

Content Discovery

Task 1 What Is Content Discovery? (İçerik Keşfi Nedir?)

İlk olarak, web uygulama güvenliği bağlamında içerik nedir diye sormalıyız. İçerik birçok şey olabilir; bir dosya, video, resim, yedekleme, bir web sitesi özelliği. İçerik keşfi hakkında konuştuğumuzda, bir web sitesinde görebileceğimiz bariz şeylerden bahsetmiyoruz; bu, bize hemen sunulmayan ve her zaman genel erişim için tasarlanmamış olan şeylerdir.

Bu içerik, örneğin, personel kullanımına yönelik sayfalar veya portallar, web sitesinin eski sürümleri, yedekleme dosyaları, yapılandırma dosyaları, yönetim panelleri vb. olabilir.

Bir web sitesindeki içeriği keşfetmenin üç ana yolu vardır ve biz bunları ele alacağız. Manuel, Otomatik ve OSINT (Açık Kaynak İstihbaratı).

AttackBox'ı ("AttackBox'ı Başlat" mavi düğmesine tıklayarak) ve bu görevdeki makineyi başlatın.

soru ⇒ M ile başlayan İçerik Keşfi yöntemi nedir?

cevap ⇒ **Manually**

soru ⇒ A ile başlayan İçerik Keşfi yöntemi nedir?

cevap ⇒ **Automated**

soru ⇒ O ile başlayan İçerik Keşfi yöntemi nedir?

cevap ⇒ **OSINT**

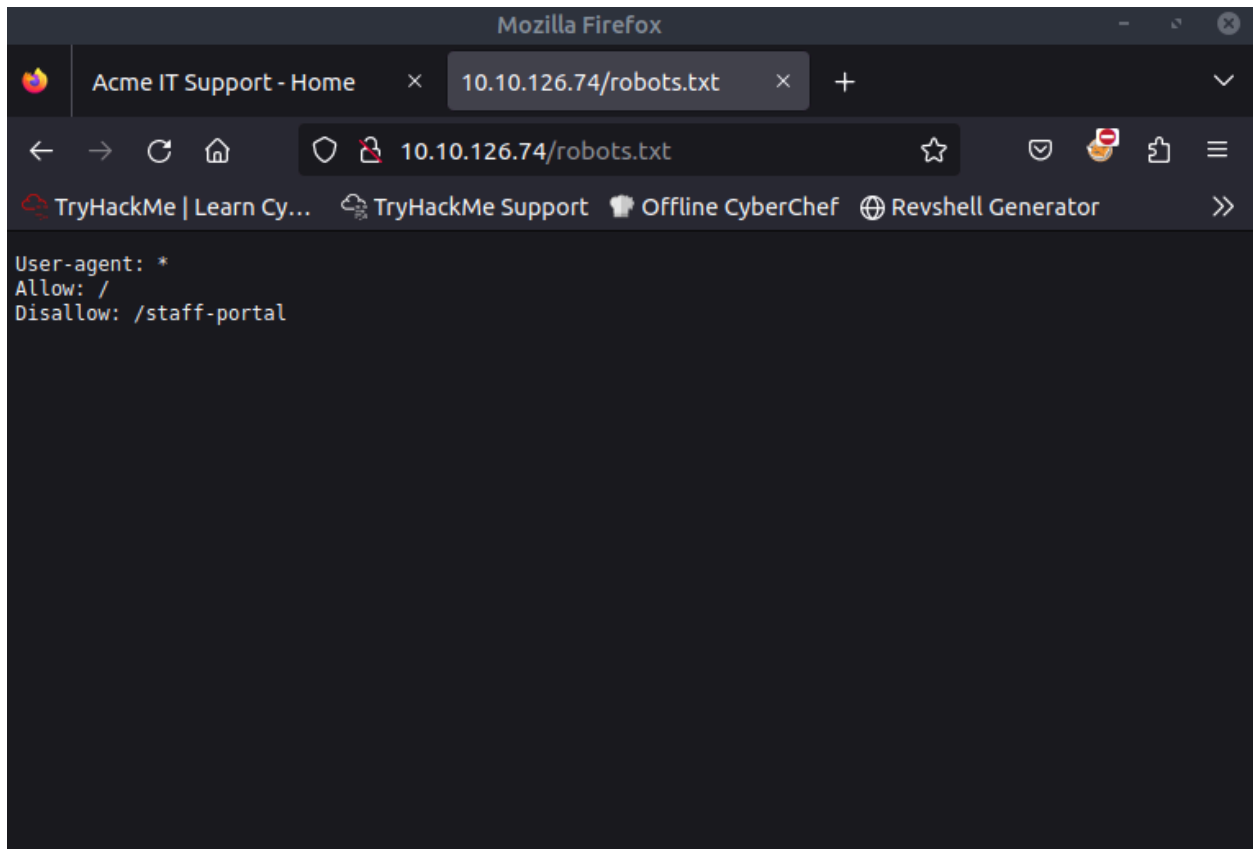
Task 2 Manual Discovery - Robots.txt (Manuel Keşif - Robots.txt)

Daha fazla içerik keşfetmeye başlamak için bir web sitesinde manuel olarak kontrol edebileceğimiz birden fazla yer vardır.

