Hackviser File Inclusion

Basic Local File Inclusion

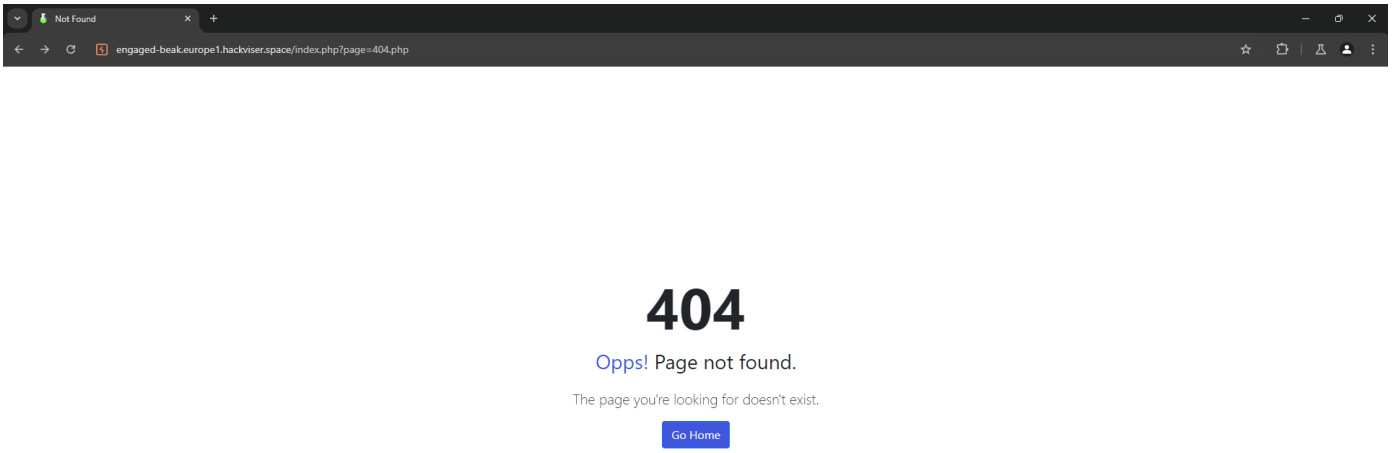
Başlangıçta bize lab hakkında bilgi vermiş

Bu laboratuvar, sistem içerisindeki yerel dosyalara izinsiz erişmeye yol açan Local File Inclusion(LFI) zafiyeti içerir.

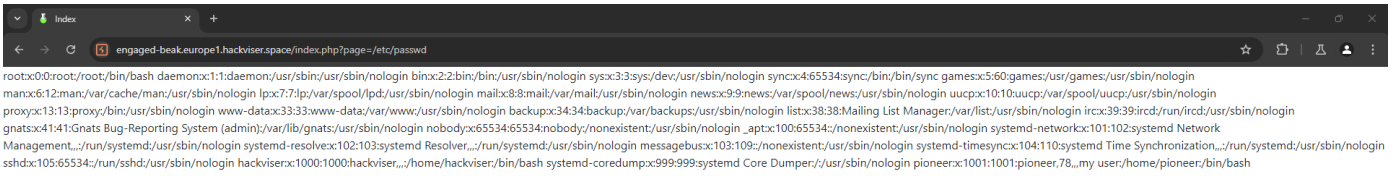
Web uygulamasında karşınıza gelen 404 hata sayfasının içeriği, URL'de yer alan "page" parametresinde bulunan yoldan getirilmektedir. "page" parametresini değiştirerek, sistemdeki diğer dosyalara erişebilirsiniz.

/etc/passwd dosyasınason eklenen kullanıcının kullanıcı adı nedir?

Öncelikle web sitesine bir bakalım



Başlangıçta bizi böyle bir sayfa karşılıyor. Urldeki **page** parametresini /etc/passwd **olarak** değiştirelim.



Ve evet **/etc/passwd** dosyasına erişerek okumayı başardık. Eklenen son kullanıcının kullanıcı adının **pioneer** olduğunu görüyoruz

Local File Inclusion Filter Bypass

Başlangıçta bize lab hakkında bilgi vermiş

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?

Öncelikle web sitesine bir bakalım

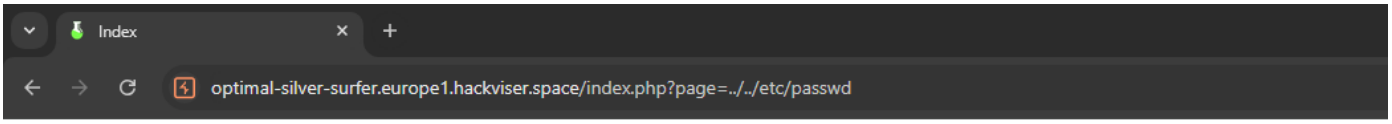
404

Opps! Page not found.

The page you're looking for doesn't exist.

Go Home

Başlangıçta bizi böyle bir sayfa karşılıyor. Parametreyi ../../etc/passwd yaptığımda ise buna izin vermiyor.



