1. FTP protokolünü kullanmak neden kötü bir örnektir?

FTP protokolü , ssh / sftp protokolüne göre daha güvensiz bir dosya aktarım biçimidir. Ftp kullanıı adı ve şifresi , çalınabilir , tahmin edilebilir

Ftp ile bağlantılarda , genellikle yanlış yetkilendirmeden ötürü dosyalar hasar görebilir , dosyalar kaybolabilir .

Ftp bağlantısının , sunucunun güvenlik duvarı tarafından engellenmesi de muhtemeldir.

Ftp protokolünü destekleyen sunucunun 21. portunun sürekli açık kalması güvenlik açığı yaratabilir.

2. Genel ve özel SSH anahtarı arasındaki fark nedir?

Ssh bağlantısı public/private anahtar çifti doğrulaması ile sağlanır . Özel , private, anahtar istemcinin bilgisayarında , açık anahtar sunucu bilgisayarda saklanır. Anahtar çiftine , doğrulama esnasında kullanılmak üzere şifre de eklenebilir .

3. Live sunucuda oturum açtınız ve başka bir geliştiricinin web kök dizininde bazı dosyalar bıraktığını gördünüz (aşağıda), ne yaparsınız?

public\_html , projenin kök dizini olarak http protokolü ile doğrudan erişime açıktır , kurulum ile ilgili install dosyalarının burada bulunmaması gerekir . Csv ve sql dosyaları da doğrudan indirilebilir olduğu için burada bulunmamalıdır. Sitemap ve robots dosyaları , google optimizasyon ile ilgili dosyalardır .

Cron.php dışarıdan çalıştırılır olması sakıncalı olabilir .

“Composer update”konutu ile kullanılmayan packageların ayıklanmasını , kullanılanların güncellenmesini sağlarım .