1 Curso POO PHP Cross-Site Request Forguerie

1.1 Cross-Site Request Forguerie (CSRF)

Un ataque CSRF consiste en aproveitar unha sesión aberta nun sitio web para, dende outra páxina do mesmo navegador, enviar unha petición que aproveite as credenciais do usuario para levar a cabo unha acción sen o seu consentimento.

Por exemplo, mentres estás logueado nunha páxina como banco.es, poderías visitar outra páxina que conteña unha etiqueta HTML como a seguinte:

```
<img src="conta.php?accion=borra" style="display: none;">
```

O que desencadenaría unha acción cos privilexios do usuario.

A mellor forma de protexerse fronte a un ataque CSRF, é asignar a cada usuario un token único por sesión, e verificar en cada acción a posesión do mesmo. Por exemplo, cando un usuario inicia sesión asignámoslle o token aleatorio:

```
$_SESSION["token"] = md5(uniqid(mt_rand(), true));
```

As funcións empregadas na xeración do token son as seguintes:

- **uniqid**. Obtén un identificador único baseándose na hora actual. O primeiro parámetro é un prefixo, e o segundo a true indica que a lonxitude o identificador sexa de 23 caracteres.
- **mt_rand**. É un xerador de números aleatorios, para engadir maior aleatoriedade ao token obtido.
- **md5**. Obtén un hash MD5 a partir dunha cadea.

Ese token deberá engadirse nun campo oculto de cada formulario que se empregue para desencadenar accións no servidor.

```
<form action="conta.php?accion=borra" method="post">
   ...
   <input type="hidden" value="<?php echo $_SESSION['token']; ?>">
</form>
```

Posteriormente, en cada páxina antes de procesar unha acción haberá que comprobar o token.

```
<?php
session_start();
if (isset($_REQUEST["token"]) && $_REQUEST["token"] == $_SESSION["token"]) {
   // O token é correcto
   ...
}
else {
   // O token NON é correcto
   ...
}
```

--Víctor Lourido 03:09 20 jul 2013 (CEST)