

Walking An Application

Task 1 Walking An Application (Bir Uygulamayı Yürütmek)

Bu odada, yalnızca tarayıcınızdaki yerleşik araçları kullanarak bir web uygulamasını güvenlik sorunları açısından manuel olarak nasıl inceleyeceğinizi öğreneceksiniz. Otomatik güvenlik araçları ve komut dosyaları çoğu zaman birçok potansiyel güvenlik açığını ve faydalı bilgiyi gözden kaçıracaktır.

İşte bu oda boyunca kullanacağınız dahili tarayıcı araçlarının kısa bir dökümü:

Kaynağı Görüntüle - Bir web sitesinin insan tarafından okunabilir kaynak kodunu görüntülemek için tarayıcınızı kullanın.

Denetçi- Sayfa öğelerini nasıl inceleyeceğinizi ve genellikle engellenen içeriği görüntülemek için nasıl değişiklik yapacağınızı öğrenin.

Hata Ayıklayıcı - Bir sayfanın JavaScript akışını inceleyin ve kontrol edin

Ağ - Bir sayfanın yaptığı tüm ağ isteklerini görün.

Bu görevde sanal makineyi başlatın, 2 dakika bekleyin ve aşağıdaki URL'yi ziyaret edin: https://LAB_WEB_URL.p.thmlabs.com (bu URL, makineyi başlattığınız andan itibaren 2 dakika içinde güncellenecektir)

Sanal makineyi dağıttığımı ve web sitesini açtığımı onaylıyorum.

cevap gerekmemektedir.

Task 2 Exploring The Website (Web Sitesini Keşfetme)

Bir sızma test uzmanı olarak, bir web sitesini veya web uygulamasını incelerken rolünüz, potansiyel olarak savunmasız olabilecek özellikleri keşfetmek ve bunların olup olmadığını değerlendirmek için bunlardan yararlanmaya çalışmaktır. Bu özellikler genellikle web sitesinin kullanıcı ile etkileşim gerektiren kısımlarıdır.

Web sitesinin etkileşimli bölümlerini bulmak, bir giriş formunu tespit etmekten web sitesinin JavaScript'ini manuel olarak incelemeye kadar kolay olabilir. Başlamak için mükemmel bir yer, tarayıcınızla web sitesini keşfetmek ve her biri için bir özetle birlikte ayrı sayfaları/alanları/özellikleri not etmektir.

Acme IT Support web sitesi için örnek bir site incelemesi aşağıdaki gibi görünebilir:

| Feature (Özellik) | URL (url) | Summary (Özet) |
|-------------------------|-----------------------|--|
| Home Page | / | Bu sayfa, Acme IT Support'un çalışanlarının bir şirket fotoğrafı ile ne yaptığının bir özetini içerir. |
| Latest News | /news | Bu sayfa, şirket tarafından yakın zamanda yayınlanan haber makalelerinin bir listesini içerir ve her haber makalesinin bir kimlik numarası olan bir bağlantısı vardır, yani /news/article?id=1 |
| News Article | /news/article?id=1 | Bireysel haber makalesini görüntüler. Bazı makaleler engellenmiş ve yalnızca premium müşteriler için ayrılmış gibi görünüyor. |
| Contact Page | /contact | Bu sayfa, müşterilerin şirketle iletişime geçmesi için bir form içerir. İsim, e-posta ve mesaj giriş alanları ve bir gönder düğmesi içerir. |
| Customers | /customers | Bu bağlantı /customers/login adresine yönlendirir. |
| Customer Login | /customers/login | Bu sayfa, kullanıcı adı ve şifre alanlarına sahip bir oturum açma formu içerir. |
| Customer Signup | /customers/signup | Bu sayfa, kullanıcı adı, e-posta, şifre ve şifre onay giriş alanlarından oluşan bir kullanıcı kayıt formu içerir. |
| Customer Reset Password | /customers/reset | E-posta adresi giriş alanına sahip parola sıfırlama formu. |
| Customer Dashboard | /customers | Bu sayfa, kullanıcının BT destek şirketine gönderdiği biletlerin bir listesini ve bir "Bilet Oluştur" düğmesini içerir. |
| Create Ticket | /customers/ticket/new | Bu sayfa, BT sorununu girmek için bir metin kutusu ve bir BT destek bileti oluşturmak için bir |

| | | |
|------------------|--------------------|---|
| | | dosya yükleme seçeneği içeren bir form içerir. |
| Customer Account | /customers/account | Bu sayfa kullanıcının kullanıcı adını, e-postasını ve şifresini düzenlemesine olanak tanır. |
| Customer Logout | /customers/logout | Bu bağlantı, kullanıcının müşteri alanından çıkışını sağlar. |

Bir sonraki görevde keşfettiğimiz bazı sayfalara daha derinlemesine bakmaya başlayacağız.

Yukarıdakileri okuyun.

cevap gerekmemektedir.

Task 3 Viewing The Page Source (Sayfa Kaynağını Görüntüleme)

Sayfa kaynağı, her istek yaptığımızda web sunucusundan tarayıcımıza/istemcimize döndürülen insan tarafından okunabilir koddur.

Dönen kod HTML (HyperText Markup Language), CSS (Cascading Style Sheets) ve JavaScript'ten oluşur ve tarayıcımıza hangi içeriğin görüntüleneceğini, nasıl gösterileceğini söyler ve JavaScript ile bir etkileşim unsuru ekler.

Bizim amaçlarımız doğrultusunda, sayfa kaynağını görüntülemek web uygulaması hakkında daha fazla bilgi edinmemize yardımcı olabilir.

Sayfa Kaynağını nasıl görüntüleyebilirim?

Bir web sitesini görüntülerken, sayfaya sağ tıklayabilirsiniz ve menüde Sayfa Kaynağını Görüntüle yazan bir seçenek görürsünüz.

Çoğu tarayıcı URL'nin önüne view-source: koymayı destekler, örneğin
viewsource:https://www.google.com/

Tarayıcınızın menüsünde, sayfa kaynağını görüntülemek için bir seçenek bulacaksınız.

