T.C.
Kayseri Üniversitesi
Siber Guvenlik Uygulama ve Arastirma Merkezi Müdürlüğü,

ARAŞTIRMA FAALİYETİ SONUÇ RAPORU

Arastirma Faaliyetinin Amacı	**:**	Web Uygulaması Sömürü Araçlarını Kullanma
Birim	**:**	Siber Güvenlik Uygulama ve Araştırma Merkezi
Arastırmadan Sorumlusu Öğretim Elemanı	**:**	Doç.Dr. Ali GEZER
Arastırma Faaliyetinde Kullanılan Araçlar	**:**	Fimap Tool
Arastırma Faaliyeti Tarih Aralığı	**:**	1.4.2023-1.5.2023
Arastırmaya Katılan Kişi Sayısı	**:**	4 (Doç.Dr. Ali GEZER, Ali Altun, Ali Akdeniz, Mehmet Gülce)
İlgili Araştırmacı Adı ve İletişim Bilgisi	**:**	aliakdeniz1881@gmail.com

Genel Bilgilendirme ve Değerlendirme

FIMAP

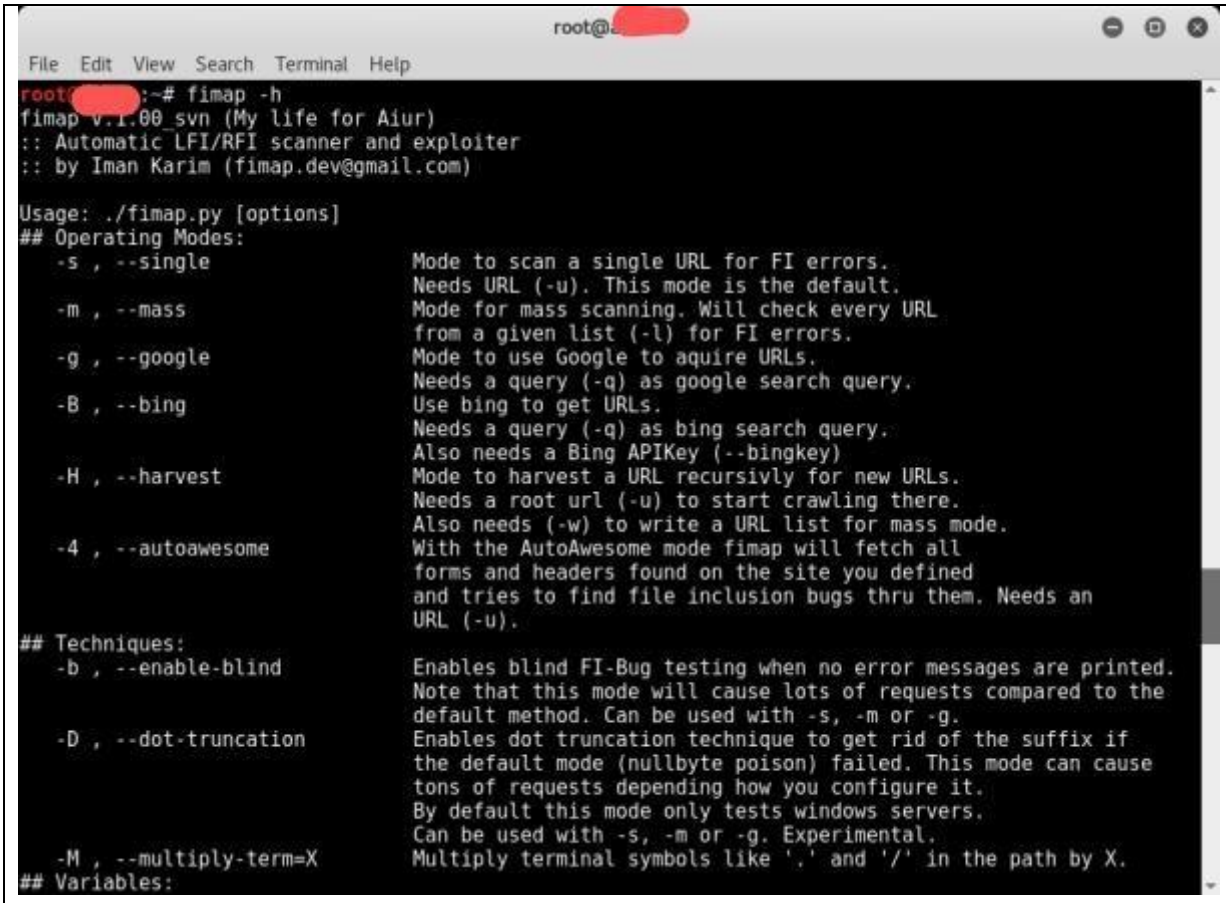
Konumuzda LFI/RFI açıklarının exploit edilmesinde oldukça işlevsel bir araç olan FIMAP ı inceleyeceğiz. Kali Linux içerisinde hazır olarak bulunmaktadır.

