Broken authentication and session management

Plusieurs type de vol de session :
-Injection SQL
-Récupération du cookie contenant les informations de session (grâce aux failles XSS).
Lien vers un article expliquant les failles XSS
http://www.xmco.fr/article-owasp-session.html

On sait que PHP utilise le PHPSESSID afin de déterminer à quel utilisateur correspond telle ou telle session. La valeur de PHPSESSID est stockée dans un cookie chez le client et est envoyée à chaque requête effectuée par celui-ci. Côté serveur, un fichier sess_{PHPSESSID} est créé dans le répertoire /tmp. Ce dernier contient le contenu sérialisé de la session ($_SESSION).

Une façon d'empêcher le vol de session est d'enregistrer l'IP à un instant 'T' et de vérifier plus tard si celle-ci à changer, dans le cas où l'ip à changer entre le début et la fin de l'utilisation du site, cela signifiera que la session à été volée.
Exemple de protection ci-dessous :

```php
/**
    * @desc Récupére l'adresse IP du client
    * @return string
    * @access public
    */
    public function getIP()
    {
        if(getenv('HTTP_X_FORWARDED_FOR'))
        {
            return getenv('HTTP_X_FORWARDED_FOR');
        }
        elseif(getenv('HTTP_CLIENT_IP'))
        {
            return getenv('HTTP_CLIENT_IP');
        }
        else
        {
            return getenv('REMOTE_ADDR');
        }
    }
```