Bu seçenek bazen geliştirici araçları veya daha fazla araç gibi alt menülerde olabilir.

Biraz Sayfa Kaynağı görüntüleyelim!

Acme IT Support web sitesinin ana sayfasının sayfa kaynağını görüntülemeyi deneyin. Ne yazık ki, burada görebileceğiniz her şeyi açıklamak bu odanın kapsamı dışındadır ve tam olarak anlamak için web sitesi tasarımı / geliştirme kurslarına bakmanız gerekecektir. Yapabileceğimiz şey, bizim için önemli olan bilgi parçalarını seçmektir.

Sayfanın üst kısmında `<!-- ile başlayan ve -->` ile biten bazı kodlar göreceksiniz, bunlar yorumlardır. Yorumlar, genellikle koddaki bir şeyi diğer programcılara açıklamak veya hatta kendileri için notlar / hatırlatmalar yapmak için web sitesi geliştiricisi tarafından bırakılan mesajlardır. Bu yorumlar gerçek web sayfasında görüntülenmez. Bu yorum, yeni bir web sayfası geliştirilirken ana sayfanın nasıl geçici olduğunu açıklamaktadır. İlk bayrağınızı almak için yorumdaki web sayfasını görüntüleyin.

HTML'de farklı sayfalara bağlantılar anchor etiketlerinde yazılır (bunlar `<a` ile başlayan HTML öğeleridir) ve yönlendirileceğiniz bağlantı href niteliğinde saklanır.

Sayfa kaynağının daha aşağısına bakarsanız, "secr" ile başlayan bir sayfaya gizli bir bağlantı vardır, başka bir bayrak almak için bu bağlantıyı görüntüleyin. Açıkçası gerçek dünyada bir bayrak almazsınız, ancak işletme tarafından şirket / personel / müşteri bilgilerini saklamak için kullanılan bazı özel alanları keşfedebilirsiniz.

CSS, JavaScript ve Görüntüler gibi harici dosyalar HTML kodu kullanılarak dahil edilebilir. Bu örnekte, bu dosyaların hepsinin aynı dizinde depolandığını fark edeceksiniz. Bu dizini web tarayıcınızda görüntülerseniz, bir yapılandırma hatası oluşur. Görüntülenmesi gereken ya boş bir sayfa ya da dizine erişiminiz olmadığını belirten bir hata içeren 403 Forbidden sayfasıdır. Bunun yerine, dizin listeleme özelliği etkinleştirilmiştir ve bu da aslında dizindeki her dosyayı listeler. Bazen bu bir sorun teşkil etmez ve dizindeki tüm dosyalar herkes tarafından güvenli bir şekilde görüntülenebilir, ancak bazı durumlarda yedekleme dosyaları, kaynak kodu veya diğer gizli bilgiler burada saklanıyor olabilir. Bu durumda, flag.txt dosyasında bir bayrak alırız.

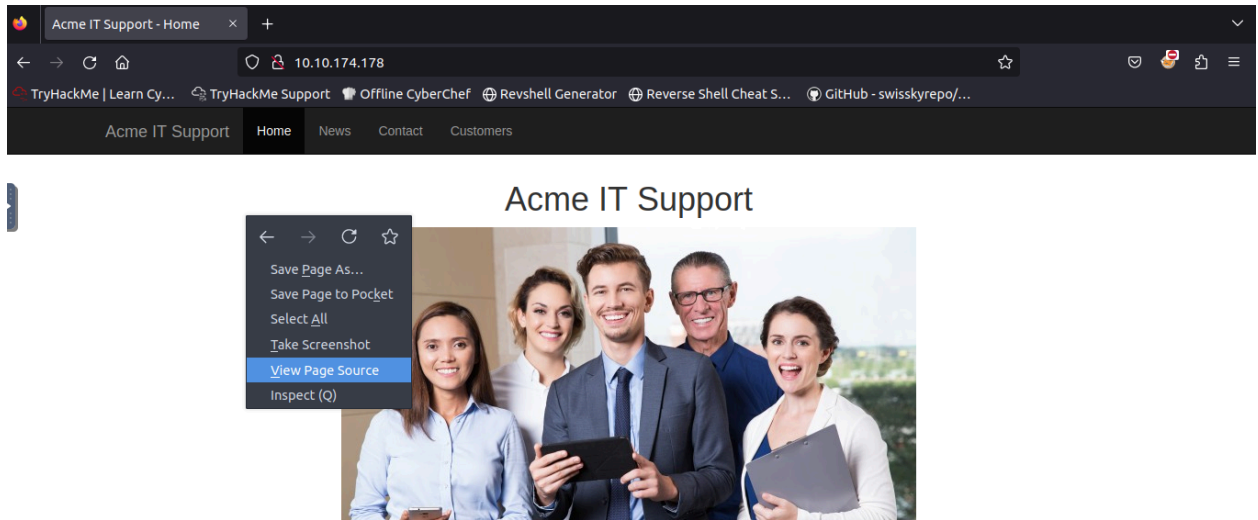
Bugünlerde birçok web sitesi sıfırdan yapılmıyor ve çerçeve adı verilen bir yapı kullanıyor. Bir çerçeve, bir geliştiricinin bloglar, kullanıcı yönetimi, form işleme ve çok daha fazlası gibi bir web sitesinin ihtiyaç duyacağı ortak özellikleri kolayca dahil etmesine olanak tanıyan ve geliştiricilere saatler veya günler kazandıran önceden hazırlanmış bir kod koleksiyonudur.