Robots.txt

Robots.txt dosyası, arama motorlarına hangi sayfaları arama motoru sonuçlarında gösterip gösteremeyeceklerini söyleyen veya belirli arama motorlarının web sitesini taramasını tamamen yasaklayan bir belgedir. Arama motoru sonuçlarında görüntülenmemeleri için belirli web sitesi alanlarını kısıtlamak yaygın bir uygulama olabilir. Bu sayfalar, yönetim portalları veya web sitesinin müşterilerine yönelik dosyalar gibi alanlar olabilir. Bu dosya bize web sitesi sahiplerinin sızma testi uzmanları olarak keşfetmemizi istemedikleri yerlerin harika bir listesini verir.

Listelenmesini istemedikleri bir şey olup olmadığını görmek için Acme IT Support web sitesindeki robots.txt dosyasına bir göz atın - Bunu yapmak için AttackBox'ta Firefox'u açın ve şu URL'yi girin: http://machine_ip/robots.txt (bu URL, görev 1'de makineyi başlattığınız andan itibaren 2 dakika içinde güncellenecektir)



soru ⇒ Robots.txt'de web tarayıcıları tarafından görüntülenmesine izin verilmeyen dizin nedir?

cevap ⇒ **/staff-portal**

Task 3 Manual Discovery - Favicon (Manuel Keşif - Favicon)

Favicon

Favicon, bir web sitesini markalamak için kullanılan, tarayıcının adres çubuğunda veya sekmesinde görüntülenen küçük bir simgedir.

Bazen bir web sitesi oluşturmak için çerçeveler kullanıldığında, kurulumun bir parçası olan bir favicon artık kalır ve web sitesi geliştiricisi bunu özel bir tane ile değiştirmezse, bu bize hangi çerçevenin kullanıldığını dair bir ipucu verebilir.

OWASP, hedef favicon

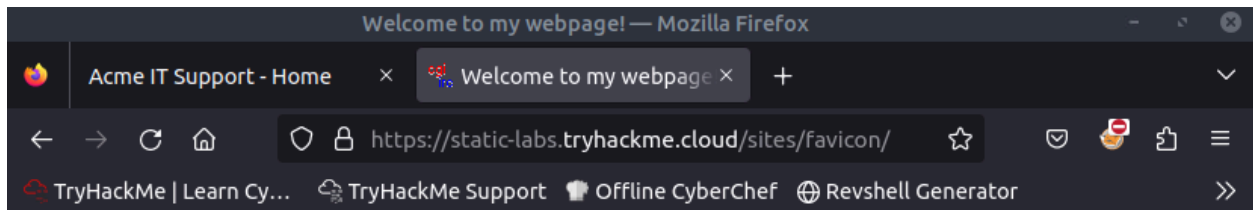
https://wiki.owasp.org/index.php/OWASP_favicon_database ile karşılaştırmak için kullanabileceğiniz ortak çerçeve simgelerinden oluşan bir veritabanı barındırmaktadır. Çerçeve yığını öğrendikten sonra, bu konuda daha fazla bilgi edinmek için harici kaynakları kullanabiliriz (bir sonraki bölüme bakın).

Pratik Alıştırma:

