Evitar ataques de Session Fixation - Fijación de sesión

Cómo dar seguridad en las variables de sesión.

- [Seguridad en las sesiones]
- [Información sobre Session Fixation (Fijación de la sesión)]
- [Información sobre Session Hijacking (Robo de Sesiones)]

Como evitar Session Fixation (Fijación de la sesión)

*** Un método es utilizando cookies para la propagación del id de la sesión:**

```
ini_set('session.use_only_cookies',1);
```

*** Otra forma es regenerando los id de sesión para sesiones nuevas:** Se consigue creando una marca en las sesiones de la página web, de tal forma que cuando se hace un session_start() se comprueba si esa sesión tiene la marca. Si no tiene esa marca cambiamos su ID de sesión por uno nuevo y creamos una marca solamente conocida por nosotros. Por ejemplo:

```
<?php
@session_start();

if (!isset($_SESSION['mimarcadecontrol']))
{
   // Regenera el ID de sesión manteniendo las variables que había en la sesión.
   // El parámetro true es para que borre el fichero de la ID de sesión antigua.
   session_regenerate_id(true);
   $_SESSION['mimarcadecontrol'] = true;
}
?>
```

*** Cambiar el id de sesión cada vez que un usuario cambie su estado (registrado, autenticado, etc..).**

```
<?php
if ($usuario_logueado === true)
{
session_regenerate_id(true);
$_SESSION['logueado'] = true;
}
?>
```

--Veiga (discusión) 23:05 16 ene 2015 (CET)