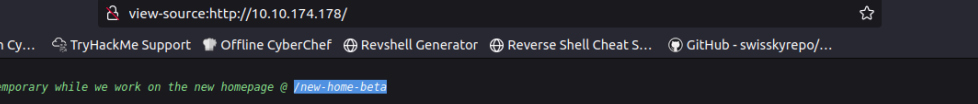
Sayfa kaynağını görüntülemek genellikle bize bir framework kullanılıp kullanılmadığına ve kullanılıyorsa hangi framework ve hatta hangi sürüm olduğuna dair ipuçları verebilir. Framework'te herkese açık güvenlik açıkları olabileceğinden ve web sitesi en güncel sürümü kullanmıyor olabileceğinden, framework'ü ve sürümü bilmek güçlü bir bulgu olabilir. Sayfanın altında, kullanılan çerçeve ve sürüm hakkında bir yorum ve çerçevenin web sitesine bir bağlantı bulacaksınız. Çerçevenin web sitesini görüntülediğinizde, web sitemizin aslında güncel olmadığını göreceksiniz. Güncelleme bildirimini okuyun ve bulduğunuz bilgileri başka bir bayrak keşfetmek için kullanın.

soru⇒

HTML yorumundaki bayrak nedir? (İPUCU⇒ Yorumda belirtilen bağlantıya gittiğinizden emin olun.)

⇒ `THM{HTML_COMMENTS_ARE_DANGEROUS}`





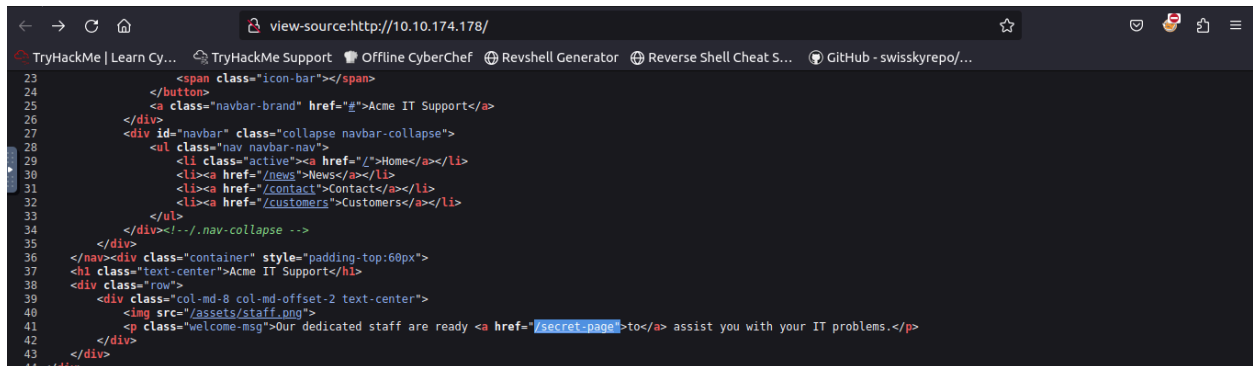
The screenshot shows a web browser window with the address bar displaying 'http://10.10.174.178/'. The page title is 'Acme IT Support - Home'. The browser's developer tools are open, showing the source code of the webpage. The code is HTML, and it includes a navigation bar with a toggle button and a list of links. The toggle button is labeled 'Acme IT Support - Home' and has a 'collapse' attribute. The navigation bar is styled with Bootstrap classes. The source code is as follows:

```
1 <!--
2 This page is temporary while we work on the new homepage @ tnew-home-beta
3 -->
4 <!DOCTYPE html>
5 <html lang="en">
6 <head>
7 <title>Acme IT Support - Home</title>
8 <meta charset="utf-8">
9 <meta http-equiv="X-UA-Compatible" content="IE=edge">
10 <meta name="viewport" content="width=device-width, initial-scale=1">
11 <link rel="stylesheet" href="https://pro.fontawesome.com/releases/v5.12.0/css/all.css" integrity="sha384-ek0ryXpBeCpWQMwSWVvQ0+1vRstPjQ54shlyR8HzQgig1v5fas6Yg0qLkZ" crossorigin="anonymous">
12 <link rel="stylesheet" href="/assets/bootstrap.min.css">
13 <link rel="stylesheet" href="/assets/style.css">
14 </head>
15 <body>
16 <nav class="navbar navbar-inverse navbar-fixed-top">
17 <div class="container">
18 <div class="navbar-header">
19 <button type="button" class="navbar-toggle collapsed" data-toggle="collapse" data-target="#navbar" aria-expanded="false" aria-controls="navbar">
20 <span class="sr-only">Toggle navigation</span>
21 <span class="icon-bar"></span>
22 <span class="icon-bar"></span>
23 <span class="icon-bar"></span>
24 </button>
25 <div class="navbar-brand" href="#">Acme IT Support</div>
26 </div>
27 <div id="navbar" class="collapse navbar-collapse">
28 <ul class="nav navbar-nav">
29 <li class="active"><a href="/">Home</a></li>
```

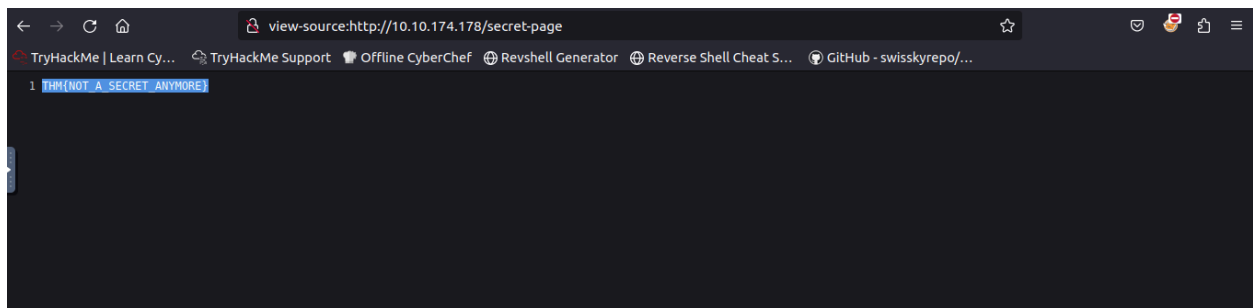
.soru

Gizli bağlantıdaki bayrak nedir?

