Arachni Kullanımı

İçindekiler

Arachni CLI (Command Line) Kullanımı

a. Default Kullanımı

(!) Uyarı

Bu default arama ile dvwa'da arama yapamazsın. Default'ta kullanılan bazı bileşenler arachni'nin hata üretmesine ve taramanın durmasına sebep oluyor. Dvwa da arama için gerekli yapılandırma uygulama başlığı altında verilecektir. Bu arada bu default aramayı localhost'taki includekarabuk_lnw/ dizinine sorunsuzca uygulayabilirsin.

```
// Tüm zafiyetleri, /plugins/defaults/ dizini altındaki tüm plugin'leri,
// tüm form - link - cookie denetlemelerini hedef üzerinde uygular.
// Rapor bulunulan dizine konur.

> ./arachni http://example.com


// Tüm zafiyetleri, /plugins/defaults/ dizini altındaki tüm plugin'leri
// tüm form - link - cookie denetlemelerini hedef üzerinde ve hedefin
// tüm subdomain'leri üzerinde uygular. Rapor bulunulan dizine konur.

> ./arachni --scope-include-subdomains http://example.com


// Tüm zafiyetleri, /plugins/defaults/ dizini altındaki tüm plugin'leri,
// tüm form - link - cookie denetlemelerini hedef üzerinde ve hedefin
// tüm subdomain'leri üzerinde uygular. Çıktılama verbose dolayısıyla
// bol olur ve tarama sonucunda rapor belirtilen dizine konur.
```

> ./arachni --scope-include-subdomains --output-verbose
--report-save-path=/path/example.com.afr http://example.com

b. Default + Ufak Ayarlama Kullanım

(!) Uyarı

> Bu default arama ile dvwa'da arama yapamazsın. Default'ta kullanılan bazı bileşenler arachni'nin hata üretmesine ve taramanın durmasına sebep oluyor. Dvwa da arama için gerekli yapılandırma uygulama başlığı altında verilecektir. Bu arada bu default aramayı localhost'taki includekarabuk_lnw/ dizinine sorunsuzca uygulayabilirsin.

// Sadece XSS (ve onun türevi zafiyet türlerini), /plugins/defaults/ dizini altındaki
// tüm plugin'leri, tüm form - link - cookie denetlemelerini hedef sistem üzerinde
// uygular.

> ./arachni --checks=xss* http://example.net

// Cross Site Request Forgery dışındaki tüm zafiyet türlerini, /plugins/defaults/
// dizini altındaki tüm plugin'leri, tüm form - link - cookie denetlemelerini hedef
// sistem üzerinde uygular.

> ./arachni --checks=*,-csrf http://example.net

// XSS ve onun türevi zafiyetler dışındaki tüm zafiyetleri, /plugins/defaults/ dizini
// altındaki tüm plugin'leri, tüm form - link - cookie denetlemelerini hedef sistem
// üzerinde uygular.

> ./arachni --checks=*,-xss* http://example.net

// Tüm aktif zafiyet türlerini (active dizini altındaki tüm zafiyet türlerini),
// /plugins/defaults/ dizini altındaki tüm plugin'leri, tüm form - link - cookie
// denetlemelerini hedef sistem üzerinde uygular.

arachni --checks=active/* http://example.net

or

arachni --checks=passive/* http://example.net

Not: active/ ve passive/ dizinleri

> > find /home/hefese/arachni-1.5.1-0.5.12 -name "active" -print

ile bulunabilir. Böylece içerisindeki zafiyet listesini görüntüleyebilirsin.

c. Custom Kullanım

i) Sık Kullanılan Arachni Parametreleri

[*] Uyarı:

Aşağıda bir arguman değerine ihtiyaç duymayan parametreler sıralanmıştır.
Argumana ihtiyaç duyan parametreler için ise örnek bir arguman değeri konulmuştur.

Audit Settings

```
--audit-headers          // Http başlıklarını denetlemeyi aktifleştirir.
--audit-forms            // Form bloklarını denetlemeyi aktifleştirir.
--audit-links            // Crawling ile bulunan linkleri denetlemeyi aktifleştirir.
--audit-cookies          // Http başlıklarındaki Cookie'yi denetlemeyi aktifleştirir.
--audit-ui-inputs        // UI'deki girdi kutularına girilen bilgilerin Javascript ile
                         // tarayıcıda işlendiği türden girdi kutularını denetlemeyi
                         // aktifleştirir.
--audit-ui-forms         // UI'deki form bloklarının tetiklenmesi sonucu bilgilerin
                         // Javascript ile tarayıcıda işlendiği türden form bloklarını
                         // denetlemeyi aktifleştirir.
--audit-parameter-names  // Denenecek payload'lar parametrelerin argumanlarına
                         // denenir. Ancak bu konfigurasyon ayarı ile payload'lar
                         // parametrelerin argumanlarına deneneceği gibi parametrelerin
                         // isimlerine de (name'lerine de) denenir.
```

