

Enumerate Applications on Webserver (Web Sunucusundaki Uygulamaları Listeleme)

Summary (Özet)

Web uygulama güvenlik açıkları için testte çok önemli bir adım, hangi uygulamaların bir web sunucusunda barındırıldığını bulmaktır. Birçok uygulama, uzaktan kumanda almak veya verileri kullanmak için istismar edilebilecek güvenlik açıklarını ve bilinen saldırı stratejilerini bilmiştir. Buna ek olarak, birçok uygulama genellikle yanlış yapılandırılır veya güncellenmez, yalnızca "içsel" olarak kullanıldığı ve bu nedenle hiçbir tehdit olmadığı algısı nedeniyle güncellenmez. Sanal web sunucularının çoğalmasıyla, bir IP adresi ile bir web sunucusu arasındaki geleneksel 1:1 tipi ilişki, orijinal öneminin çoğunu kaybediyor. Sembolik isimleri aynı IP adresine karar veren birden fazla web sitesine veya uygulamaya sahip olmak nadir değildir. Bu senaryo barındırma ortamlarıyla sınırlı değildir, aynı zamanda sıradan kurumsal ortamlar için de geçerlidir.

Güvenlik profesyonellerine bazen test için bir hedef olarak bir dizi IP adresi verilir. Bu senaryonun penetrasyon testi tipi bir katılıma daha çok benzemesi tartışmalıdır, ancak her durumda böyle bir atamanın tüm web uygulamalarını bu hedef aracılığıyla erişilebilir olarak test etmesi beklenmektedir. Sorun, verilen IP adresinin 80 numaralı bağlantı noktasında bir HTTP hizmetine ev sahipliği yapmasıdır, ancak bir test cihazı IP adresini (bildikleri tek şey) ile erişirse, "Bu adreste yapılandırılmış web sunucusu yok" veya benzer bir mesajı bildirir. Ancak bu sistem, ilgisiz sembolik (DNS) isimlerle ilişkili bir dizi web uygulaması "gizleyebilir". Açıkçası, analizin boyutu test eden testçinin tüm uygulamalarından derinden etkilenir veya yalnızca farkında oldukları uygulamaları test eder.

Bazen, hedef şartname daha zengindir. Test cihazına IP adreslerinin bir listesi ve ilgili sembolik isimleri verilebilir. Bununla birlikte, bu liste kısmi bilgileri iletebilir,

yani bazı sembolik isimleri atabilir ve müşteri bunun farkında bile olmayabilir (büyük organizasyonlarda gerçekleşme olasılığı daha yüksektir).

Değerlendirmenin kapsamını etkileyen diğer konular, açık olmayan URL'lerde yayınlanan web uygulamaları ile temsil edilir (örneğin, <http://www.example.com/some-strange-URL>),

başka bir yerde referans alınmıyor. Bu, hatayla (yanlış yapılandırmalar nedeniyle) veya kasıtlı olarak (örneğin, reklamsız idari arayüzler) gerçekleşebilir.

Bu sorunları ele almak için web uygulama keşfini gerçekleştirmek gerekir.

Test Objectives (Test Hedefleri)

- Bir web sunucusunda bulunan kapsam dahilinde uygulamaların numaralandırılması.

How to Test (Nasıl Test Edilir)

Web uygulaması keşfi, belirli bir altyapıda web uygulamalarını tanımlamayı amaçlayan bir süreçtir. İkincisi genellikle bir dizi IP adresi olarak tanımlanır (belki bir net blok), ancak bir dizi DNS sembolik isimden veya ikisinin bir karışımından oluşabilir. Bu bilgiler, klasik tarzda bir penetrasyon testi veya uygulama odaklı bir değerlendirme olsun, bir değerlendirmenin yürütülmesinden önce verilir. Her iki durumda da, katılım kuralları aksini belirtmedikçe (örneğin, yalnızca URL'de bulunan uygulamayı test edin <http://www.example.com/>), değerlendirme kapsamda en kapsamlı olmaya çalışmalıdır, yani verilen hedef aracılığıyla erişilebilen tüm uygulamaları belirlemelidir. Aşağıdaki örnekler, bu hedefe ulaşmak için kullanılabilecek birkaç tekniği inceler.

Aşağıdaki tekniklerden bazıları İnternet'e bakan web sunucuları, yani DNS ve ters IP web tabanlı arama hizmetleri ve arama motorlarının kullanımı için geçerlidir. Örnekler özel IP adreslerinden yararlanır (örneğin 192.168.1.100Aksi belirtilmedikçe, jenerik IP adreslerini temsil eden ve yalnızca anonimlik amacıyla kullanılan).