⇒ THM{NOT_A_SECRET_ANYMORE}



```
23 <span class="icon-bar"></span>
24 </button>
25 <a class="navbar-brand" href="#">Acme IT Support</a>
26 </div>
27 <div id="navbar" class="collapse navbar-collapse">
28 <ul class="nav navbar-nav">
29 <li class="active"><a href="/">Home</a></li>
30 <li><a href="/news">News</a></li>
31 <li><a href="/contact">Contact</a></li>
32 <li><a href="/customers">Customers</a></li>
33 </ul>
34 </div><!--/.nav-collapse -->
35 </div>
36 </nav><div class="container" style="padding-top:60px">
37 <h1 class="text-center">Acme IT Support</h1>
38 <div class="row">
39 <div class="col-md-8 col-md-offset-2 text-center">
40 
41 <p class="welcome-msg">Our dedicated staff are ready <a href="/secret-page">to</a> assist you with your IT problems.</p>
42 </div>
43 </div>
44 </div>
```

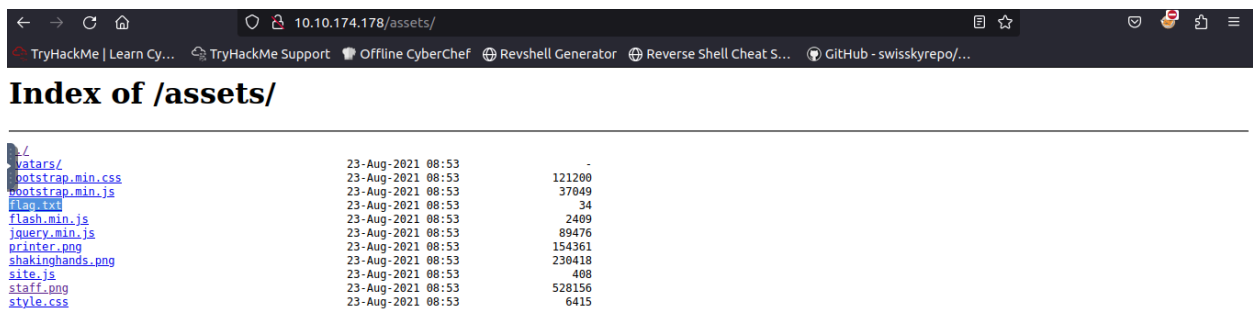
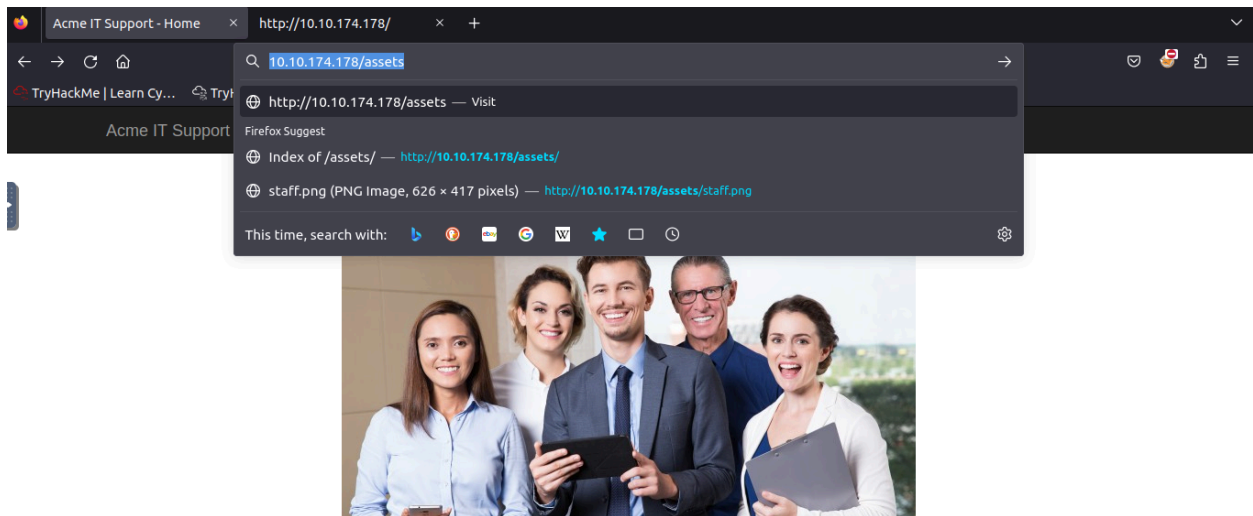


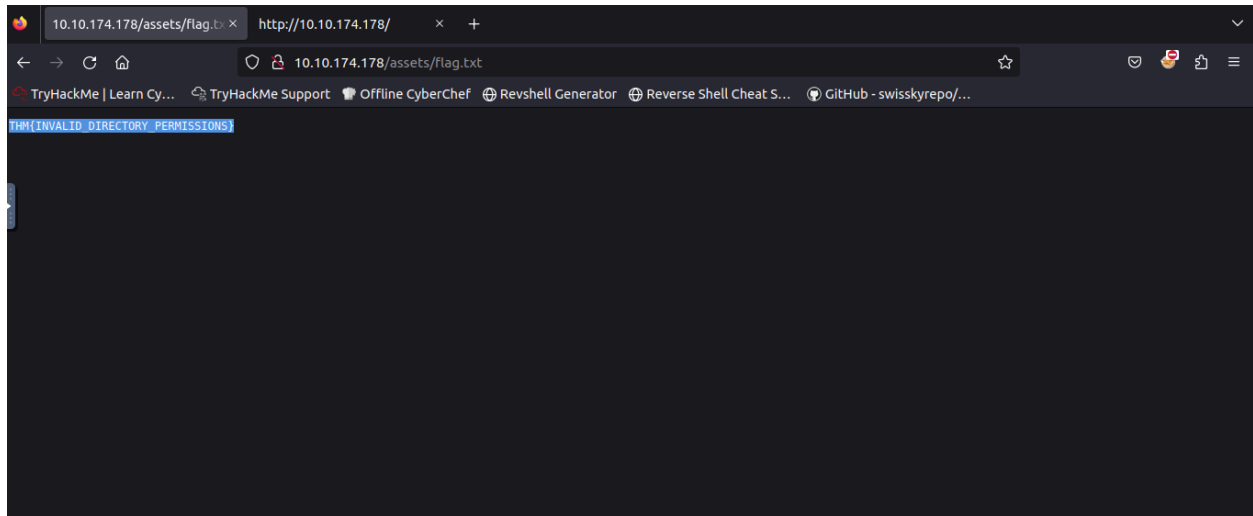
```
1 THM{NOT_A_SECRET_ANYMORE}
```

.soru

Dizin listeleme bayrağı nedir?