Öncelikle LFI ve RFI ne demek biraz açalım ve günümüzde bu açıkların önemini inceleyelim.

LFI (Local File Include) ; Yerel dosya çağırma anlamına gelmektedir. RFI (Remote File Include) ; Yerel değil uzak sunucuda bulunan bir dosyayı çağırma anlamına gelmektedir. Yani web sitesi üzerinden sunucuda bulunan dosyaları okuyup görebilmek diyebiliriz.

Fakat araştırmalarıma göre apache nin remote file çağırma konusunda yaptığı güncellemeler ile günümüzde RFI açığının eski işlevini yitirdiğini tespit edebiliriz. Fakat LFI açığının önemi ve işlevi hala etkili bir şekilde devam etmektedir.

İlk olarak aracımızın parametrelerine göz atalım .

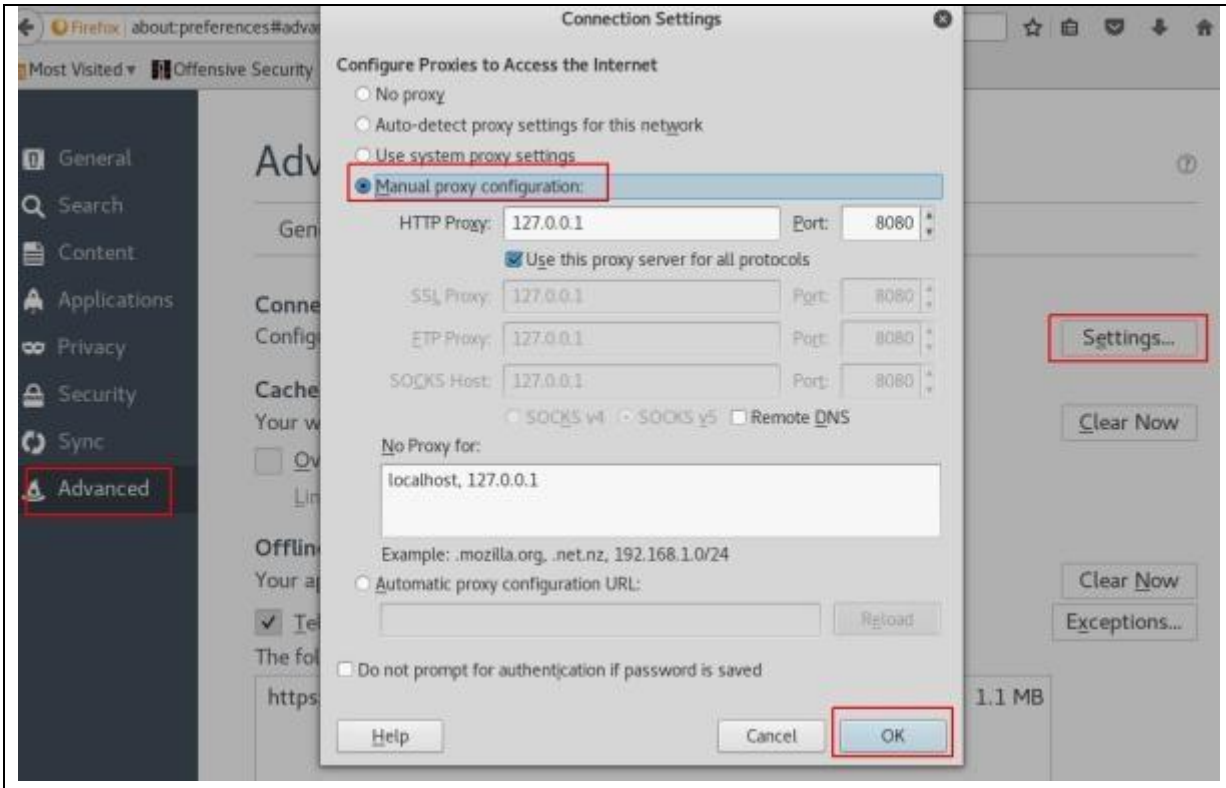


Konsolumuza fimap -h komutunu yazdığımızda karşımıza gelecektir.

Bir çok parametre mevcuttur. Detaylı olarak inceleme yapabilirsiniz. Örneğin ben birazdan taramamı yaparken standart tarama komutunun içinde ekstra olarak -b parametresini kullanacağım. Bu parametre aracın hata olmadığı bilgisini ekrana yanısttığında file injection bug taramasının aktif edilmesini sağlamaktadır.

Testimi local e değil dış bir sunucuya kurmuş olduğum DVWA Lab üzerinden örneklendirip taratacağım.

