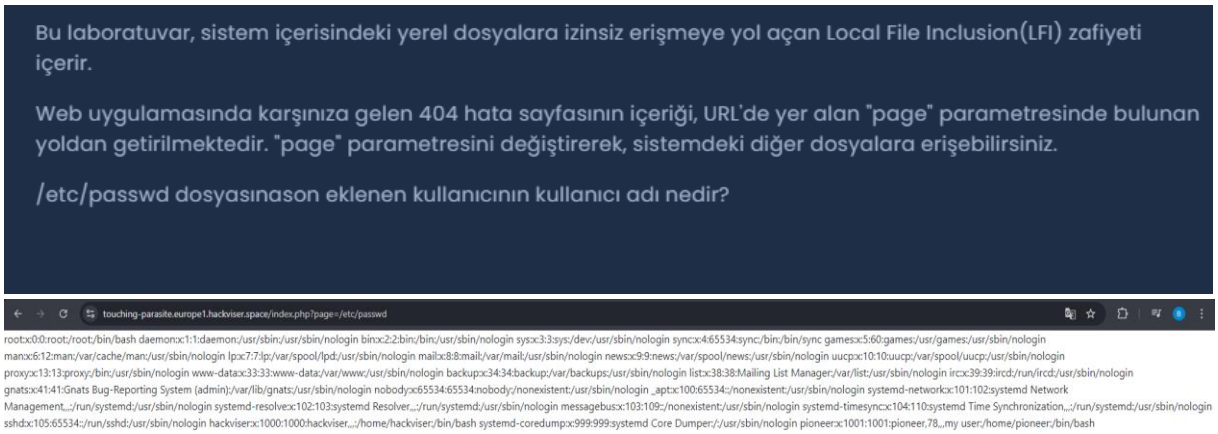
File Inclusion

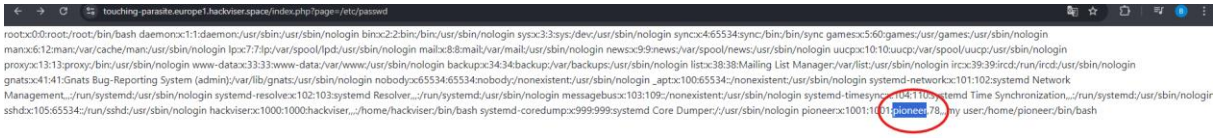
File Inclusion bu zafiyet kullanıcının girişlerini doğru bir şekilde kontrol etmeden dosya sistemindeki yerel dosyalara erişimine izin verir. 2 tür File Inclusion vardır. LFI ve RFI

LFI (Local File Inclusion) genellikle url üzerinden sömürülmeye müsaittir.

RFI (Remote File Inclusion) uzaktan dosya çalıştırmak ile olur.

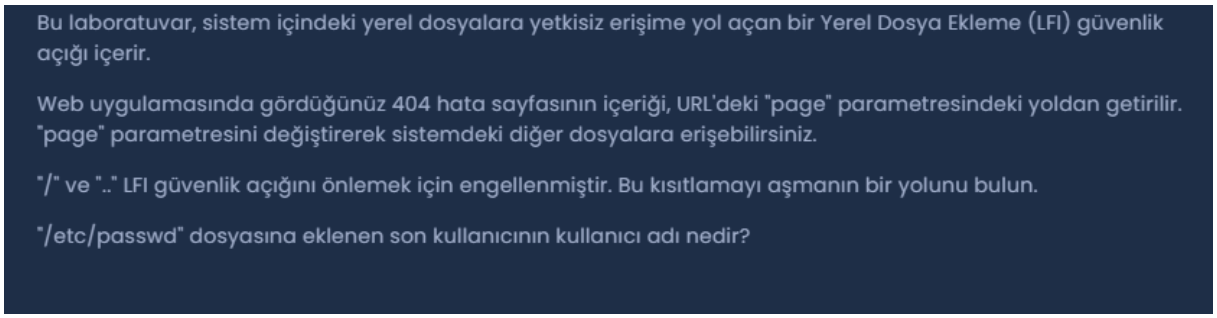


Direk url den page= değerini değiştirerek etc/passwd dizinine gitmesini istedim ve doğrduan bilgiler önüme çıkmış oldu. Benden istenen son eklenen kişinin username'ini alarak görevimi bitirdim.



İkinci level görevimde ise url e / ve .. gibi parametreleri engelleyerek çıkıyor.

Bypass yöntemim ise olması gereken parametreyi bölerek içerisine engelleyeceği (Kaldıracağı) parametreyi yerleştirmek.



pen stream: No such file or directory in **/var/www/html/index.php** on line **36**

asswd' for inclusion (include_path='.:/usr/share/php') in **/var/www/html/index.php** on line **36**

/ ve .. gibi parametrelerin yasaklanmasının nedeni bazı durumlarda o dizinin alt dizini olmayan klasörlere erişmek istediğimizde /../../../.. ile üst dizine çıkıp aramak oluyor.

Bypass yöntemim //….//….//…. Sistem her gördüğü / ve .. parametresini silse de sildikten sonra birleşen nesneler bana yine istediğim parametreyi getirecek.