LOCAL FILE INCLUSION FILTER BYPASS WRİTE-UP

Bu yazımda sizlere Hackviser platformu üzerinde bulunan Web Lab kısmı altında File Inclusion zafiyetinin Local File Inclusion Filter Bypass labının çözümünü anlatacağım.

SENARYO: Bu laboratuvar, sistem içindeki yerel dosyalara yetkisiz erişime yol açan bir Yerel Dosya Ekleme (LFI) güvenlik açığı içerir.

Web uygulamasında gördüğünüz 404 hata sayfasının içeriği, URL'deki "page" parametresindeki yoldan getirilir. "page" parametresini değiştirerek sistemdeki diğer dosyalara erişebilirsiniz.

"/" ve ".." LFI güvenlik açığını önlemek için engellenmiştir. Bu kısıtlamayı aşmanın bir yolunu bulun.

"/etc/passwd" dosyasına eklenen son kullanıcının kullanıcı adı nedir?

ÇÖZÜM: Bir önceki write-up'u çözerken ../../../../../etc/passwd yaparak cevabı bulmuştuk. Aynı şeyi tekrar deneyince

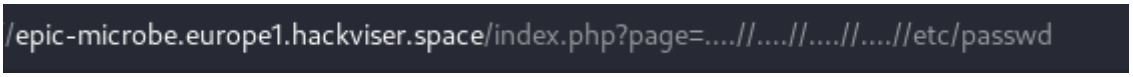
Warning: include(includes/etc/passwd): Failed to open stream: No such file or directory in **/var/www/html/index.php** on line **36**

Warning: include(): Failed opening 'includes/etc/passwd' for inclusion (include_path='.:/usr/share/php') in **/var/www/html/index.php** on line **36**

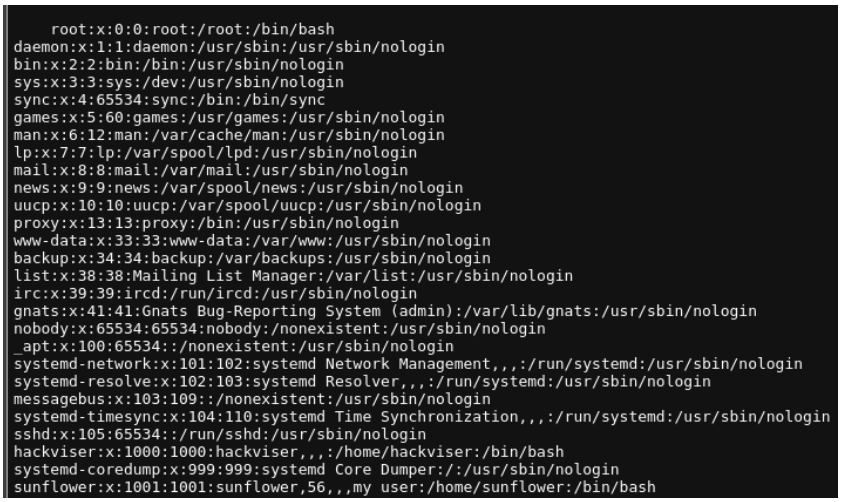
Hatasını aldık. Bu yüzden bypass yapmamız gerek.

Hacktricks sayfasında payload'lar fazlasıyla mevcuttu. Bende bunlardan birini kullandım.

….//….//….//….//etc/passwd = komutu ile bilgilere ulaştım.



Artık sayfaya eriştik.



Burada en son eklenen kullanıcının **sunflower** olduğunu bulduk ☺