Http Settings

```
--http-user-agent "Arachni/v1.5.1"          // İstemci bilgisi manuel belirtilebilir.
--http-request-concurrency 1                // Thread sayısı girilir.
--http-request-header "TEST=TUBITAK-SGE"    // Custom http header'lar girilebilir.
--http-request-header "Cookie=PHPSESSID=xyz"
--input-force                               // Input default bir value'ya sahip olsa
                                            // bile denenecek payload'lar bu input'un
                                            // üzerinde denensin direktifi verilir
                                            // (zorlaması yapılır).
```

Vuln Types

```
--checks=*,-trainer          //  - ile belirtilen zafiyet(ler) dışında tüm
                             // zafiyetleri hedef sistem üzerinde
                             // dene.
```

Ayrıca;

--checks=[eklenecekZafiyetTürleri]

Arachni'de mevcut zafiyet türlerini görmek istersen

Terminal:
>./arachni --checks-list

komutunu girebilir ve böylece sıralanan zafiyetlerden uygun gördüğünün .rb uzantılı dosya ismini (.rb'sini almadan)

--checks=vulnName1 // sadece vulnName1 taraması

ya da

--checks=*,-vulnName1,-vulnName2 // vulnName1 ve vulnName2
// dışında tüm taramalar

şeklinde kullanarak spesifik zafiyet taramaları yapabilirsin.

Plugins

--plugin=autologin:url=http://tubitak-hasanfsimsek3 // AutoLogin Plugin'i (Tarama
/DVWA-master/login.php,parameters='username=admin // Yapmadan Önce Oturum Açma
&password=password',check='Logout' // İşlemi)

>>>>> **Açıklama**
autologin plugin'inin son parametresi olan check ile oturum açıldığında görünen ama oturum açılmamışken görünmeyen bir string girilir. Böylece tool, tarama esnasında oturumun açık olduğundan emin olur. Aksi durumda tekrar login olmaya çalışır. Bu, örneğin login timeout'a düştüğünde otomatikmen yeniden login olmayı sağlar ve taramanın sağlıklı bir şekilde devam etmesini sağlar.

--scope-exclude-pattern="csrf|setup\.php|security\.php // AutoLogin ile Oturum Açma
|logout\.php" // Sonrası Oturumun Kaybına
// Neden Olabilecek ya da Oturu-
// mu bir Şekilde Bozacak
// Muhtemel Dizinleri ya da Web
// Sayfalarını Hariç Tutma

>>>>> **Açıklama**
DVWA'nın csrf dizini (şifre değiştirme senaryosuna sahip), setup.php web sayfası, security.php web sayfası ve logout.php web sayfası oturumun kaybına neden olabilecek aktiviteler içerdiğinden tarama scope'unun dışında tutulmuşlardır.

--plugin=timing_attacks // Tarama zamanını uzatsa da
// timing türü saldırıları yap.

--plugin=uncommon_headers // Yaygın olmayan http
// header'larını kullan.

--plugin=uniformity

--plugin=autothrottle // Taramanın stabilitesini temin
// etmek amacıyla gerekirse
// tarama hızını düşür ve hızı
// optimum hale getir.

--plugin=discovery

Ayrıca;

--plugin=[eklenecekBaşkaPluginler]

Başka seçilebilecek plugin'ler görmek ve ne işe yaradıklarını okuyarak ona göre seçmek istersek

Terminal:
>./arachni --plugins-list

komutunu kullanabilir ve böylece ekranda sıralanan plugin'lerden uygun gördüğünün .rb uzantılı dosya ismini (.rb'sini almadan)

--plugin=pluginIsmi

şeklinde kullanarak plugin'leri taramana dahil edebilirsin. Eğer plugin'in açıklamasını okurken plugin'in parametrelerinin olduğunu görürsen yukarıda gösterilmiş AutoLogin plugin'inin parametre ekleme syntax'ına bakarak seçtiğin plugin'inin parametrelerini uygun şekilde kullanabilirsin.