Belirli bir DNS adı (veya bir IP adresi) ile ilgili kaç uygulama olduğunu etkileyen üç faktör vardır:

1. Farklı Temel URL

Bir web uygulaması için bariz giriş noktasıdır www.example.com , yani, bu kısa nota ile, web uygulamasının kaynaklandığını düşünüyoruz <http://www.example.com/> (Aynı şey https için de geçerlidir). Ancak, bu en yaygın durum olsa da, başvuruyu başlatmaya zorlayan hiçbir şey yoktur. / . .

Örneğin, aynı sembolik isim, aşağıdaki gibi üç web uygulamasıyla ilişkilendirilebilir:
<http://www.example.com/url1><http://www.example.com/url2><http://www.example.com/url3>

Bu durumda, URL <http://www.example.com/> Anlamlı bir sayfayla ilişkilendirilmezdi ve test cihazı onlara nasıl ulaşacağını açıkça bilmedikçe üç uygulama **gizlenecek**, yani test cihazı *url1**url1*, *url2* veya *url3**url3*'ü biliyor. Genellikle web uygulamalarını bu şekilde yayınlamaya gerek yoktur, ancak sahibi standart bir şekilde erişilebilir olmalarını istemedikçe ve kullanıcıları tam konumları hakkında bilgilendirmeye hazır değildir. Bu, bu uygulamaların gizli olduğu anlamına gelmez, sadece varlıklarının ve konumlarının açıkça reklamı yapılmadığı anlamına gelmez.

2. Standart olmayan Limanlar

Web uygulamaları genellikle 80 (http) ve 443 (https) üzerinde yaşarken, bu liman numaraları hakkında sihirli bir şey yoktur. Aslında, web uygulamaları keyfi TCP bağlantı noktaları ile ilişkilendirilebilir ve aşağıdaki gibi bağlantı noktası numarasını belirterek referans verilebilir:

[http\[s\]://www.example.com:port/](http[s]://www.example.com:port/) . . Örneğin, <http://www.example.com:20000/> . .

3. Sanal Ev Sahipleri

DNS, tek bir IP adresinin bir veya daha fazla sembolik isimle ilişkilendirilmesini sağlar. Örneğin, IP adresi 192.168.1.100 DNS isimleriyle ilişkilendirilebilir

www.example.com , helpdesk.example.com , webmail.example.com . . Tüm isimlerin aynı DNS alanına ait olması gerekli değildir. Bu 1'e N ilişkisi, sanal konakçılar kullanılarak farklı içerikler sunmak için yansıtılabilir. Bahsettiğimiz sanal ev sahibini belirten bilgiler HTTP 1.1 Host başlığına gömülüdür.

Açıklığa ek olarak diğer web uygulamalarının varlığından şüphelenmez.

www.example.com , bilmiyorlarsa helpdesk.example.com ve webmail.example.com . .

Approaches to Address Issue 1 - Non-standard URLs (Sorunu Ele Almak İçin Yaklaşımlar 1 - Standart Olmayan URL'ler)

Standart adı verilmeyen web uygulamalarının varlığını tam olarak belirlemenin bir yolu yoktur. Standart olmayan olmak, adlandırma sözleşmesini düzenleyen sabit bir kriter yoktur, ancak testçinin bazı ek bilgiler elde etmek için kullanabileceği bir dizi teknik vardır.

İlk olarak, web sunucusu yanlış yapılandırılmışsa ve dizin taramasına izin veriyorsa, bu uygulamaları tespit etmek mümkün olabilir. Güvenlik açığı tarayıcıları bu açıdan yardımcı olabilir.

İkincisi, bu uygulamalar diğer web sayfaları tarafından referans alınabilir ve web arama motorları tarafından örümceklenme ve dizine eklenme şansı vardır. Testçiler bu tür **gizli** uygulamaların varlığından şüpheleniyorsa www.example.com Site operatörünü kullanarak ve bir sorgunun sonucunu inceleyerek arama yapabilirler.

site: www.example.com . . Geriye dönen URL'ler arasında, böyle bariz olmayan bir uygulamaya işaret eden bir tane olabilir.

Başka bir seçenek, yayınlanmamış uygulamalar için aday olabilecek URL'leri araştırmaktır. Örneğin, bir web posta ön ucuna URL'lerden erişilebilir olabilir.