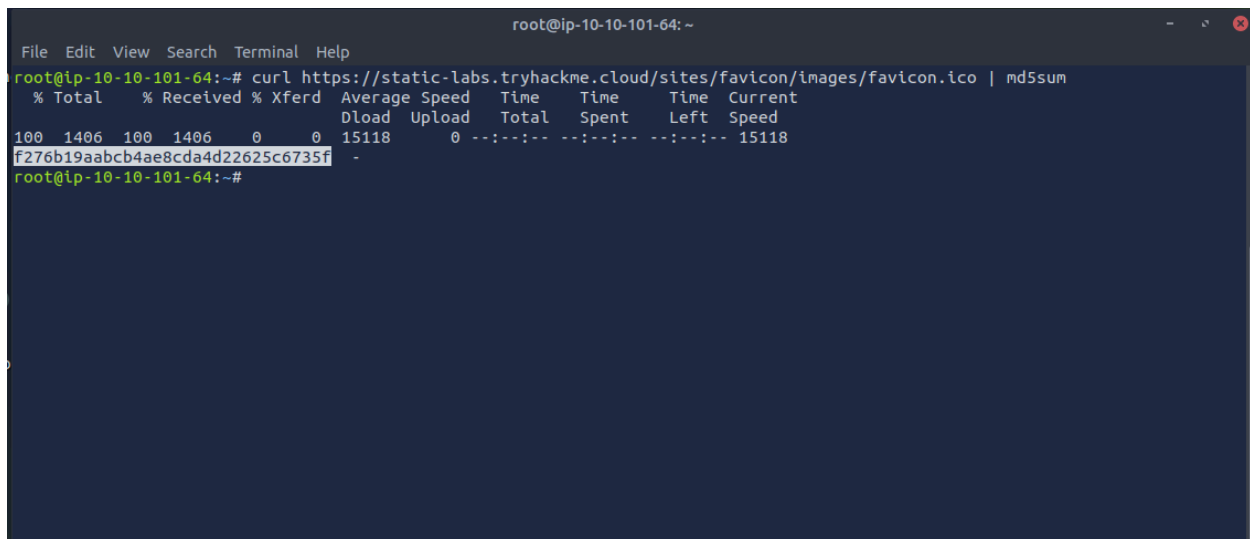
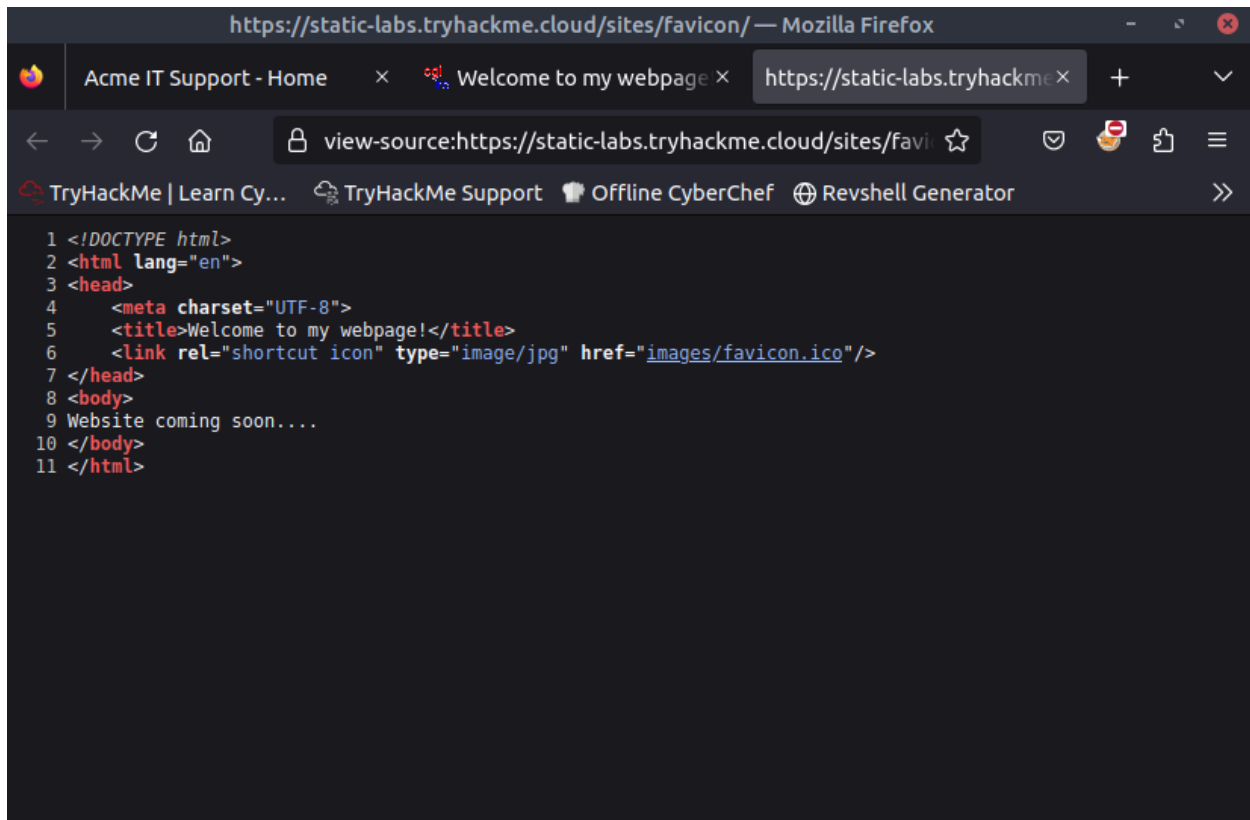
AttackBox'ta firefox'u açın ve <https://static-labs.tryhackme.cloud/sites/favicon/> url'sini girin, burada "Web sitesi yakında..." yazan bir notla birlikte basit bir web sitesi göreceksiniz, sekmelerinize bakarsanız bu sitenin bir favicon kullandığını doğrulayan bir simge göreceksiniz.