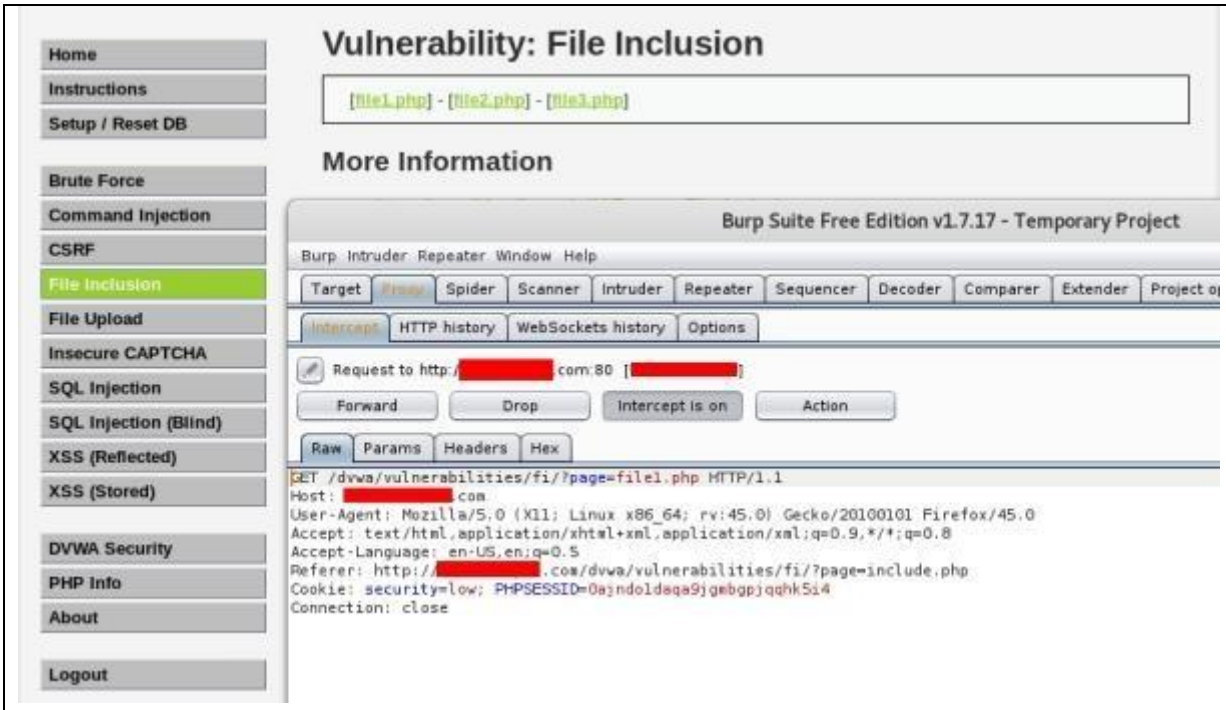
Öncelikle DVWA Lab üzerinden File Inclusion bölümüne giriyorum. Hem URL mizi hemde cookie bilgimizi edineceğiz ve testimizi gerçekleştireceğiz.



Tarayıcımın proxy ayarını gerçekleştirerek BurpSuite üzerinden cookie bilgisini edineceğim.

Firefox -> Prefences -> Advenced -> Network -> Settings yolula proxy ayarlarına erişebilirsiniz. (Tercihler -> Gelişmiş -> Ağ -> Ayarlar)

Manuel Proxy tikini işaretleyerek 127.0.0.1 Port:8080 olarak ayarlıyoruz kaydedip çıkıyoruz .
Hemen BurpSuite aracımızıda açarak proxy/intercept bölümünden intercept is on butonunu aktif hale getiriyoruz. Son olarak DVWA Lab a tekrar tarayıcımızdan giriş yaparak bilgileri alıyoruz



Referer: http://site.com/dvwa/vulnerabilities/fi/?page=include.php

Cookie: security=low; PHPSESSID=0ajndo1daqa9jgmbgpjqqhk5i4

Benim bilgilerim bunlar. Taramamıza geçelim.