⇒ THM{INVALID_DIRECTORY_PERMISSIONS}

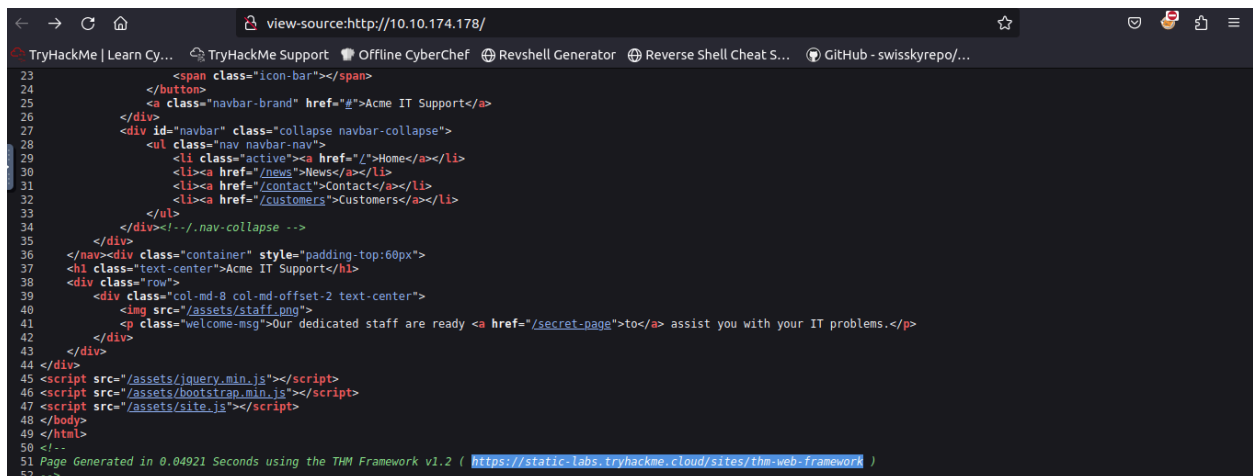


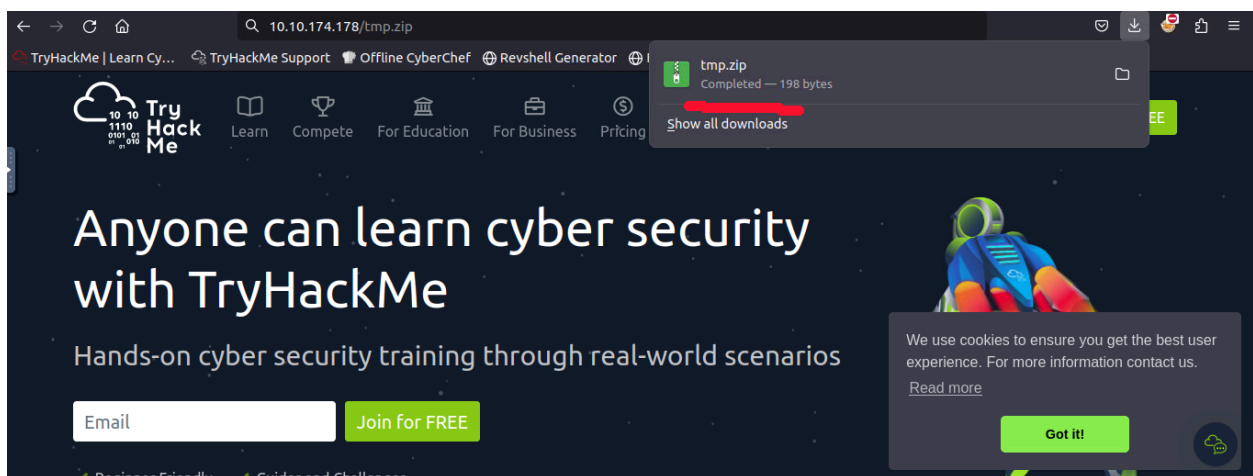
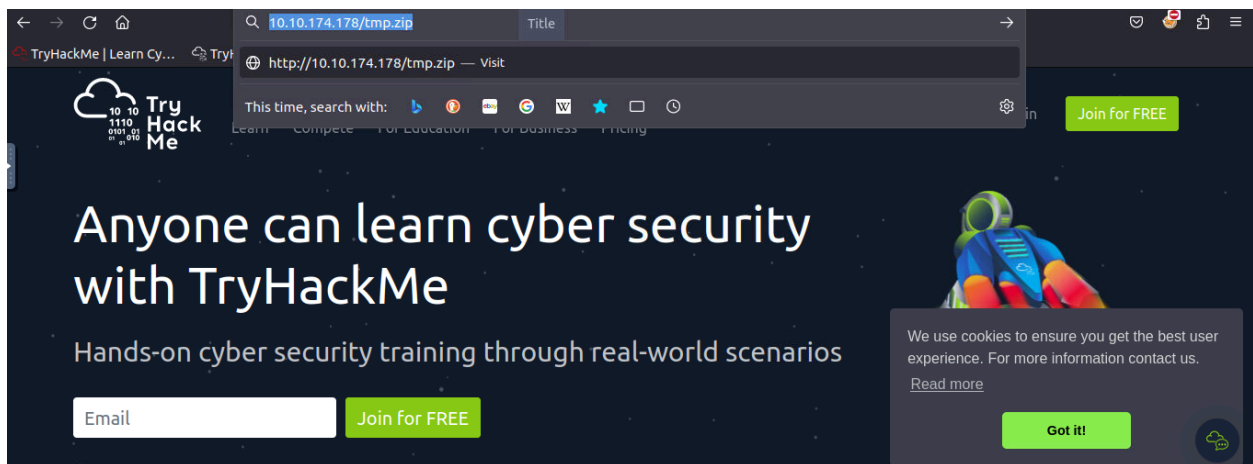
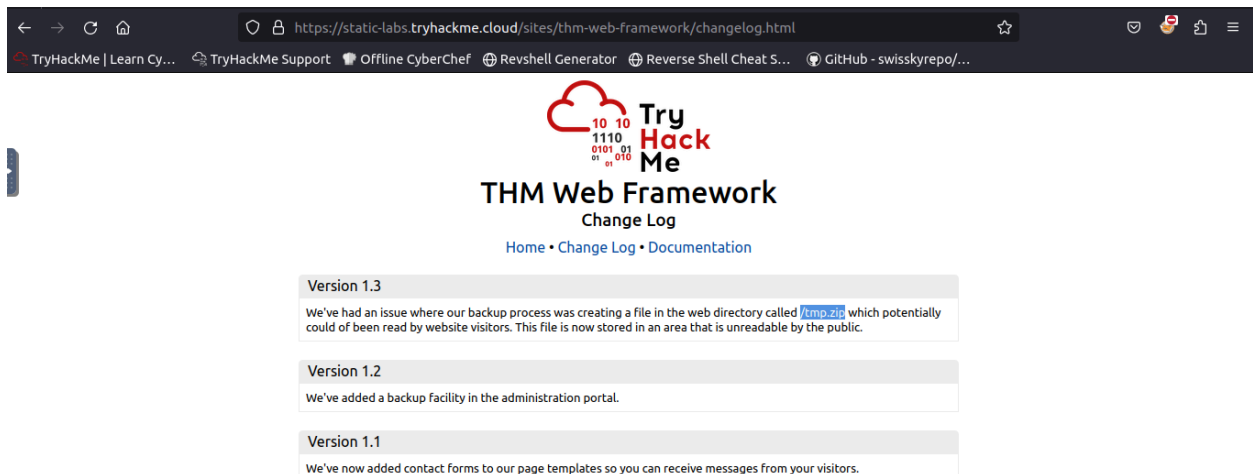


