Acunetix ile Tarama Adımları

Acunetix ile web uygulaması tarama adımları şu şekildedir:

a) Yetkilendirme Ayarlarını Girme

i) Http Basic Auth *(optional)*

Tarayıcıdan http basic yetkilendirmesi geçilir ve artık tarayıcıda taleplere eklenen Authorization çerezi Acunetix->Advanced->Custom Headers kısmına olduğu gibi (Authorization: sdlkfjdsklfjds) eklenir.

ii) Http Custom Cookies *(optional)*

Web uygulamasında çeşitli aksiyonlar çerezler üzerinden gerçekleşiyorsa (örn; dvwa'da uygulama davranışı security çerezi üzerinden değişiklik arz etmekte) o zaman tarayıcıda uygulama oturumunu açıp F12 ile uygulama davranışını etkileyen çerezler etkin oldukları dizin yoluyla beraber (örn; dvwa'da security çerezi /dvwa dizininde etkinken PHPSESSID çerezi / dizininde etkindir) Acunetix->Advanced->Custom Cookies kısmına aşağıdaki gibi eklenmelidir.

Custom Cookies:

[url]	[çerezIsmi]=[çerezDegeri]	// http://192.168.0.28	PHPSESSID=sdlkfdskljfds
[url2]	[çerezIsmi2]=[çerezDegeri2]	// http://192.168.0.28/dvwa	security=low

iii) Http Web Login Auth *(optional)*

Acunetix taramaya başladığında hedef web uygulamasında oturum açabilmesi ve içerinin de taranabilmesi için Acunetix->General->Login Recorder->Use pre-recorded login sequence->New seçeneği kullanılmalıdır. Gelen login adımları kaydetme penceresinde ilk aşamada Login panelin yer aldığı URL, pencerenin adres çubuğuna ENTER'lanarak kaydedilmelidir. Sonra, gelen login paneli ekranına hesap bilgileri girilmelidir. Ardından oturum aç butonuna tıklanmalı ve oturum açılmalıdır. Bu yapılan (gerçekleştirilen) adımlar sağ yan boşlukta satır satır sıralanacaktır. Login işlemi sonrası pencere ekranında Next denerek bir sonraki aşamaya (logout adımını / adımlarını gösterme aşamasına) geçilir ve logout butonuna / butonlarına tıklanarak "Restrict Request Using Exact Match" denir. Bu sayede acunetix, logout yapan noktaları öğrenmiş olur. Logout yapan yerlerin işaretlemesi (tıklamaları) işlemi sonrası sağ yan boşlukta satır satır bu tıklama noktaları sıralanacaktır. Acunetix'e logout'u öğreten bu ikinci aşama pencere ekranında Next denerek son aşamaya (yani login ve logout aşamalarındaki adımlar / mekanizmalar sorunsuz çalışıyor mu testinin yapıldığı aşamaya) geçilir ve ekrana "...successfully..." popup'ı gelir. Böylece ilk iki aşamada sorun olmadığı görülür. Son olarak bulunulan aşamadaki (yani son aşamadaki) yan sağ boşlukta yer alan url incelenir. Bu url acunetix'in, tarama esnasında oturumu kaybedip kaybetmediğini test etmek için kullanacağı bir url olacaktır. Bu url sadece oturum açıkken erişilebilen bir url olmalıdır. Böylece acunetix tarama esnasında bu url'i test ederek halen oturumda mıyım yoksa oturum (örn; timeout gibi) bir nedenden dolayı sonlandırılmış mı anlayabilecektir. Sadece login'ken erişilebilen bir url uygulamada seçilip acunetix login recorder son aşamasındaki sağ yan boşlukta url olarak girilir ve Check Pattern ile girilen url'de problem / erişimde sıkıntı var mı kontrolü yapılır. Ekrana gelen "...pattern verified..." popup'ı sonrası pencerede Finish diyerek Login Recorder işlemi tamamlanır. Artık acunetix tarama sırasında login

olabilecektir. Logout noktalarına girmeyerek oturumun devamlılığını sağlayabilecektir. Ayrıca oturum, zaman aşımı v.b. nedenlerden ötürü düşmüşse bu durumda test url'i ile yaptığı testler neticesinde oturumun kaybedildiğini gördüğü an login olma adımlarını tekrar işleterek taramasına oturum açık vaziyette halen devam edebilecektir.