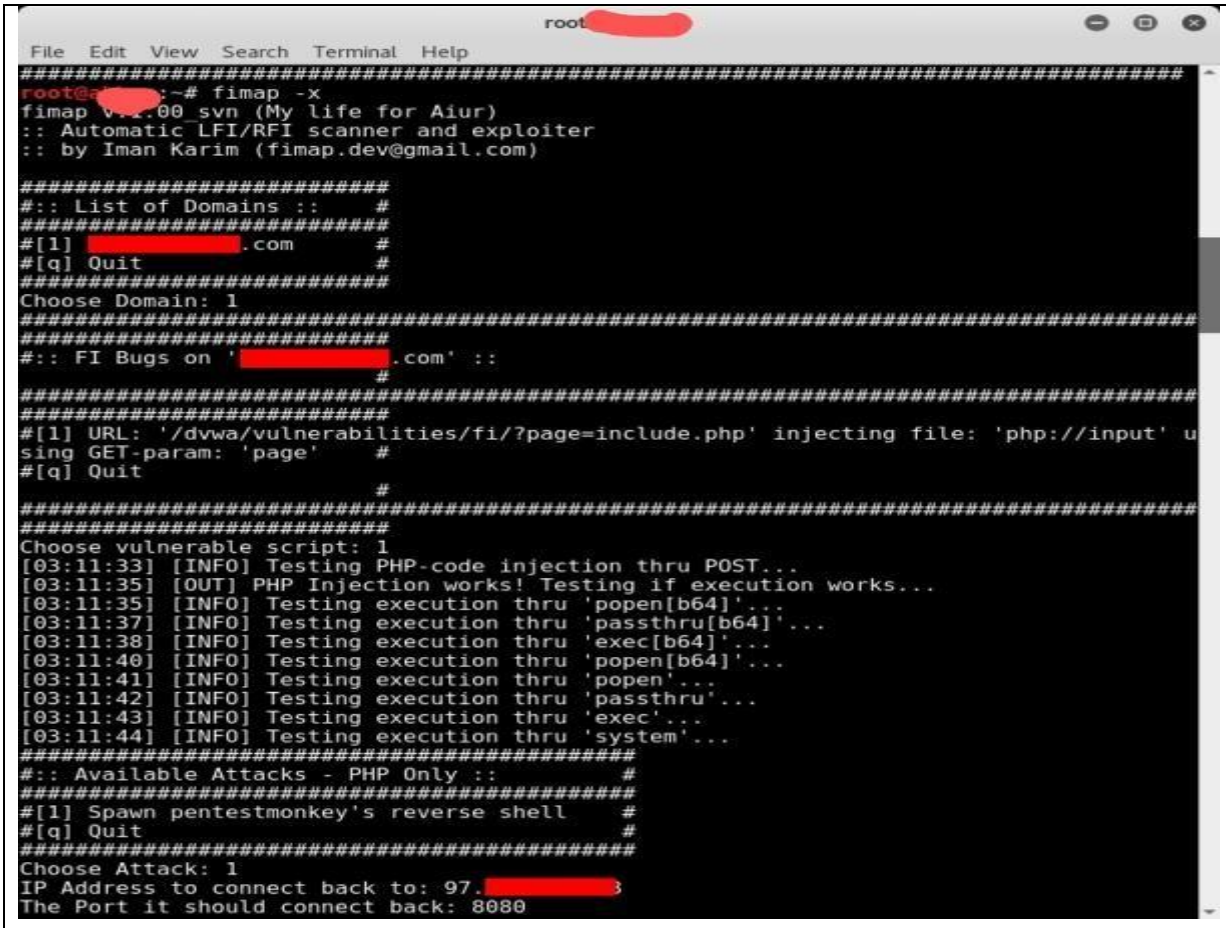
Konsola fimap -b -u URL --cookie="bilgi" komutumuzu yazarak çalıştıralım.

Taramamız başladı eğer File Includes açıklarına uygun değilse Target URL isn't affected by any file inclusion bug şeklinde hata verecektir.

Taramamızda FI için uygun olduğunu söyleyen bilgiyi görebiliyoruz. Tarama bittiğinde fimap kapanarak komut satırına sizi geri atacaktır.

Bundan sonra ise exploitleme işlemi gerçekleştireceğiz.

Konsola fimap -x yazarsak exploit için hazır (Önceden Taranmışta Olabilir) taramaları sunacaktır.



İlk önce taranmış olan domainlerin seçimi yaptırıyor. (Bende No:1)

Sonrasında FI açığının bulunduğu script seçini göreceğiz ve seçim yapacağız. (Bende No:1)

Karşımıza bağlantı yani uygun olan atak seçenekleri geldi. Bazı durumlarda fimap direkt olarak shell oturumu başlatabiliyor . Bu seçeneğin adı Spawn Fimap Shell olarak gözüküyor. Fakat bizde bu seçenek mevcut değil.

Bize sunulan seçenek Spawn pentestmonkey's reverse shell bunun içinse yine seçim yaparak işlemlerime devam ediyorum. (Bende No:1)

Son olarak ise fimap bizden bağlanılacak IP adresini ve Port u istemektedir. IP bilgisi ve dinlenmesini istediğimiz port bilgisini yaptıktan sonra

Konsola nc -lvp PORT komutunu girerek dinlemeye başlayabilir.

Sorumlu Öğretim Elemanı

Unvan: Doç.Dr.

Adı Soyadı:Ali GEZER

Görevi: Siber Güvenlik Uygulama ve Araştırma Merkezi Müdür