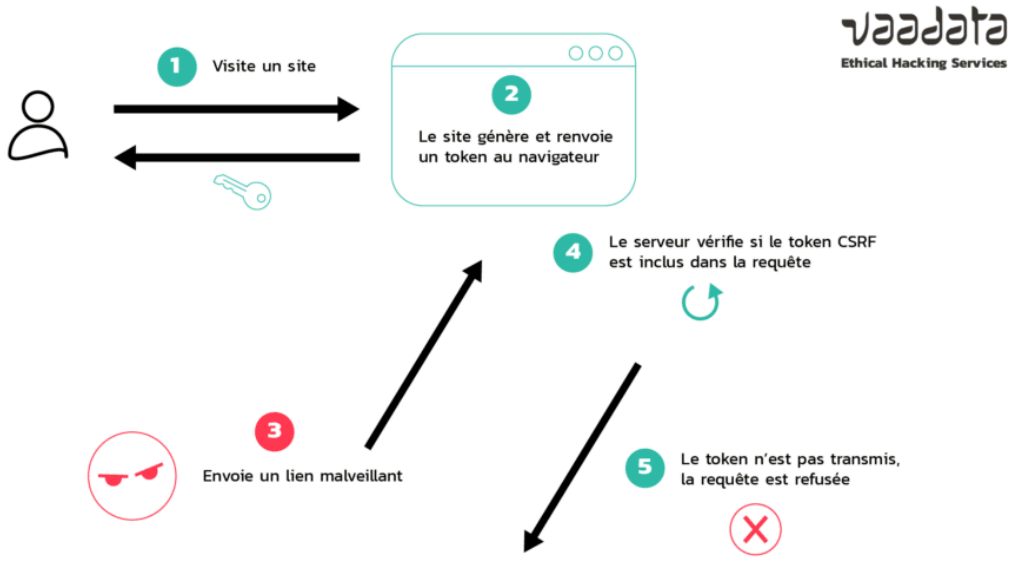
Faille CSRF

Looten AXEL

Quesque la Faille CSRF :

CSRF = Cross Site Request Forgery est une faille qui utilise l'utilisateur, un navigateur web et le serveur. Il force un utilisateur authentifié sur un site ou une application web à exécuter des actions spécifiques à son insu (par l'ouverture d'un lien). Cela peut donc permettre à l'attaquant d'accéder au compte de la victime et de forcer le changement de mots de passe ainsi que d'autre donné sensible à la connexion.