Not: Login Recorder seçeneği ile
-> Recording'de Login olma,
-> Restriction'da sadece logout olma,
yapılır. Restriction aşamasında (logout'u öğretme aşamasında) dışlanacak path'i de öğreteyim maksadıyla link tıklaması kesinlikle yapılmamalı. Dışlanacak path'ler için Acunetix Crawling sekmesi kullanılacaktır. Restriction aşamasında Logout dışında yapılacak tıklamalar oturumun sürdürülebilirliğini sekteye uğratmaktadır / uğratabilir.

b) Acunetix Crawling Ayarlarını Girme

Hedef web uygulamasında tarama esnasında tarama dışında tutulacak dizin ve dosya yolları için Acunetix->Crawl sekmesine gelip Exclude Paths seçeneğine regexp pattern formatında dosya ve dizin yolları girilebilir. Bu; uygulamanın yapısında değişikliğe sebep olabilecek ve istenmeyen aktivitelere yol açabilecek (örn; uygulama veritabanını sıfırlama, uygulama hesap parolasını değiştirme,… gibi) dosya ve dizin yollarının tarama dışında tutulmasını sağlamak için vardır. Böylece Acunetix, uygulamanın yapısını bozmayak şekilde tarama yapabilir. Not: Exclude Path seçeneği sadece regexp pattern formatında değer alabilmektedir. Dizin yolu regexp pattern'ları için https://regex101.com/ adresinden yararlanabilirsin.

Exclude Paths;	Dvwa için Exclude Path Pattern Örnekleri;
dizinYolu\/dizinIsmi\/	// örn; vulnerabilities\/csrf\/
dizinYolu\/dizinIsmi\/dosyaIsmi\.php	// örn; vulnerabilities\/csrf\/index\.php
dosyaIsmi2\.php	// örn; security\.php veya setup\.php

Ek Bilgi;

[+] Birebir deneyimlenmiştir.

Acunetix ile Dvwa'yı tararken (bkz. Yaz Tatili 2014 / Acunetix ile Vulnerable Uygulama Tarama ve Zararlı Trafiği Dinleme.docx) tarama ayarlarında exclude paths kısmına dvwa sayfası setup.php, security.php ve csrf/ dizinini girmen gerekmişti. Çünkü setup.php sayfası uygulamanın kullandığı veritabanını reset'lediğinden dışlanmak istenmiştir. security.php sayfası uygulamanın güvenlik seviyesini arttırdığından taramanın bulgularını azaltmasın diye dışlanmak istenmiştir. csrf/ dizini ise senaryosu gereği uygulamanın hesap parolasını değiştirdiğinden tarama dışında tutulması tercih edilmiştir.

Acunetix exclude paths kısmına bu üç dışlanacak yolu (setup.php, security.php, csrf/ 'i) regexp pattern'ı halinde doğruca koyabilmek için regexp101.com sitesinde test edilmişlerdir.

Örn;

x-)

Regexp101.com’da pattern kutucuğuna girdiğim string:

Pattern textbox;

setup\.php

Test String textbox; (yani pattern kutucuğu bu test string’i içerisinde bir yerde eşleşebilecek mi testi):

http://X.Y.Z.T/dvwa/setup.php // Regexp101 'e bu test string'i
// verildiğinde yukarıdaki regexp
// pattern’ı ile eşleşme yeşil
// oluyor.

y-)

Regexp101.com’da pattern kutucuğuna girdiğim string:

Pattern textbox;

security\.php

Test string: (yani pattern kutucuğu bu test string’i içerisinde bir yerde eşleşebilecek mi testi):

http://X.Y.Z.T/dvwa/security.php // Regexp101 'e bu test string'i
// verildiğinde yukarıdaki regexp
// pattern’ı ile eşleşme yeşil
// oluyor.

z-)

Regexp101.com’da pattern kutucuğuna girdiğim string:

Pattern textbox;

vulnerabilities\/csrf\/

Test string: (yani pattern kutucuğu bu test string’i içerisinde bir yerde eşleşebilecek mi testi):

http://X.Y.Z.T/dvwa/vulnerabilities/csrf/ // Regexp101 'e bu test string'i
// verildiğinde yukarıdaki regexp
// pattern’ı ile eşleşme yeşil
// oluyor.

Yani Acunetix yazılımı hedef makinadaki vulnerable web uygulaması Dvwa’yı

Hedef adres: http://X.Y.Z.T/dvwa/

tarayacak şekilde ayarlandığında ve exclude path olarak örneğin

vulnerabilities\/csrf\/

verildiğinde tarama sırasında vulnerabilities/csrf/ dizinini taramayacaktır.

Not (1):

Acunetix'e hedef adres olarak http://X.Y.Z.T/dvwa/ verilmiştir. Yani http://X.Y.Z.T/dv
wa değil. Sonda slash vardır. O nedenle exclude path'te dışlanacak yol olarak /vulnerabili
ties/csrf/ yerine vulnerabilities/csrf/ koymak mantıklı olandır. Yani vulnerabilities\/csrf\/
Diğer türlü \/vulnerabilities\/csrf\/ denseydi bu durumda

http://X.Y.Z.T/dvwa//vulnerabities/csrf

yolu var olamayacağından

http://X.Y.Z.T/dvwa/vulnerabities/csrf

yolu acunetix taramasına denk geldiğinde atlanacak bir yol olarak görülmeyecektir ve
taranacaktır. Çünkü

http://X.Y.Z.T/dvwa//vulnerabities/csrf (=> Çıktı: 404 Not found)

yolu ile

http://X.Y.Z.T/dvwa/vulnerabities/csrf (=> Çıktı: CSRF sayfası)

yolu aynı değildir. Bunu ilk adresi girdiğinde tarayıcının verdiği 404 ve ikincisini girdiğinde
tarayıcının verdiği csrf sayfasının kendisi mukayesesiyle anlayabilirsin. Aynı yol olsalar ikisi
de aynı sonuca götürmeliydi.

Not (2):

Daha önce exclude path kısmından dışla dediğinde uygun pattern'ı kullanamadığın için
dizinler dışlanmadığından (örn; csrf/ dizini için;

/csrf/$

veya

*/csrf/index\.php$

gibi) bu yanlış girdiğin pattern'lar dolayısıyla csrf dizini altındaki parola değiştirme
işlemi çalışmaktaydı ve acunetix parolayı değiştirmekteydi. Dolayısıyla iK Test
makinasındaki Dvwa'da admin ve password hesap bilgisiyle oturum açamama durumu
yaşıyordun. Bu ise eski bir snapshot'a restore yapmak külfetini sana veriyordu. Fakat bu
sefer Regexp101 ile test edip doğru pattern'ı girdiğinde

vulnerabilities\/csrf\/

ve Acunetix taraması bittiğinde parola değişikliği gibi bir problem olmadığını defalarca
yaptığın taramalar sonucu gördün. DVWA login sayfasından admin ve password ikilisiyle
(yani mevcut hesap bilgileriyle) halen giriş yapabiliyor olduğunu görebildin.

Kaynaklar

// Login Recorder'da sadece Login Olabilme ve Logout
// Yapma Adımları Takip edilmeli. Baþka iþ deðil.
https://www.youtube.com/watch?v=uWx4M7rPrX0

// Exclude Paths Ayarı
https://www.acunetix.com/blog/docs/exclude-directory-file-from-scan/

// Exlude Paths Ayarını Test Etme
https://regex101.com/