<https://www.example.com/webmail> , <https://webmail.example.com/> , ya da <https://mail.example.com/> . . Aynı şey, gizli URL'lerde (örneğin, bir Tomcat yönetimi arayüzü) yayınlanabilecek ve yine de hiçbir yere atıfta bulunulmayan idari arayüzler için geçerlidir. Bu nedenle, biraz sözlük tarzı arama yapmak (veya "akıllı tahmin") bazı sonuçlar verebilir. Güvenlik açığı tarayıcıları bu açıdan yardımcı olabilir.

Approaches to Address Issue 2 - Non-standard Ports (Konu 2 - Standart Olmayan Limanlar)

Standart olmayan limanlarda web uygulamalarının varlığını kontrol etmek kolaydır. Harita gibi bir port tarayıcı, hizmet tanımayı gerçekleştirebilir **-sV** Seçenek,ve keyfi limanlarda http[s] hizmetlerini tanımlayacaktır. Gerekli olan, tüm 64k TCP bağlantı adresi alanının tam bir taramasıdır.

Örneğin, aşağıdaki komut, bir TCP bağlantı taraması, IP'deki tüm açık bağlantı noktaları ile bakacaktır. 192.168.1.100 ve hangi hizmetlerin kendilerine bağlı olduğunu

belirlemeye çalışacaktır (sadece *temel* anahtarlar gösterilir - harita, tartışmaları kapsamı olmayan geniş bir seçenek kümesine sahiptir):

```
nmap -Pn -sT -sV -p0-65535 192.168.1.100
```

Çıkışı incelemek ve SSL sarılmış hizmetlerin enflörtüsünü http veya endikasyon için aramak yeterlidir (bu, https olduklarını doğrulamak için araştırılmalıdır). Örneğin, önceki komutun çıktısı şöyle görünebilir:

Interesting ports on 192.168.1.100:

(The 65527 ports scanned but not shown below are in state: closed)

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 3.5p1 (protocol 1.99)
--------	------	-----	-------------------------------

80/tcp	open	http	Apache httpd 2.0.40 ((Red Hat Linux))
--------	------	------	---------------------------------------

443/tcp	open	ssl	OpenSSL
---------	------	-----	---------

901/tcp	open	http	Samba SWAT administration server
---------	------	------	----------------------------------

1241/tcp	open	ssl	Nessus security scanner
----------	------	-----	-------------------------

3690/tcp	open	unknown	
----------	------	---------	--

8000/tcp	open	http-alt?	
----------	------	-----------	--

8080/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1
----------	------	------	-------------------------------------

Bu örnekten, şunu görebilirsiniz:

- 80 numaralı portda çalışan bir Apache HTTP sunucusu bulunmaktadır.
- Bağlantı noktasında 443 numaralı telefonda bir HTTPS sunucusu var gibi görünüyor (ancak bunun örneğin ziyaret ederek doğrulanması gerekiyor
<https://192.168.1.100> Bir tarayıcı ile birlikte).
- 901 numaralı bağlantı noktasında Samba SWAT web arayüzü bulunmaktadır.
- Bağlantı noktasındaki 1241 numaralı telefonda yapılan hizmet HTTPS değil, SSL sarılı Nessus daemon'dur.
- Port 3690, belirtilmemiş bir hizmete sahiptir (nmap, *parmak izini* geri verir - burada netlik için atlanmış - hangi hizmeti temsil ettiğini bildiğiniz için, nmap parmak izi veritabanına dahil etmek için gönderme talimatlarıyla birlikte).
- 8000 numaralı bağlantı noktasındaki başka bir belirtilmemiş hizmet; bu, bu bağlantı noktasında HTTP sunucularını bulmak nadir olmadığı için HTTP

olabilir. Şu konuyu inceleyelim:

```
$ telnet 192.168.10.100 8000
Trying 192.168.1.100...
Connected to 192.168.1.100.
Escape character is '^]'.
GET / HTTP/1.0
```

```
HTTP/1.0 200 OK
pragma: no-cache
Content-Type: text/html
Server: MX4J-HTTPD/1.0
expires: now
Cache-Control: no-cache
```

```
<html>
```

```
...
```

Bu, aslında bir HTTP sunucusu olduğunu doğrular. Alternatif olarak, testçiler URL'yi bir web tarayıcısı ile ziyaret edebilirdi; veya yukarıdaki gibi HTTP etkileşimlerini taklit eden GET veya HEAD Perl komutlarını kullanabilirdi (ancak BAŞALI istekler tüm sunucular tarafından onurlandırılmayabilir).

- Apache Tomcat 8080 numaralı limanda çalışıyor.