Reporting Settings
--report-save-path /home/hefese/Desktop/

Restore Settings
--snapshot-save-path /home/hefese/

Output Settings During Scanning
--output-verbose

ii) Custom Kullanım Örnek

Terminal:

> **./arachni** --audit-headers --audit-forms --audit-links --audit-cookies --audit-ui-inputs --audit-ui-forms --audit-parameter-names --audit-with-extra-parameter --http-user-agent "Arachni/v1.5.1" --http-request-concurrency 1 --http-request-header "TEST=TUBITAK-SGE" --input-force --checks=*,-trainer --plugin=pluginName:param1=http://example.com/login.asp='username=abc&password=sifre',check='Logout' --scope-exclude-pattern="logout\.php" --plugin=timing_attacks --plugin=uncommon_headers --plugin=uniformity --plugin=autothrottle --plugin=discovery --report-save-path /home/hefese/Desktop/ --snapshot-save-path /home/hefese/ --output-verbose **http://example.com**

Terminal:

> chmod a+x "/home/hefese/Desktop/example.com 2018-11-19 23_44_55+0300.afr"
> ./arachni_reporter "/home/hefese/Desktop/example.com 2018-11-19 23_44_55+0300.afr" --reporter=html:outfile=/home/hefese/Desktop/**rapor.html.zip**

> unzip /home/hefese/Desktop/rapor.html.zip
> cd rapor/
> firefox /home/hefese/Desktop/rapor.html

Not:

Rapor çıktı paketinin uzantısını zip yapman şarttır. Böylece afr uzantılı binary rapor kaynağı düzgün bir şekilde html dosyasına zip halinde çıkabilecektir. Zip içerisindeki HTML dosyasını sorunsuz görüntüleyebilmek için html dosyasını ve diğer bileşenlerini zip'in içerisinden çıkarman gerekmektedir.

Not 2:

Html dışında başka rapor formatlar da vardır. Örn; json, yaml, xml, txt, … gibi.
Tüm rapor formatlarını görmek için

> ./arachni_reporter --reporters-list

komutunu girebilirsin.

d. Uygulama

[+] Aşağıdaki default ve custom taramalar birebir denenmiştir ve başarıyla uygulanmıştır.

■ Default Tarama

Saldırgan Makina : Ubuntu 18.04 LTS Ana Makina
Hedef : Localhost'taki IncludeKarabuk_Lnw

(-) Uyarı

Default taramadaki bazı default bileşenler DVWA'da uyumsuzluk çıkardığından tarama fail olmakta. O nedenle default tarama includekarabuk_lnw/ dizinine yapılmıştır ve başarılı olunmuştur.

(-) Uyarı

Arachni tasarımı gereği localhost'taki uygulamalar taranacağı zaman hedef url olarak http://localhost ya da http://127.0.0.1 yerine http://hostname istemektedir.

(-) Uyarı

Taramayı kök url yerine kök url'deki bir dizin altında (includekarabuk_lnw/ altında) yapmak istediğinden default taramana --scope-include-pattern (only certain path) parametresini ilave etmen gerekir.

Ubuntu 18.04 LTS Terminal: // Tarama Başlar

> ./arachni --scope-include-pattern "^http://tubitak-hasanfsimsek3/includeka
rabuk_lnw/" http://tubitak-hasanfsimsek3/includekarabuk_lnw/

Çıktı:

[~] Scanned completed.
[~] Report is saved in /home/hefese/arachni-1.5.3/tubitak-hasanfsimsek3 2018-11-19
23_44_55 +0300.afr

Ubuntu 18.04 LTS Terminal: // Rapor hazırlanır

> chmod a+x "tubitak-hasanfsimsek3 2018-11-19 23_44_55 +0300.afr"
> ./arachni_reporter "2018-11-19 23_44_55 +0300.afr" --reporter=html:outfile=/ho
me/hefese/Desktop/**nihai_rapor.html.zip**

Ubuntu 18.04 LTS Terminal: // Rapor görüntülenir

> unzip /home/hefese/Desktop/nihai_rapor.html.zip
> cd nihai_rapor/
> firefox nihai_rapor.html

■ Custom Tarama

Saldırgan Makina : Ubuntu 18.04 LTS Ana Makina
Hedef : Localhost'taki DVWA (Yenisi)