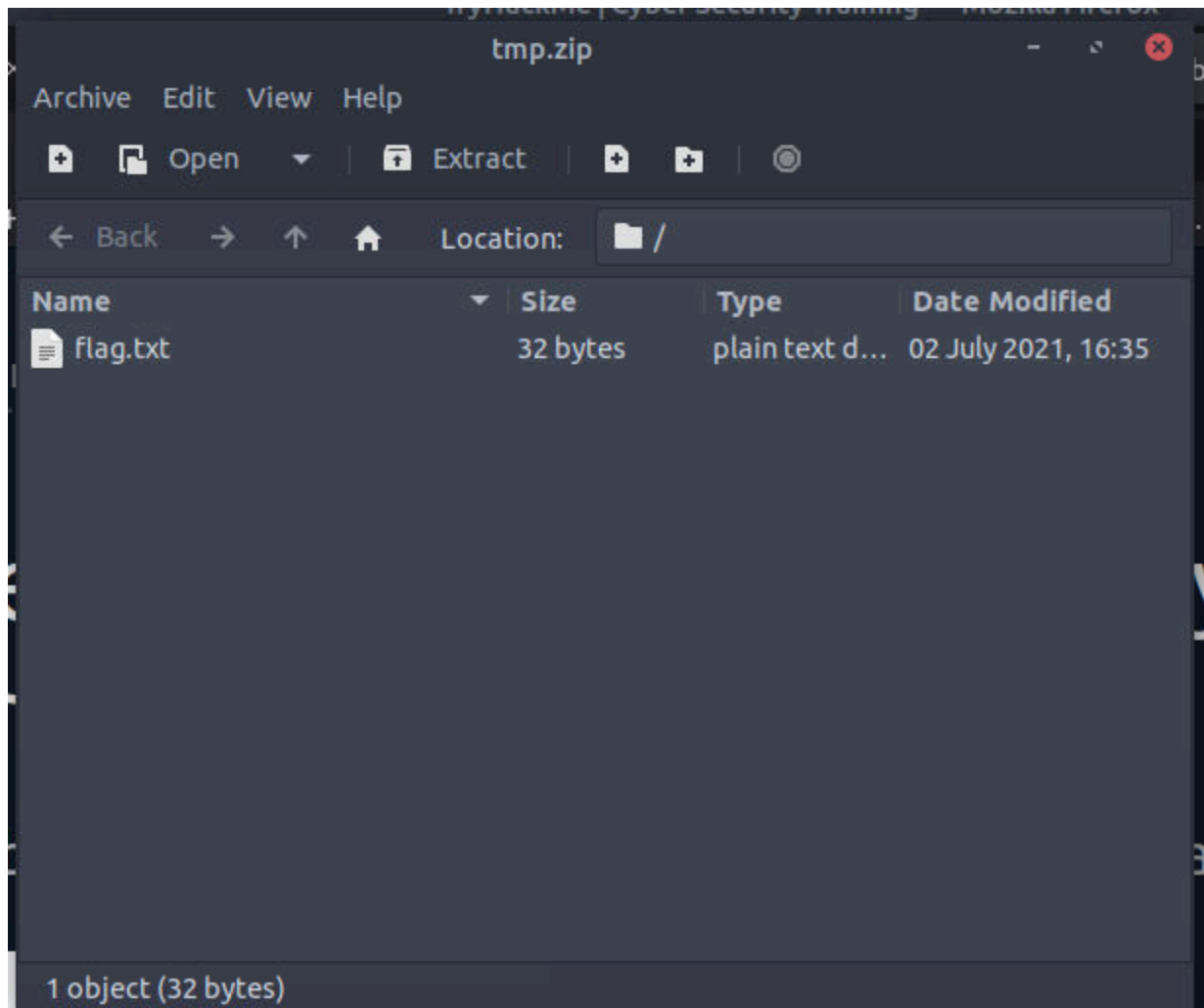
.soru

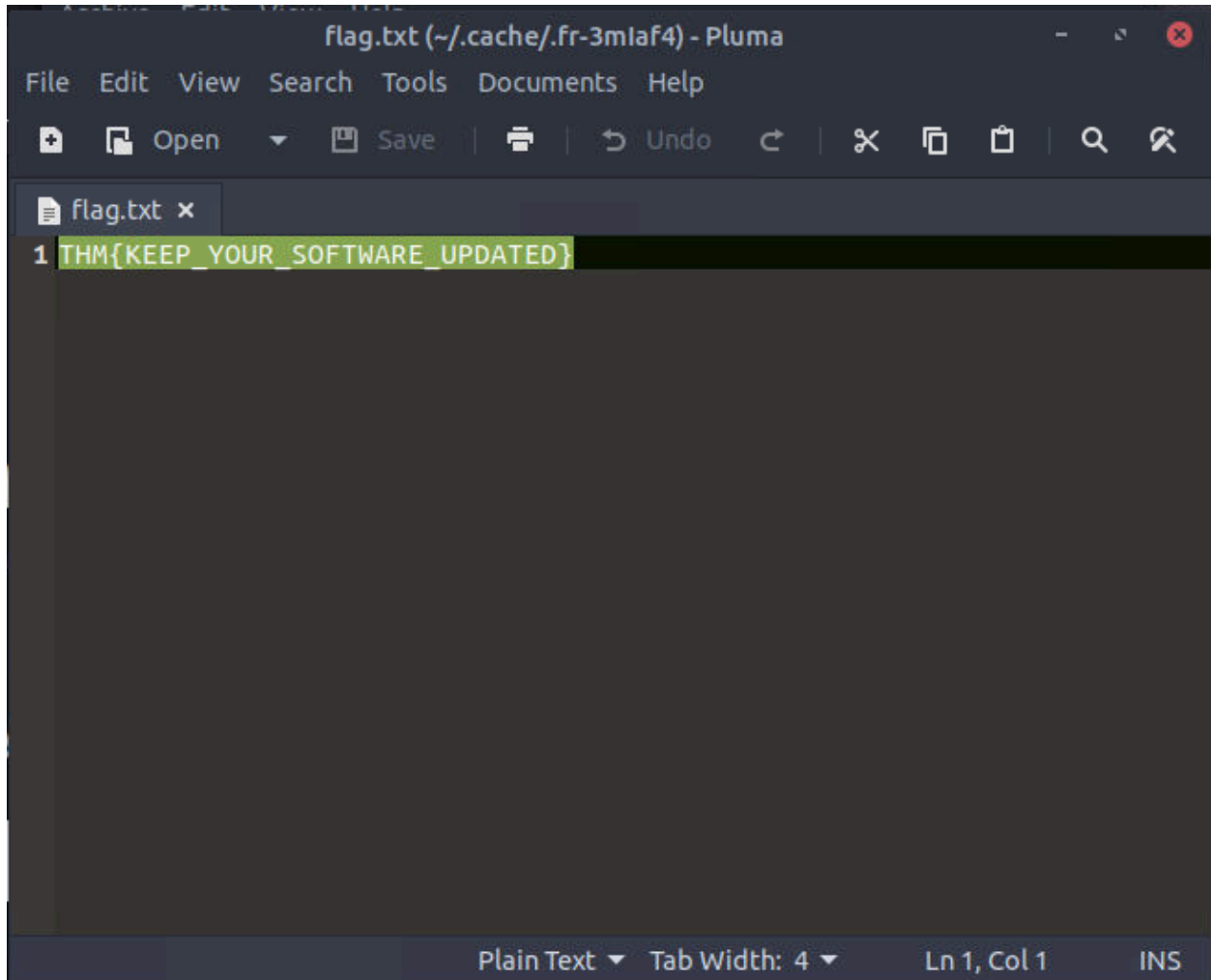
Çerçeve bayrağı nedir? (İPUCU⇒ https://LAB_WEB_URL.p.thmlabs.com/<file.zip>
- Dosyayı çerçeve değişiklik günlüğü sayfasında bulun.)

⇒ THM{KEEP_YOUR_SOFTWARE_UPDATED}









Task 4 Developer Tools - Inspector (Geliştirici Araçları - Inspector)

Geliştirici Araçları

Her modern tarayıcı geliştirici araçları içerir; bunlar web geliştiricilerinin web uygulamalarında hata ayıklamasına yardımcı olmak için kullanılan ve neler olup bittiğini görmek için bir web sitesinin kaputunun altına göz atmanızı sağlayan bir araç kitidir. Bir pentester olarak, web uygulamasını çok daha iyi anlamamızı sağlamak için bu araçlardan yararlanabiliriz. Özellikle geliştirici araç kitinin üç özelliğine odaklanıyoruz: Inspector, Debugger ve Network.

Geliştirici Araçlarını Açma

Geliştirici araçlarına erişmenin yolu her tarayıcı için farklıdır. Nasıl erişeceğinizden emin değilseniz, tarayıcınız için araçlara nasıl erişeceğinize dair talimatları almak için bu görevin sağ üst köşesindeki "Siteyi Görüntüle" düğmesine tıklayın.

Müfettiş

Sayfa kaynağı her zaman bir web sayfasında gösterilenleri temsil etmez; bunun nedeni CSS, JavaScript ve kullanıcı etkileşiminin sayfanın içeriğini ve stilini değiştirebilmesidir, bu da tarayıcı penceresinde tam o anda neyin görüntülendiğini görmenin bir yoluna ihtiyacımız olduğu

anlamına gelir. Element inspector bize web sitesinde o anda ne olduğunun canlı bir temsilini sağlayarak bu konuda bize yardımcı olur.