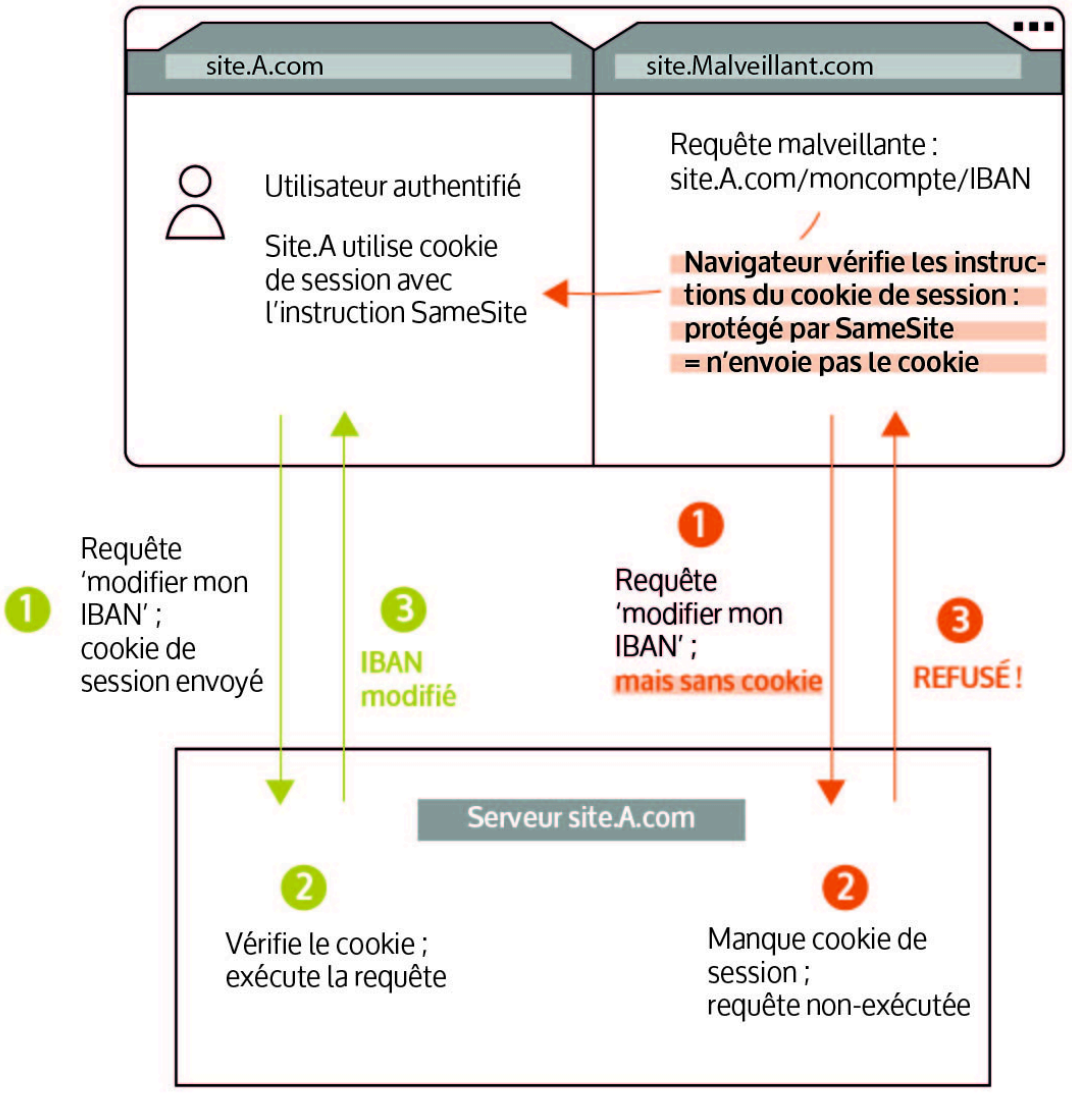


Quelle son les moyen pour s'en prémunir :

Pour se prémunir on peut implémenter des jetons CSRF pour prévenir les attaques : Les jetons CSRF sont des valeurs uniques générées aléatoirement côté serveur et envoyées au client. Ces valeurs étant uniques pour chaque requête, elles permettent de renforcer la sécurité d'une application en rendant difficile pour un attaquant de les deviner et donc d'exploiter une vulnérabilité CSRF.(voir le schéma ci dessus)

On peut également utiliser l'attribut SameSite sur les cookies pour contrer les attaques CSRF : SameSite est un attribut qu'une application peut insérer sur les cookies. En effet, lorsque cet attribut est placé sur les cookies de sessions, ceux-ci ne seront pas envoyés au serveur si la requête ne provient pas du domaine de l'application.

voir ci dessous



Le code php des token :

```
        //session_start() nous permet de sauvegarder $_SESSION['csrf_token'] jusqu'au
        prochain rechargement de la page
session_start();
        //notre fonction qui générera un token pour la page en cours
function csrf_token(){
                //on "global" $csrf_token, on pourra appeler autant de fois qu'on le souhaite
        csrf_token() et garder le même token (sans en générer un nouveau à chaque appel
        de la fonction, pour la page actuelle)
global $csrf_token;
        //nombre de caractères hexadécimaux du jeton de sécurité
$csrf_token_length = 50;
if(!isset($csrf_token)){
                //ceil() permet d'avoir une division du nombre de caractère à l'entier supérieur
        (substr() permet de couper l'entier supérieur)
        //random_bytes() génère des octets aléatoires cryptographiquement sécurisés
        //bin2hex() convertit les octets aléatoires en représentation hexadécimale
$csrf_token = substr(bin2hex(random_bytes(ceil($csrf_token_length / 2))), 0,
$csrf_token_length);
        //enregistre le token pour cette session
$_SESSION['csrf_token'] = $csrf_token;
}
return $csrf_token;
}
if(isset($_GET['id'])){
echo '<h1>Méthode GET</h1>';
//vérifie si le token existe et s'il est bon
if(!isset($_GET['csrf_token']) || ($_GET['csrf_token'] !== ($_SESSION['csrf_token'] ?? ''))){
echo '<p style="color:red">TOKEN PAS BON</p>';
}else{
echo '<p style="color:green">TOKEN BON</p>';
}
}
if(isset($_POST['id'])){
echo '<h1>Méthode POST</h1>';
        //vérifie si le token existe et s'il est bon
if(!isset($_POST['csrf_token'])
|| !isset($_SESSION['csrf_token'])
|| $_POST['csrf_token'] !== $_SESSION['csrf_token']){
echo '<p style="color:red">TOKEN PAS BON</p>';
}else{
echo '<p style="color:green">TOKEN CORRECT</p>';
}
}
```

```
?>
<p><a href="?id=1">Sans CSRF (GET)</a></p>
<p><a href="?id=1&csrf_token=<?= csrf_token() ?>">Avec CSRF (GET)</a></p>
<p><a href="?id=1&csrf_token=123">Avec faux CSRF (GET)</a></p>
<p><a href="?id=1&csrf_token=">Avec CSRF vide (GET)</a></p>
<form method="post" action="csrf_test.php">
<input type="hidden" name="id" value="1">
<input type="submit" value="Sans CSRF (POST)">
</form>
<form method="post" action="csrf_test.php">
<input type="hidden" name="id" value="1">
<input type="hidden" name="csrf_token" value="<?= csrf_token() ?>">
<input type="submit" value="Avec CSRF (POST)">
</form>
<form method="post" action="csrf_test.php">
<input type="hidden" name="id" value="1">
<input type="hidden" name="csrf_token" value="1234">
<input type="submit" value="Avec faux CSRF (POST)">
</form>
<form method="post" action="csrf_test.php">
<input type="hidden" name="id" value="1">
<input type="hidden" name="csrf_token" value="">
<input type="submit" value="Avec CSRF vide (POST)">
</form>
<?php
```