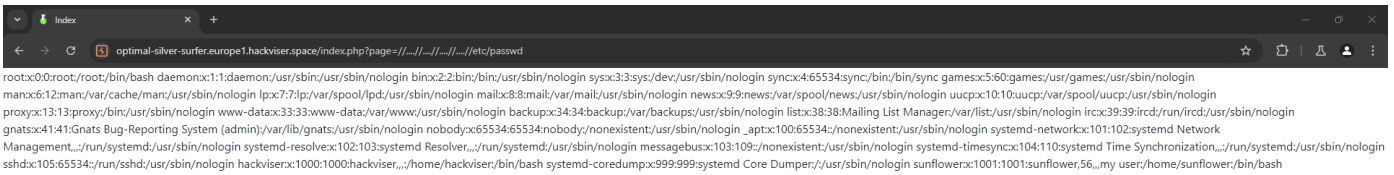
Warning: include(includes/etc/passwd): Failed to open stream: No such file or directory in **/var/www/html/index.php** on line **36**

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

Bunu bypass etmek için farklı payloadlar deneyelim.

Sayısız payload denedikten sonra sonunda buldum

https://optimal-silver-surfer.europe1.hackviser.space/index.php?page=//....//....//....//....//etc/passwd



Ve evet /etc/passwd dosyasına erişerek okumayı başardık. Eklenen son kullanıcının kullanıcı adının **sunflower** olduğunu görüyoruz.

Basic Remote File Inclusion

Başlangıçta bize lab hakkında bilgi vermiş

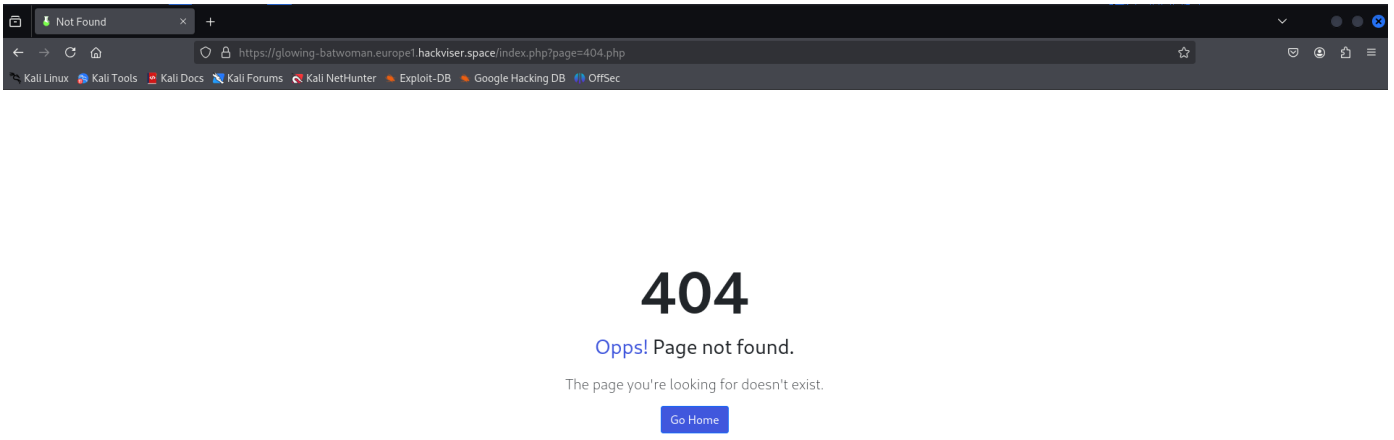
Bu laboratuvar, saldırganın uzak bir sunucuda barındırılan rastgele kodları çalıştırmasına olanak tanıyarak uzaktan kod yürütülmesine yol açan bir Uzaktan Dosya Ekleme (RFI) güvenlik açığı içerir.

Web uygulamasında gördüğünüz 404 hata sayfasının içeriği, URL'deki "page" parametresindeki yoldan getirilmektedir. "page" parametresi değiştirilerek uzaktaki bir sistemden bir dosya sayfaya dahil edilebilir.

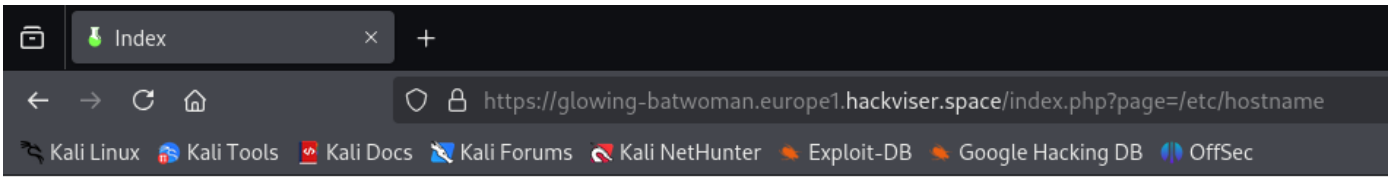
Payload'ı HackerBox üzerinde veya VPN kullanarak kendi bilgisayarınız üzerinde servis etmelisiniz.

Web sitesinin çalıştığı sunucunun ana bilgisayar adı nedir?

Öncelikle web sitesine bir bakalım



Sitemiz yine aynı şimdi hostname'i öğrenebilmek için page parametresinden sonra /etc/hostname yazarak hostname'imizi öğrenelim



imperial

Başka bir yazıda görüşmek üzere !

Linkedin

Github

İnstagram

Medium

Ayberk İlbaş