

Two overlapping parallelogram shapes, one blue and one light green, positioned diagonally on the left side of the slide.

Simulation de failles

32%

Des applications testées sont vulnérables
aux attaques par injection SQL



6,6 Millions

De mots de passe volés à LinkedIn en Juin 2012

11 Millions

De mots de passe hashés + 8,2 Millions d'adresses
e-mail volées chez Gamingon en Juillet 2012





Les failles testées

- Injection de commentaire SQL
- Condition OR 1 = 1
- Exécution de code JavaScript (XSS)
- UNION
- DROP TABLE

Présentation de l'application

Espace client

Connexion

Identifiant

Mot de passe

Se connecter

Formulaire non sécurisé

Formulaire sécurisé

Espace client

Connexion

Identifiant

Mot de passe

Se connecter

Formulaire non sécurisé

Formulaire sécurisé

Présentation de l'application

Espace personnel



Comptes & Contrats

Monsieur toto

Livret A	+ 1235 EUR
Livret B	+ 355 EUR
PEL	+ 212 EUR
Compte courant	+ 700 EUR

Injection de commentaire SQL



Injection d'un commentaire SQL

Espace client

Connexion

Identifiant

Mot de passe

Formulaire non sécurisé
Formulaire sécurisé

Espace client

Connexion

Identifiant

Mot de passe

Formulaire non sécurisé
Formulaire sécurisé

Injection d'un commentaire SQL

Espace personnel

Login ou Mot de passe incorrect



Espace personnel



Comptes & Contrats

Monsieur toto

Livret A	+ 1235 EUR
Livret B	+ 355 EUR
PEL	+ 212 EUR
Compte courant	+ 700 EUR
Livret A	+ 3188 EUR
Compte courant	+ 1000 EUR
Compte courant	+ 4444 EUR
Livret Jeune	+ 1244 EUR
Compte courant	+ 250 EUR
Livret A	+ 11200 EUR
Livret Jeune	+ 15000 EUR

Injection de condition
toujours vraie OR $1=1$



Injection de condition toujours vraie OR 1=1

Espace client

Connexion

Identifiant

Mot de passe

Formulaire non sécurisé
Formulaire sécurisé

Espace client

Connexion

Identifiant

Mot de passe

Formulaire non sécurisé
Formulaire sécurisé

Injection de condition toujours vraie OR 1=1

Espace personnel

Login ou Mot de passe incorrect



Espace personnel

Comptes & Contrats

Monsieur toto



Livret A	+ 1235 EUR
Livret B	+ 355 EUR
PEL	+ 212 EUR
Compte courant	+ 700 EUR
Livret A	+ 3188 EUR
Compte courant	+ 1000 EUR
Compte courant	+ 4444 EUR
Livret Jeune	+ 1244 EUR
Compte courant	+ 250 EUR
Livret A	+ 11200 EUR
Livret Jeune	+ 15000 EUR

Exécution de code Javascript : XSS



Exécution de code Javascript : XSS

Espace client

Connexion

Identifiant

Mot de passe

Formulaire non sécurisé
Formulaire sécurisé

Espace client

Connexion

Identifiant

Mot de passe

Formulaire non sécurisé
Formulaire sécurisé

Exécution de code Javascript : XSS



Cette page ne fonctionne pas

Chrome a détecté un code inhabituel sur cette page et a bloqué cette dernière pour protéger vos informations personnelles (mots de passe, numéros de téléphone et de cartes de paiement).

Essayez de [consulter la page d'accueil du site](#).

