Vicent Jordà

Bones pràctiques

Seguretat i gestió d'errors

Usa sempre https

Usa sessions

A diferència de les galetes les dades emmagatzemades en les sessions no s'envien mitjançant els encapçalats HTTP, romanen al servidor.

El que sí s'envia és l'identificador de sessió. Caldrà prendre mesures perquè l'identificador no puga ser accessible per tercers i així poder accedir a les dades emmagatzemades.

Segons l'OWASP:

Usa sessions

Configuració bàsica

I proposen la següent configuració bàsica:

```
session.save_path                   = /path/PHP-session/
session.name                        = myPHPSESSID
session.auto_start                  = Off
session.use_trans_sid               = 0
session.cookie_domain               = full.qualified.domain.name
#session.cookie_path                = /application/path/
session.use_strict_mode             = 1
session.use_cookies                 = 1
session.use_only_cookies            = 1
session.cookie_lifetime             = 14400 # 4 hours
session.cookie_secure               = 1
session.cookie_httponly             = 1
session.cookie_samesite             = Strict
```

Control de la vida de sessió

1. **Fes que expire la sessió després d'un curt període d'inactivitat**: ajusteu el temps d'inactivitat a 5 minuts per a aplicacions altament protegides fins a no més de 30 minuts per a aplicacions de baix risc.
2. **Habilita l'opció de tancament de sessió**: caduca i destrueix explícitament la sessió en tancar la sessió.
3. **Eviteu els inicis de sessió persistents (opció "recordeu-me")**: opcionalment podeu restringir

Identificador de sessió

1. **Utilitzeu només galetes per propagar l'ID de sessió**, ja que quan es transmeten mitjançant un paràmetre URL, les sol·licituds GET poden ser emmagatzemades a l'historial del navegador, a la memòria cau i als marcadors. Aleshores també es pot visualitzar fàcilment.
2. **Regenereu l'identificador de sessió**: regenereu (substituïu-ne per un de nou) l'identificador de sessió, almenys cada cop que canvie el nivell de privilegi de l'usuari. Generalment es pot regenerar abans de qualsevol transacció

Cookie de sessió

1. Definiu el domini de la galeta a quelcom més específic que el domini de primer nivell.
2. No emmagatzeneu res a la galeta (almenys qualsevol informació sensible com el nom d'usuari o la contrasenya) sols'ID de sessió.
3. Definiu el senyalador només http per desactivar la captura de l'identificador de sessió mitjançant XSS.
4. Quan siga possible, utilitzeu un xifrat fort (SSL) i l'atribut `cookie_secure` per permetre la