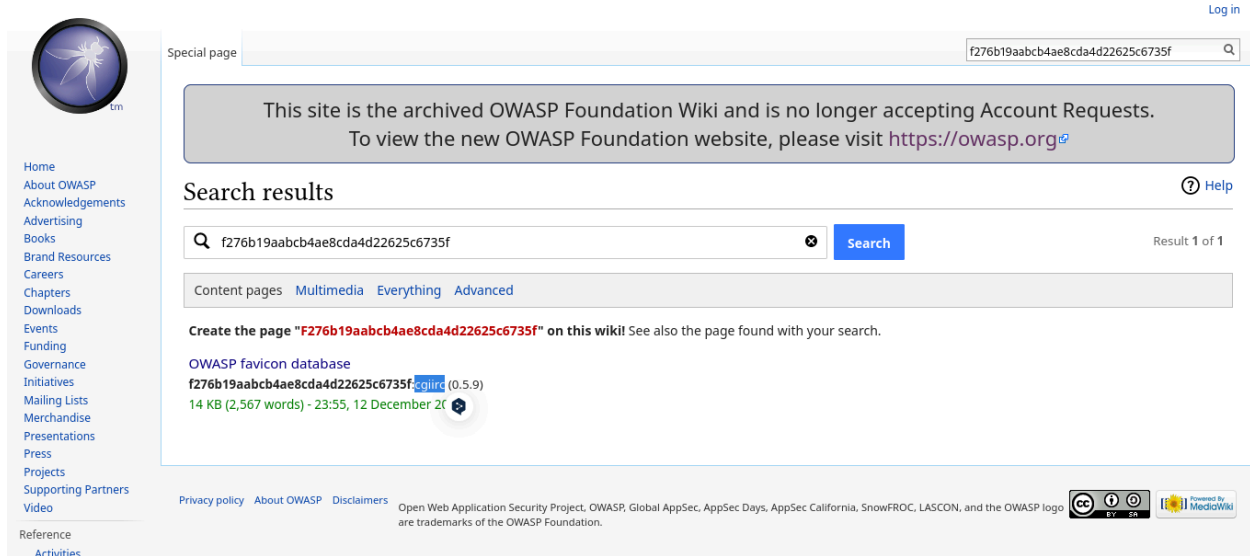
Sayfa kaynağını incelediğinizde altıncı satırın images/favicon.ico dosyasına bir bağlantı içerdiğini göreceksiniz.

AttackBox'ta aşağıdaki komutu çalıştırırsanız, favicon'u indirecek ve daha sonra bakabileceğiniz md5 hash değerini alacaktır.



Website coming soon....





Special page

This site is the archived OWASP Foundation Wiki and is no longer accepting Account Requests.
To view the new OWASP Foundation website, please visit <https://owasp.org>

Search results Help

Result 1 of 1

Content pages [Multimedia](#) [Everything](#) [Advanced](#)

Create the page "**f276b19aabc4ae8cda4d22625c6735f**" on this wiki! See also the page found with your search.

OWASP favicon database
f276b19aabc4ae8cda4d22625c6735f.cgiirc (0.5.9)
14 KB (2,567 words) - 23:55, 12 December 2012

Privacy policy About OWASP Disclaimers Open Web Application Security Project. OWASP, Global AppSec, AppSec Days, AppSec California, SnowFROC, LASCON, and the OWASP logo are trademarks of the OWASP Foundation.

soru⇒ Favicon hangi çerçeveye aitti?