ERR_BLOCKED_BY_XSS_AUDITOR



Espace personnel

(XSS) Bonjour

hello world

OK



Afficher d'autres tables
avec UNION



UNION

toto' UNION SELECT * FROM accounts --

Espace client

Connexion

Identifiant	<input type="text" value="toto' UNION SELECT * FROM accounts --"/>
Mot de passe	<input type="password"/>
<input type="button" value="Se connecter"/>	

Formulaire non sécurisé

Formulaire sécurisé

Espace personnel



Comptes & Contrats

Monsieur toto

Livret A	+ 1235 EUR
Livret B	+ 355 EUR
PEL	+ 212 EUR
Compte courant	+ 700 EUR
Livret A	+ 1235 EUR
Livret B	+ 355 EUR
PEL	+ 212 EUR
Livret A	+ 3188 EUR
Compte courant	+ 700 EUR
Compte courant	+ 1000 EUR
Compte courant	+ 3000 EUR
Compte courant	+ 4444 EUR
Livret Jeune	+ 1244 EUR
Compte courant	+ 250 EUR
Livret A	+ 11200 EUR
Livret Jeune	+ 15000 EUR

Supprimer une table :
DROP TABLE



Supprimer une table : DROP TABLE

Espace client

Connexion

Identifiant

Mot de passe

Se connecter

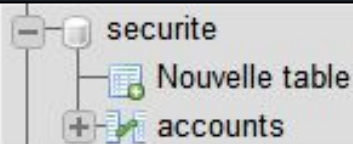
Formulaire non sécurisé

Formulaire sécurisé

Espace personnel



Array ([0] => 42S02 [1] => 1146 [2] => Table 'securite.users' doesn't exist) 1



Contrer les failles



Se protéger contre les CSRF (Cross site request forgery)

Transmission à un utilisateur connecté
d'une requête falsifiée pointant vers une
action interne au site.

```
$token = random_bytes();
```

→ Création d'une session avec un token

```
<?php  
  
session_start();  
$token = bin2hex(mcrypt_create_iv(32, MCRYPT_DEV_URANDOM));  
$_SESSION['token'] = $token;  
?>
```

```
<input type="hidden" name="token" id="token" value="<?php echo $token; ?>" />
```

```
session_start();  
// on vérifie que tous les jetons sont présents  
if(isset($_SESSION['token']) AND isset($_POST['token']) AND !empty($_SESSION['token']) AND !empty($_POST['token']))  
{  
    // On vérifie que les deux correspondent  
    if($_SESSION['token'] == $_POST['token'])  
    {  
        // Action interne au site  
    }  
}
```

Ralentir les attaques par force brute ou par dictionnaire

Bombardement du formulaire avec des mots de passe générés ou couplés à une base de données de mots de passe fréquents.

→ Mise en place de cookies limitant le nombre de tentative de connexion

```
session_start();

if(isset($_SESSION['nombre']) and $_SESSION['timestamp_limite'] < time())
{
    // Destruction des variables de session
    unset($_SESSION['nombre']);
    unset($_SESSION['timestamp_limite']);
}

// Si le cookie n'existe pas
if(!isset($_COOKIE['marqueur']))
{
    // Si le formulaire est rempli
    if(isset($_POST['connexion']) AND !empty($_POST['login']) AND !empty($_POST['mot_de_passe']))
    {
        // Initialisation du compteur
        $_SESSION['nombre'] = 0;
        $_SESSION['timestamp_limite'] = time() + 60;
    }
}
```

```
// Si le cookie marqueur n'existe pas on le crée
if(!isset($_COOKIE['marqueur']))
{
    $timestamp_marque = time() + 60; // On le marque pendant une minute
    $cookie_vie = time() + 60*60*24; // Durée de vie de 24 heures pour le décalage horaire
    setcookie("marqueur", $timestamp_marque, $cookie_vie);
}
```



Empêcher les injections SQL

- `session_start();`
- `isset();`
- `htmlspecialchars();`
- Requêtes préparées : `$req = $bdd->prepare("SELECT * FROM users WHERE users.login=? AND users.password=?");`



Bilan et best practices

- Hasher les mots de passes dans la BDD
- Utiliser des requêtes préparées
- Ne jamais faire confiance aux données reçues

Two overlapping parallelogram shapes, one blue and one light green, positioned diagonally on the left side of the slide.

Merci pour votre attention



Sources & applications

- Git & GitHub
- OpenClassroom
- Developpez.net
- Cours

