



Seguretat: No exposar els fitxers del directori .git al directori públic de la web

Publicat per [Oriol Roselló i Castells](#) [1] el 25/03/2024 - 12:21 | Última modificació: 26/03/2024 - 11:03

Els projectes que utilitzen git per desplegar fitxers als servidors de producció poden exposar el seu codi font a través del directori /.git que GIT genera quan es sincronitza amb el repositori de codi. Exposar aquests fitxers pot significar un problema de seguretat que cal evitar.

La solució immediata hauria de ser impedir que el servidor serveixi els fitxers del directori /.git del servidor, i posteriorment configurar el repositori git i la carpeta del projecte de tal manera que la carpeta /.git no estigui mai en un directori d'accés públic.

La forma preferent de bloqueig ha de ser servir un error 404, per no donar informació de si aquell directori existeix o no.

Caldria aplicar les solucions de bloqueig 1 i/o 2 el més aviat possible en el cas de servidor Apache per acabar aplicant la solució 3 més estructural. En tot cas es recomana mantenir la solució 2 i 3 sempre per seguretat simultàniament.

1. Com bloquejar l'accés als fitxers de la carpeta /.git a nivell d'aplicació

Cal afegir o editar el fitxer .htaccess al directori on apunta el domini o subdomini de la web amb la següent directiva:

```
RedirectMatch 404 /\.git
```

Això bloquejarà l'accés en aquest projecte.

2. Com bloquejar l'accés als fitxers de la carpeta /.git a nivell de servidor web

Afegir la següent directiva al fitxer apache2.conf o similar on es configura els servidors apache.

```
RedirectMatch 404 /\.git
```

Això bloquejarà l'accés al directori /.git a tots els projectes que serveixi aquest servidor web.

3. Configurar una carpeta pública del projecte i apuntar el virtual host a la carpeta pública i no a l'arrel del projecte

Una solució més estructural és que la carpeta /.git no sigui accessible directament i no estigui en cap directori públic. Per fer això caldrà configurar el virtualhost del subdomini perquè apunti a una carpeta pública on residirà el codi que ha de ser accessible:

SUBDOMINI o DOMINI => /director/carpeta-projecte/public

I configurarem el git un nivell abans fora del directori públic => /director/carpeta-projecte/.git

De la mateixa manera que es recomana que les llibreries o dependències no estiguin al directori públic per seguretat com fan Symfony i altres frameworks.

4. Migració d'un projecte sense carpeta pública

Per migrar a projecte que no disposi de carpeta pública i estigui exposant tots els fitxers del projecte caldrà crear



una carpeta /public al repositori de codi i moure tot el codi a dins d'aquesta carpeta.

Després caldrà ajustar el virtual host perquè apunti a la carpeta /public del projecte i resincronitzar el codi del git perquè faci el moviment dels fitxers de l'arrel a la carpeta pública.

Ens haurem d'assegurar que el domini o subdomini apunten a nivell de virtual host a la nostre carpeta pública, i que la carpeta /.git no estigui dins de la carpeta pública del nostre projecte.

Estructura correcta:

```
/carpeta-projecte/.git/  
/carpeta-projecte/public/ <== index.php i directori on apunta el DOMINI o SUBDOMINI  
/carpeta-projecte/vendor  
/carpeta-projecte/var  
etc.
```

Estructura insegura si no es bloqueja l'accés a la carpeta /.git:

```
/carpeta-projecte/.git/  
/carpeta-projecte/ <== index.php i directori on apunta el DOMINI o SUBDOMINI  
/carpeta-projecte/vendor  
/carpeta-projecte/var  
etc.
```

- [2]

URL d'origen: <https://comunitatdstsc.diba.cat/wiki/seguretat-no-exposar-fitxers-del-directori-git-al-directori-public-de-web>

Enllaços:

[1] <https://comunitatdstsc.diba.cat/members/admindiba>

[2] <https://comunitatdstsc.diba.cat/node/1427>