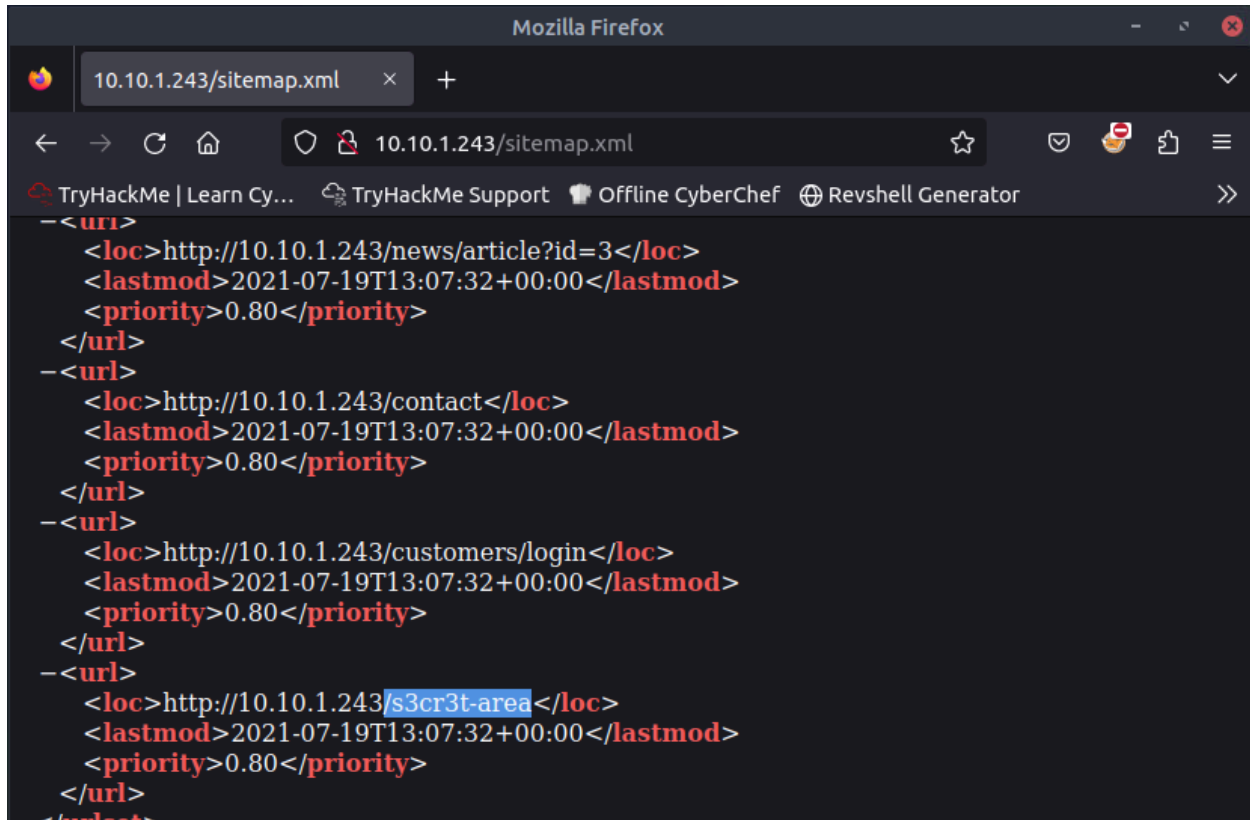
cevap ⇒ **cgirc**

Task 4 Manual Discovery - Sitemap.xml (Manuel Keşif - Sitemap.xml)

Sitemap.xml

Arama motoru tarayıcılarının nelere bakabileceğini kısıtlayan robots.txt dosyasının aksine sitemap.xml dosyası, web sitesi sahibinin bir arama motorunda listelenmesini istediği her dosyanın bir listesini verir. Bunlar bazen web sitesinin gezinmesi biraz daha zor olan alanlarını içerebilir veya hatta mevcut sitenin artık kullanmadığı ancak perde arkasında hala çalışan bazı eski web sayfalarını listeleyebilir.

Henüz keşfetmediğimiz yeni bir içerik olup olmadığını görmek için Acme IT Support web sitesindeki sitemap.xml dosyasına bir göz atın:
<http://10.10.1.243/sitemap.xml> (bunu AttackBox'taki FireFox tarayıcısında açın).



soru ⇒ Sitemap.xml dosyasında bulunabilecek gizli alanın yolu nedir?

cevap ⇒ **/s3cr3t-area**

Task 5 Manual Discovery - HTTP Headers (Manuel Keşif - HTTP Headers)

HTTP Headers

Web sunucusuna istekte bulunduğumuzda, sunucu çeşitli HTTP başlıkları döndürür. Bu başlıklar bazen web sunucusu yazılımı ve muhtemelen kullanılan programlama/komut dosyası dili gibi faydalı bilgiler içerebilir. Aşağıdaki örnekte, web sunucusunun NGINX sürüm 1.18.0 olduğunu ve PHP sürüm 7.4.3 çalıştığını görebiliriz. Bu bilgileri kullanarak, kullanılan yazılımın savunmasız sürümlerini bulabiliriz. Aşağıdaki curl komutunu web sunucusuna karşı çalıştırmayı deneyin; burada -v anahtarı, başlıkların çıktısını alacak olan verbose modunu etkinleştirir (ilginç bir şey olabilir!).

```
root@ip-10-10-101-64: ~  
File Edit View Search Terminal Help  
root@ip-10-10-101-64:~# curl http://10.10.1.243 -v  
* Rebuilt URL to: http://10.10.1.243/  
* Trying 10.10.1.243...  
* TCP_NODELAY set  
* Connected to 10.10.1.243 (10.10.1.243) port 80 (#0)  
> GET / HTTP/1.1  
> Host: 10.10.1.243  
> User-Agent: curl/7.58.0  
> Accept: */*  
>  
< HTTP/1.1 200 OK  
< Server: nginx/1.18.0 (Ubuntu)  
< Date: Fri, 26 Jul 2024 15:01:59 GMT  
< Content-Type: text/html; charset=UTF-8  
< Transfer-Encoding: chunked  
< Connection: keep-alive  
< X-FLAG: THM{HEADER_FLAG}  
<  
<!--  
This page is temporary while we work on the new homepage @ /new-home-beta  
-->  
<!DOCTYPE html>  
<html lang="en">  
<head>
```

soru ⇒ X-FLAG başlığındaki bayrak değeri nedir?

cevap ⇒ **THM{HEADER_FLAG}**

Task 6 Manual Discovery - Framework Stack (Manuel Keşif - Framework Stack)

Framework Stack

Yukarıdaki favicon örneğinden ya da sayfa kaynağında yorumlar, telif hakkı bildirimleri veya krediler gibi ipuçları arayarak bir web sitesinin çerçevesini belirledikten sonra, çerçevenin web sitesini bulabilirsiniz. Buradan, yazılım ve diğer bilgiler hakkında daha fazla bilgi edinebilir ve muhtemelen keşfedebileceğimiz daha fazla içeriğe ulaşabiliriz.

Acme IT Support web sitemizin (<http://10.10.1.243>) sayfa kaynağına baktığınızda, her sayfanın sonunda sayfa yükleme süresiyle ilgili bir yorum ve ayrıca <https://static-labs.tryhackme.cloud/sites/thm-web-framework> olan çerçevenin web sitesine bir bağlantı göreceksiniz. Şimdi bu web sitesine bir göz atalım.