Aynı görev güvenlik açığı tarayıcıları tarafından gerçekleştirilebilir, ancak önce tercih edilen tarayıcının standart olmayan bağlantı noktalarında çalışan HTTP[S] hizmetlerini tanımlayabileceğini kontrol edin. Örneğin, Nessus bunları keyfi bağlantı noktalarında tanımlayabilir (tüm limanları taraması talimatı verilir) ve nmap ile ilgili olarak, bilinen web sunucusu güvenlik açıklarında bir dizi testin yanı sıra HTTPS hizmetlerinin SSL yapılandırmasında da sağlayacaktır. Daha önce de belirtildiği gibi, Nessus ayrıca, başka türlü fark edilmeyecek popüler uygulamaları veya web arayüzlerini de tespit edebilir (örneğin, bir Tomcat idari arayüzü).

Approaches to Address Issue 3 - Virtual Hosts (Konu 3 - Sanal Ev Sahipleri Ele Almak İçin Yaklaşımlar)

Belirli bir IP adresiyle ilişkili DNS adlarını tanımlamak için kullanılabilecek bir dizi teknik vardır. `x.y.z.t` . .

DNS Zone Transfers (DNS Bölgesi Transferleri)

Bu teknik, bölge aktarımlarının DNS sunucuları tarafından büyük ölçüde onurlandırılmadığı gerçeği göz önüne alındığında, günümüzde sınırlı bir kullanıma sahiptir. Ancak, denemeye değer olabilir. Her şeyden önce, testçiler hizmet veren isim sunucularını belirlemelidir. `x.y.z.t` . . Eğer sembolik bir isim biliniyorsa `x.y.z.t` (Olmasına izin verin `www.example.com`), isim sunucuları, gibi araçlarla belirlenebilir `nslookup` , `host` , ya da `dig` DNS NS kayıtlarını isteyerek.

sembolik bir isim bilinmiyorsa `x.y.z.t` Ancak hedef tanım en az sembolik bir isim içerir, testçiler aynı işlemi uygulamaya çalışabilir ve bu ismin isim sunucusunu sorgulayabilir (bunu umarak `x.y.z.t` Bu isim sunucusu tarafından da servis edilecektir). Örneğin, hedef IP adresinden oluşuyorsa `x.y.z.t` ve adı `mail.example.com` , alan adı için isim sunucularını belirleyin `example.com` . .

Aşağıdaki örnek, isim sunucularının nasıl tanımlanacağını gösterir

`www.owasp.org` Kullanarak `host` Komuta:

```
$ host -t ns www.owasp.org
www.owasp.org is an alias for owasp.org.
owasp.org name server ns1.secure.net.
owasp.org name server ns2.secure.net.
```

Bölge aktarımı artık alan adı için isim sunucularına talep edilebilir `example.com` . . Test cihazı şanslıysa, bu etki alanı için DNS girişlerinin bir listesini geri alacaklar. Bu bariz olanı içerecektir `www.example.com` ve çok açık olmayanlar `helpdesk.example.com` ve `webmail.example.com` (muhtemelen diğerleri). Bölge transferi ile iade edilen tüm isimleri kontrol edin ve hedefin değerlendirilmesiyle ilgili olanların tümünü düşünün.

Bölge transferi talep etmeye çalışmak `owasp.org` İsim sunucularından bir tanesinden:

```
$ host -l www.owasp.org ns1.secure.net
Using domain server:
Name: ns1.secure.net
```

Address: 192.220.124.10#53

Aliases:

Host www.owasp.org not found: 5(REFUSED)
; Transfer failed.

DNS Inverse Queries (DNS Ters Sorgular)

Bu işlem öncekine benzer, ancak ters (PTR) DNS kayıtlarına dayanır. Bir bölge transferi talep etmek yerine, rekor türünü PTR'ye ayarlamayı deneyin ve verilen IP adresinde bir sorgu yayınlayın. Testçiler şanslıysa, bir DNS adı girişini geri alabilirler. Bu teknik, garanti edilmeyen IP-sembolik isim haritalarının varlığına dayanır.

Web-based DNS Searches (Web Tabanlı DNS Aramaları)

Bu tür bir arama DNS bölgesi aktarımına benzer, ancak DNS'de isim tabanlı aramalar sağlayan web tabanlı hizmetlere dayanır. Bu hizmetlerden biri Netcraft Search DNS hizmetidir. Test cihazı, seçtiğiniz alana ait isimlerin bir listesini sorgulayabilir. [example.com](#) . . Ardından, elde ettikleri isimlerin inceledikleri hedefle ilgili olup olmadığını kontrol edeceklerdir.