Ubuntu 18.04 LTS Terminal: // Tarama Başlar

./arachni --audit-headers --audit-forms --audit-links --audit-cookies --audit-ui-inputs --audit-ui-forms --audit-parameter-names --audit-with-extra-parameter --http-user-agent "Arachni/v1.5.1" --http-request-concurrency 16 --http-request-header "TEST=TUBITAK-SGE" --input-force --checks=*,-trainer --plugin=autologin:url=http://tubitak-hasanfsimsek3/DVWA-master/login.php,parameters='username=admin&password=password',check='Logout' --scope-include-pattern="^http://tubitak-hasanfsimsek3/DVWA-master/" --scope-exclude-pattern="csrf|setup\.php|security\.php|logout\.php" --plugin=timing_attacks --plugin=uncommon_headers --plugin=uniformity --plugin=autothrottle --plugin=discovery --report-save-path /home/hefese/Desktop/ --snapshot-save-path /home/hefese/ --output-verbose **http://tubitak-hasanfsimsek3/DVWA-master/**

(*) Not: --scope-include-pattern ile hedef url'deki sadece belirli dizin ve altını tara dedik. Ardından gelen --scope-exclude-pattern ile arachni'nin dvwa'daki login'inini kaybetmesine neden olabilecek subdir ve web sayfalarını dışla dedik. Hedef url olarak da kök url + spesifik dizin dedik. Bu şekilde tarama sorunsuz gerçekleşmiştir ve tarama raporunda sitemap sekmesine gelindiğinde gerçekten de taramanın kök url sonrasına eklenen DVWA-master/ dizini yukarısına çıkmadığı ve DVWA-master/ 'ın alt dizinlerini taramada da belirtilen oturum bozması muhtemel dizin ve sayfaların crawl edilmediği & taranmadığı (yani rapordaki sitemap'de taranan url'ler arasında yer almadığı) görülmüştür.

Çıktı:

[~] Scanned completed.
[~] Report is saved in /home/hefese/Desktop/tubitak-hasanfsimsek3 2018-11-19 23_44_55 +0300.afr

Ubuntu 18.04 LTS Terminal: // Rapor hazırlanır

> chmod a+x "tubitak-hasanfsimsek3 2018-11-19 23_44_55 +0300.afr"
> ./arachni_reporter "/home/hefese/Desktop/tubitak-hasanfsimsek3 2018-11-19 23_44_55 +0300.afr"--reporter=html:outfile=/home/hefese/Desktop/**nihai_rapor.html.zip**

Ubuntu 18.04 LTS Terminal: // Rapor görüntülenir

> unzip /home/hefese/Desktop/nihai_rapor.html.zip
> cd nihai_rapor/
> firefox nihai_rapor.html

Arachni Web App Kullanımı

a. Default Kullanımı

New -> Scan -> http://www.example.com

b. Custom Kullanımı

- Custom Profil Oluşturma

Tarama profil adı : Deneme
Oluşturulma Şekli : Default profil seçilip sol üstteki mavi simgeye (Create a new profile based on 'Default') tıklanarak custom şablon oluşturulur.

- Oluşan Profili Konfigure Etme

Oluşan profil dosyasında taramada ihtiyaç duyulabilecek konfigurasyon ayarları yapılabilir. Örn;

i) AutoLogin Plugin'i enable edilir ve arachni'nin tarayacağı web uygulamasına login olması sağlanır.

URL: http://example.com/login.asp
Parameters: username=admin&password=123&login=1
Check: Logout

ii) Tarama boyunca hariç tutulacak scope belirlenir.

Scope Exclude Path Patterns: logout\.asp
changePassword\.asp
profile

Not
Arachni web arayüzündeki "Scope Exclude Path Patterns" arachni command line'da --scope-exclude-pattern="logout\.asp|changePassword\.asp|profile" şeklinde kullanılmaktadır.

- Taramaya Başlama

URL: http://example.com
Profil: Deneme (Bizim oluşturduğumuz)
Instance Count : 1
Method: Direct

Go!

[-] Uyarı

Thread sayısı 1'den fazla olunca taramanın stabilitesi bozulabilir. Bunu gözönünde bulunur.

- Raporlama

Taramanın bittiği ekranın en solundaki kısımda yer alan indir butonuna basılır.

c. Uygulama

[+] Birebir denenmiştir ve başarıyla uygulanmıştır.

Saldırgan Makina	: Ubuntu 18.04 LTS Ana Makinası
Hedef	: Localhost'taki DVWA (Yenisi)

- Custom Profil Oluşturma

Tarama Profili Adı	: DVWA
Oluşturulma Şekli	: Default profil seçilip sol üstteki mavi simgeye (Create a new profile based on 'Default') tıklanarak custom şablon oluşturulmuştur.

- Ayarlama #1

Plugins başlığı altındaki AutoLogin script'i tick yapılmıştır ve açılan panele aşağıdakiler girilmiştir.