Dokümantasyon sayfasını görüntülemek bize çerçevenin yönetim portalının yolunu verir, bu da Acme IT Support web sitesinde görüntülenirse bize bir bayrak verir.

http://10.10.1.243/ — Mozilla Firefox

view-source:http://10.10.1.243/

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator

```

class="navbar-brand" href="#">Acme IT Support</a>

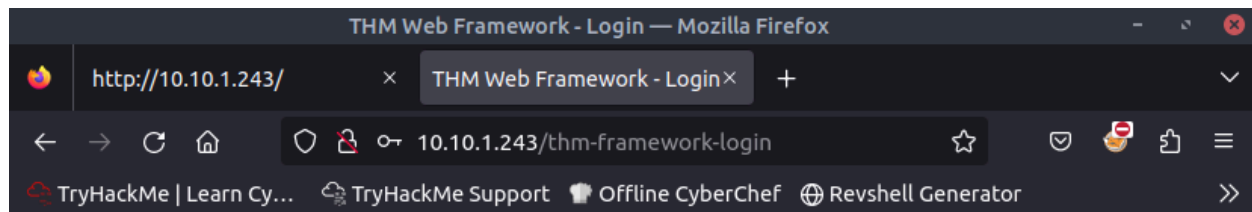
d="navbar" class="collapse navbar-collapse">
l class="nav navbar-nav">
<li class="active"><a href="/">Home</a></li>
<li><a href="/news">News</a></li>
<li><a href="/contact">Contact</a></li>
<li><a href="/customers">Customers</a></li>
</li>
<!--/.nav-collapse -->

ss="container" style="padding-top:60px">
t-center">Acme IT Support</h1>
w">
s="col-md-8 col-md-offset-2 text-center">
rc="/assets/staff.png">
ss="welcome-msg">Our dedicated staff are ready <a href="/secret-page">to</a> assist you with your IT problems.</p>

ts/jquery.min.js"></script>
ts/bootstrap.min.js"></script>
ts/site.js"></script>

0.03172 Seconds using the THM Framework v1.2 ( https://static-labs.tryhackme.cloud/sites/thm-web-framework )

```



THM Web Framework

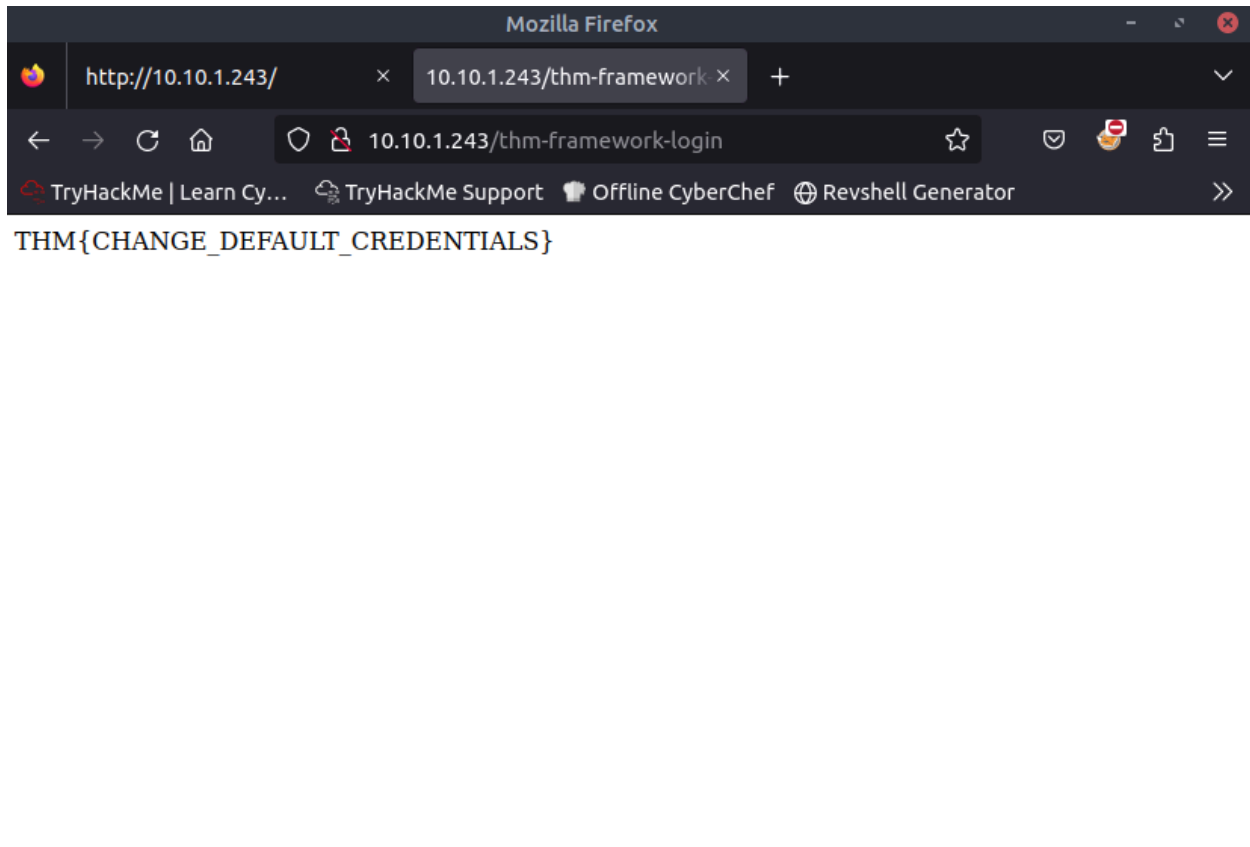
Login

Login

Username:

Password:

Login



soru ⇒ Çerçevenin yönetim portalındaki bayrak nedir?

cevap ⇒ **THM{CHANGE_DEFAULT_CREDENTIALS}**

Task 7 OSINT - Google Hacking / Dorking (OSINT - Google Hacking / Dorking)

Hedef web siteniz hakkında bilgi keşfetmeye yardımcı olabilecek harici kaynaklar da mevcuttur; bu kaynaklar genellikle OSINT veya (Açık Kaynak İstihbaratı) olarak adlandırılır, çünkü bilgi toplayan ücretsiz olarak kullanılabilen araçlardır:

Google Hacking / Dorking

Google hacking / Dorking, Google'ın özel içerik seçmenize olanak tanıyan gelişmiş arama motoru özelliklerini kullanır. Örneğin site: filtresini kullanarak belirli bir alan adından gelen sonuçları seçebilirsiniz, örneğin (site:tryhackme.com) daha sonra bunu belirli arama terimleriyle eşleştirebilirsiniz, örneğin admin kelimesi

(site:tryhackme.com admin) bu daha sonra yalnızca tryhackme.com web sitesinden içeriğinde admin kelimesini içeren sonuçları döndürür. Birden fazla filtreyi de birleştirebilirsiniz. İşte kullanabileceğiniz daha fazla filtrenin bir örneği:

Filtre	Örnek	Açıklama
site	site:tryhackme.com	yalnızca belirtilen web sitesi adresinden sonuçlar döndürür
inurl	inurl:admin	URL'de belirtilen kelimeye sahip sonuçları döndürür
filetype	filetype:pdf	belirli bir dosya uzantısı olan sonuçları döndürür
intitle	intitle:admin	başlıkta belirtilen kelimeyi içeren sonuçları döndürür

Google korsanlığı hakkında daha fazla bilgiyi burada bulabilirsiniz:

https://en.wikipedia.org/wiki/Google_hacking

soru ⇒ Yalnızca belirli bir siteden gelen sonuçları göstermek için hangi Google dork operatörü kullanılabilir?(ipucu= (format xxxx:))

cevap ⇒ **site:**

Task 8 OSINT - Wappalyzer (OSINT - Wappalyzer)

Wappalyzer

Wappalyzer (<https://www.wappalyzer.com/>), bir web sitesinin çerçeveler, İçerik Yönetim Sistemleri (CMS), ödeme işlemcileri ve çok daha fazlası gibi hangi teknolojileri kullandığını belirlemeye yardımcı olan ve hatta sürüm numaralarını da bulabilen çevrimiçi bir araç ve tarayıcı uzantısıdır.

soru ⇒ Bir web sitesinin hangi teknolojileri kullandığını belirlemek için hangi çevrimiçi araç kullanılabilir?

cevap ⇒ **Wappalyzer**

Task 9 OSINT - Wayback Machine (OSINT - Wayback Machine)

Wayback Machine

Wayback Machine (<https://archive.org/web/>), 90'ların sonlarına kadar uzanan web sitelerinin tarihsel bir arşividir. Bir alan adını arayabilirsiniz ve hizmet size web sayfasını kazıyıp içeriğini kaydettiği tüm zamanları gösterecektir. Bu hizmet, mevcut web sitesinde hala aktif olabilecek eski sayfaların ortaya çıkarılmasına yardımcı olabilir.

soru ⇒ Wayback Machine için web sitesi adresi nedir?

cevap ⇒ <https://archive.org/web/>

Task 10 OSINT - GitHub (OSINT - GitHub)

GitHub

GitHub'ı anlamak için öncelikle Git'i anlamamız gerekir. Git, bir projedeki dosyalarda yapılan değişiklikleri izleyen bir sürüm kontrol sistemidir. Bir ekipte çalışmak daha kolaydır çünkü her ekip üyesinin neyi düzenlediğini ve dosyalarda hangi değişiklikleri yaptığını görebilirsiniz. Kullanıcılar değişikliklerini yapmayı bitirdiklerinde, bunları bir mesajla taahhüt ederler ve ardından diğer kullanıcıların bu değişiklikleri yerel makinelerine çekmeleri için merkezi bir konuma (depo) geri gönderirler. GitHub, Git'in internet üzerinde barındırılan bir sürümüdür. Depolar genel ya da özel olarak ayarlanabilir ve çeşitli erişim kontrollerine sahip olabilir. Hedefinize ait depoları bulmak için GitHub'ın arama özelliğini kullanarak şirket adlarını veya web sitesi adlarını arayabilirsiniz. Bulduğunda, kaynak koduna, şifrelere veya henüz bulamadığınız diğer içeriklere erişebilirsiniz.

soru ⇒ Git nedir?

cevap⇒ **version control system**

Task 11 OSINT - S3 Buckets (OSINT - S3 Buckets)

