nous permettent également d'adapter le contenu de nos sites à vos préférences, de vous faciliter le partage de contenu sur les réseaux sociaux et de réaliser des statistiques

[En savoir plus](#)

Avant de poursuivre, vous pouvez sélectionner l'usage que nous ferons de vos données en cochant les cases ci-dessous. Vous pourrez mettre à jour votre choix à tout moment en cliquant sur le lien Politique Cookies en bas de notre site.

Merci d'avance pour votre confiance.  
**Boulangers #Sibienensemble**

Statistiques ⓘ	<input type="checkbox"/>	Réseaux sociaux ⓘ	<input type="checkbox"/>	Relation Client ⓘ	<input type="checkbox"/>
Personnalisation de contenu ⓘ	<input type="checkbox"/>	Publicité ⓘ	<input type="checkbox"/>		

Tout refuserEnregistrerTout accepter

Depuis de **mars 2021**, le consentement aux cookies est devenu plus strict. Les sites doivent proposer plusieurs alternatives concernant l'acceptation de ces cookies et ne pas se contenter du bandeau avec la mention "Accepter les cookies".

En effet, il est devenu nécessaire de donner plus de précisions et d'inscrire dans le bandeau qui est mis en évidence dès l'arrivée sur le site "Tout accepter" / "Tout refuser" / "En savoir plus". C'est ce que l'on appelle le **consentement éclairé de l'utilisateur**.

Il est également important d'informer correctement l'utilisateur sur les finalités de traitement de ses données personnelles dans le cadre des cookies, leur potentielle diffusion à des partenaires et le détail de chaque cookie ainsi que sa durée de vie..

# En conclusion :

Est-il possible de sécuriser toutes les données personnelles à 100% ?

Comme nous l'avons vu dans les pages précédentes aucune données personnels ne peut être sécurisé à 100%. Mais il existe pas mal de moyen de moyen pour lutter contre les fraudes informatiques. Dans notre exemple nous avons montré comment réduire les requêtes d'un pirate sur une base de données par exemple en bloquant les caractères spéciaux ainsi qu'en limite le nombre de caractères possible pour le choix de son pseudo. Tous ces petits morceaux de codes vont aider à lutter contre les cybercriminalités et donc essayer de sécuriser au mieux sont site. Même si on le sait que si aujourd'hui votre site est sécurisé pour la protection des données il ne le sera peut-être pas demain, car les techniques de pirate sont de plus en plus furtives et il y'aura toujours des fuites que le codeur ne connaîtra pas sur son code et c'est la que le pirate va profiter de ce système afin de récolter les données.

Après la sensibilisation du personnel reste quand même la meilleure technique afin d'éviter le phishing et le ransomware qui sont des techniques qui joue sur l'absence de vigilance d'une personne afin de s'intégrer sur un ordinateur ou lui dérober des données personnelles. En plus de ces mesures de prévention spécifiques à chaque méthode de piratage, il est conseillé aux entreprises de faire appel à un expert en sécurité informatique afin de garantir la sécurité du Système d'Information de l'entreprise.

Matias Brice