URL:	
http://hostname/DVWA-master/login.php	Arachni loopback adresi (127.0.0.1 veya localhost'u) tarayamıyor. O nedenle kendi makinendeki bir web uygulamasını taramak için makinenin hostname'ini url'ye koymalısın. Bu örnek için http://TUBITAK-HASANFSIMSEK3/DVWA-master/ kullanıldı.
Parameters:	
username=admin&password=password	Belki başka uygulamalarda kullanıcı adı ve şifre dışında başka gönderilen değişkenler de olabilir. Onları da (yani o ekstra parametre ve değerlerini de) tahminimce eklemek gerekir
Check Pattern:	
Logout	Login olunduktan sonra ekrana gelen sayfadaki bir string buraya konur.

DVWA için Logout string'i konulmuştur. Yalnız, buraya konacak string login ekranında olmamalı. Bu sayede program login olunup olunmadığı check'ini yapabilecek

- Ayarlama #2

Scope başlığı altındaki "Scope exlude path patterns" bölümüne

csrf
setup\.php
security\.php
logout\.php

bilgileri satır satır girilmiştir.

- Ayarlama #3

Audit başlığı altındaki "Audits elements with both GET and POST requests" seçeneği checked yapılmıştır.

- DVWA'ya Özel Ayarlama #1

DVWA'yı taramak için DVWA-master/config/config.inc.php dosyasındaki default security level ayarı low yapılmıştır.

- DVWA'ya Özel Ayarlama #2

DVWA'yı tararken Trainer modülü hata üretmekte. O nedenle profil konfigurasyon ayarlarındaki Active başlığı altında yer alan Trainer (trainer) seçeneği unchecked yapılmıştır ve sorun çözülmüştür.

- DVWA'ya Özel Ayarlama #3

DVWA'yı tararken Health Map modülü hata üretmekte. O nedenle profil konfigurasyon ayarlarındaki Plugins başlığı altında yer alan Health map (healthmap) seçeneği unchecked yapılmıştır ve sorun çözülmüştür.

- Taramaya Başlama

URL:	http://TUBITAK-HASANFSIMSEK3/DVWA-master/
Profil:	DVWA (Bizim oluşturduğumuz)
Instance Count :	1
Method:	Direct

Go!

[-] Uyarı

Loopback adreste hem arachni web app için bir sunucu hem de DVWA web app için bir sunucu çalışır vaziyette olduğunda arachni web app tarama yükünü taşıyamayabilir. Bu nedenle tarama, olması gerekenden daha erken bitebilir.

Örneğin arachni web app'de thread sayısı 1'den fazla yapılınca hedef web uygulaması DVWA'da bulunan zafiyet bulguları thread sayısı 1 iken bulunan zafiyet bulgularına göre oldukça az olmaktadır. Ne zaman thread sayısı 1'e indirilince o zaman tarama epey uzun sürüyor ve bulgularda göreceli olarak fazlalaşma ve çeşitlenme oluyor. Bu nedenle arachni web app ile loopback'teki bir web uygulamasını test edeceksek arachni thread sayısını 1'den yukarıya çıkarmamalıyız. Ayrıca loopback'teki bir uygulamayı test ederken arachni web app'i 1 thread'le bile çalıştırsak arachni komut satırı aracı kadar stabil sonuçlara ulaşamayabiliriz. Bu nedenle loopback'teki web uygulamalarını test ederken arachni'nin komut satırı arayüzünü kullanmak daha doğru sonuca götürür.

Son olarak loopback'teki bir web uygulamayı tarayacaksak ya da harici bir web uygulamasını tarayacaksak her şartta arachni'nin komut satırı arayüzü arachni'nin web app arayüzüne göre daha performanslı olacağı için arachni'yi komut satırı arayüzü ile kullanma tercih edilebilir. Zaten arachni'nin komut satırı aracı web app arayüzünde oluşan rapor çıktısının aynısını ürettiğinden gayet işlevseldir ve gözönünde bulundurulabilir.

- Raporlama

Taramanın bittiği ekranın en solundaki kısımda yer alan indir butonuna basılır.

Kaynaklar

https://github.com/Arachni/arachni/wiki/Command-line-user-interface
https://github.com/Arachni/arachni/issues/520
http://support.arachni-scanner.com/discussions/problems/1399-no-results-against-dvwa-damn-vulnerable-web-application-and-mutillidae
http://www.arachni-scanner.com/features/framework/crawl-coverage-vulnerability-detection/
http://support.arachni-scanner.com/discussions/questions/12850-use-of-scope-restrict-paths