S3 Buckets

S3 Kovaları, Amazon AWS tarafından sağlanan ve insanların dosyaları ve hatta statik web sitesi içeriğini HTTP ve HTTPS üzerinden erişilebilen buluta kaydetmelerine olanak tanıyan bir depolama hizmetidir. Dosyaların sahibi, dosyaları herkese açık, özel ve hatta yazılabilir hale getirmek için erişim izinlerini ayarlayabilir. Bazen bu erişim izinleri yanlış ayarlanır ve yanlışlıkla herkese açık olmaması gereken dosyalara erişime izin verir. S3 kovalarının biçimi `http(s)://{name}.s3.amazonaws.com` şeklindedir ve burada {name} tryhackme-assets.s3.amazonaws.com gibi sahibi tarafından belirlenir. S3 kovaları, web sitesinin sayfa kaynağındaki URL'leri, GitHub depolarını bulmak veya hatta işlemi otomatikleştirmek gibi birçok yolla keşfedilebilir. Yaygın bir otomasyon yöntemi, şirket adını ve ardından {name}-assets, {name}-www, {name}-public, {name}-private gibi yaygın terimleri kullanmaktır.

soru ⇒ Amazon S3 kovaları hangi URL biçiminde sonlanır?(ipucu=Cevabınızın . (nokta) ile başladığından emin olun)

cevap ⇒ **.s3.amazonaws.com**

Task 12 Automated Discovery (Otomatik Keşif)

Otomatik Keşif Nedir?

Otomatik keşif, içeriği keşfetmek için manuel olarak yapmak yerine araçları kullanma sürecidir. Bu süreç genellikle bir web sunucusuna yapılan yüzlerce, binlerce hatta milyonlarca isteği içerdiğinden otomatiktir. Bu istekler, bir web sitesinde bir dosya veya dizinin var olup olmadığını kontrol eder ve bize daha önce var olduğunu bilmediğimiz kaynaklara erişim sağlar. Bu işlem wordlist adı verilen bir kaynak kullanılarak mümkün kılınmıştır.

Kelime listeleri nedir?

Kelime listeleri, yaygın olarak kullanılan kelimelerin uzun bir listesini içeren metin dosyalarıdır; birçok farklı kullanım durumunu kapsayabilirler. Örneğin, bir parola kelime listesi en sık kullanılan parolaları içerir, oysa bizim durumumuzda içerik arıyoruz, bu nedenle en sık kullanılan dizin ve dosya adlarını içeren bir listeye ihtiyacımız var. THM AttackBox'a önceden yüklenmiş olan kelime listeleri için mükemmel bir kaynak, Daniel Miessler'in küratörlüğünü yaptığı <https://github.com/danielmiessler/SecLists> adresidir.

Otomasyon Araçları

Her birinin kendine has özellikleri ve kusurları olan birçok farklı içerik keşif aracı mevcut olsa da, biz saldırı kutumuzda önceden kurulu olan üç tanesini ele alacağız: ffuf, dirb ve gobuster.

AttackBox'ta Acme IT Support web sitesini hedefleyerek aşağıdaki üç komutu çalıştırın ve ne gibi sonuçlar elde ettiğinizi görün.

ffuf kullanıyorum:

```
user@machine$ ffuf -w /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt -u http://MACHINE_IP/FUZZ
```

dirb kullanarak:

```
user@machine$ dirb http://MACHINE_IP/ /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt
```

Gobuster'ı kullanma:

```
user@machine$ gobuster dir --url http://MACHINE_IP/ -w /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt
```

Yukarıdaki komutlardan elde edilen sonuçları kullanarak lütfen aşağıdaki soruları yanıtlayın:

```
root@ip-10-10-131-135: ~
File Edit View Search Terminal Help
root@ip-10-10-131-135:~# gobuster dir -u http://10.10.43.81 -w /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.43.81
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Timeout:      10s
=====
2024/07/27 08:01:14 Starting gobuster
=====
/assets (Status: 301)
/contact (Status: 200)
/customers (Status: 302)
/development.log (Status: 200)
/monthly (Status: 200)
/news (Status: 200)
/private (Status: 301)
/robots.txt (Status: 200)
/sitemap.xml (Status: 200)
=====
2024/07/27 08:01:16 Finished
=====
root@ip-10-10-131-135:~#
```

soru ⇒ Keşfedilen "/mo...." ile başlayan dizinin adı nedir(ipucu⇒ AttackBox üzerinde bir terminal açın ve yukarıda gösterilen komutları çalıştırın.)?

cevap ⇒ **/monthly**

```
root@ip-10-10-131-135: ~
File Edit View Search Terminal Help
root@ip-10-10-131-135:~# gobuster dir -u http://10.10.43.81 -w /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.43.81
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Timeout:      10s
=====
2024/07/27 08:01:14 Starting gobuster
=====
/assets (Status: 301)
/contact (Status: 200)
/customers (Status: 302)
/development.log (Status: 200)
/monthly (Status: 200)
/news (Status: 200)
/private (Status: 301)
/robots.txt (Status: 200)
/sitemap.xml (Status: 200)
=====
2024/07/27 08:01:16 Finished
=====
root@ip-10-10-131-135:~#
```

soru⇒ Keşfedilen günlük dosyasının adı nedir?

cevap ⇒ **/development.log**