Reverse-IP Services (Ters-IP Hizmetleri)

Reverse-IP hizmetleri, DNS ters sorgularına benzer, testçilerin bir isim sunucusu yerine web tabanlı bir uygulamayı sorguladığı farkla. Bu tür hizmetlerin bir kısmı mevcuttur. Kısmi (ve genellikle farklı) sonuçları iade etme eğiliminde olduklarından, daha kapsamlı bir analiz elde etmek için birden fazla hizmet kullanmak daha iyidir.

Alan Aletleri Ters IP (ücretsiz üyelik gerektirir)

BingBing, sözdizim: [ip:x.x.x.x](#)

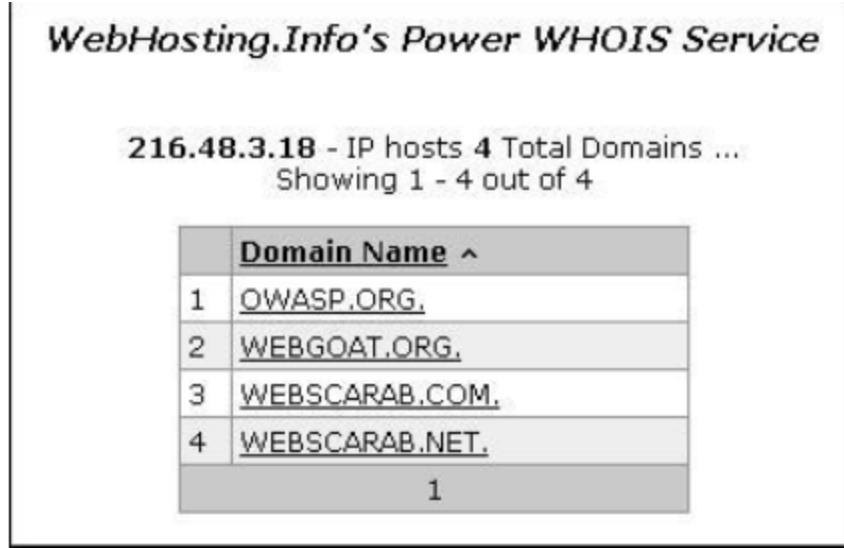
Webhosting Bilgisi, sözdizimi: <http://whois.webhosting.info/x.x.x.x>

DNSstuff (çoklu hizmetler mevcuttur)

Net Kare (yaşam alanları ve IP adreslerinde birden fazla sorgu, kurulum gerektirir)

Aşağıdaki örnek, yukarıdaki ters IP hizmetlerinden birine yapılan bir sorgunun sonucunu gösterir. [216.48.3.18](#) , www.owasp.org'un IP adresi. Aynı adrese haritalanan

üç tane daha bariz olmayan sembolik isim ortaya çıktı.



The screenshot shows a web interface titled "WebHosting.Info's Power WHOIS Service". It displays the IP address "216.48.3.18" and states "IP hosts 4 Total Domains ... Showing 1 - 4 out of 4". Below this is a table with the following content:

	Domain Name ^
1	OWASP.ORG
2	WEBGOAT.ORG
3	WEBSCARAB.COM
4	WEBSCARAB.NET

At the bottom of the table, the number "1" is displayed.

Şekil 4.1.4-1: OWASP Whois Bilgisi

Googling (Kategori: Google)

Önceki tekniklerden toplanan bilgileri takiben, testçiler analizlerini rafine etmek ve artırmak için arama motorlarına güvenebilirler. Bu, hedefe ait ek sembolik isimlerin veya bariz olmayan URL'ler aracılığıyla erişilebilen uygulamaların kanıtlarını verebilir.

Örneğin, ilgili önceki örneği göz önünde bulundurularak www.owasp.org Test cihazı, Google ve diğer arama motorlarını yeni keşfedilen alan adı ile ilgili bilgi (dolana, DNS isimleri) arayan sorgulayabilir. webgoat.org , webscarab.com - , ve webscarab.net . .

Google teknikleri Test: Spiders, Robots ve Crawlers'da açıklanmıştır.

Tools (Araçlar)

- DNS arama araçları gibi [nslookup](#) , [dig](#) Ve benzer.
- Arama motorları (Google, Bing ve diğer büyük arama motorları).
- DNS ile ilgili özel web tabanlı arama hizmeti: metne bakın.
- Nmap
- Nessus Güvenlik Açığı Tarayıcı

- Nikto'nun