Bu canlı görünümü görüntülemenin yanı sıra, sayfa öğelerini düzenleyebilir ve bunlarla etkileşime girebiliriz; bu da web geliştiricilerinin sorunlarda hata ayıklamasına yardımcı olur.

Acme IT Support web sitesinde haberler bölümüne tıklayın, burada üç haber makalesi göreceksiniz.

İlk iki makale okunabilir durumda, ancak üçüncüsü içeriğin üzerinde makaleyi görüntülemek için premium müşteri olmanız gerektiğini belirten kayan bir bildirimle engellenmiş. Sayfa içeriğini engelleyen bu kayan kutular, ödeme yapana kadar görmek istediğiniz içeriğin önüne metaforik bir duvar ördüğü için genellikle ödeme duvarları olarak adlandırılır.

Premium bildirimine (ödeme duvarı) sağ tıkladığınızda, tarayıcınıza veya tercihlerinize bağlı olarak alt veya sağ tarafta geliştirici araçlarını açan menüden İncele seçeneğini seçebilmeniz gerekir. Şimdi web sitesini oluşturan öğeleri/HTML'yi göreceksiniz (aşağıdaki ekran görüntülerine benzer şekilde).

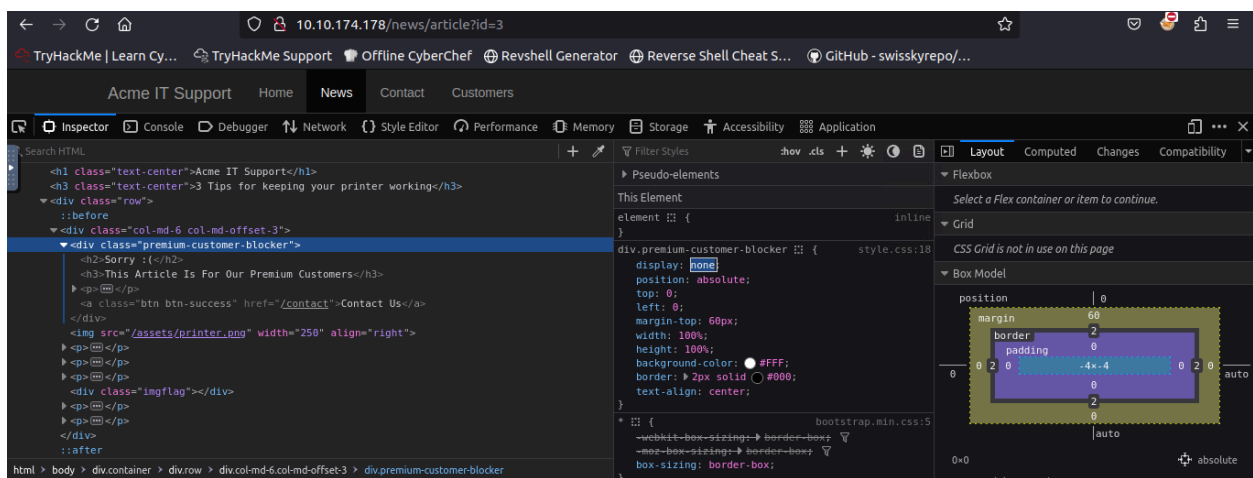
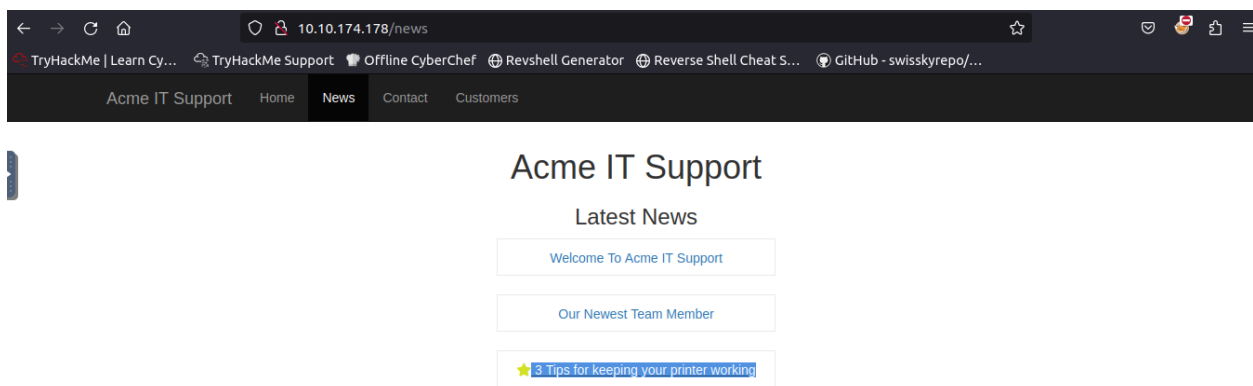
premium-customer-blocker sınıfına sahip DIV öğesini bulun ve üzerine tıklayın. Stiller kutusunda, margin-top: 60px ve text-align: center gibi bu öğe için geçerli olan tüm CSS stillerini göreceksiniz. Bizim ilgilendiğimiz stil display: block'tur. Eğer block kelimesine tıklarsanız, kendi seçtiğiniz bir değeri yazabilirsiniz. none yazmayı deneyin, bu kutunun kaybolmasını sağlayacak ve altındaki içeriği ve bir bayrağı ortaya çıkaracaktır. Eğer öğenin bir görüntüleme alanı yoksa, son stilin altına tıklayabilir ve kendi stilinizi ekleyebilirsiniz. Eleman denetçisi ile oynadığınızda, içerik de dahil olmak üzere web sitesindeki herhangi bir bilgiyi değiştirebileceğinizi göreceksiniz. Bunun yalnızca tarayıcı pencerenizde

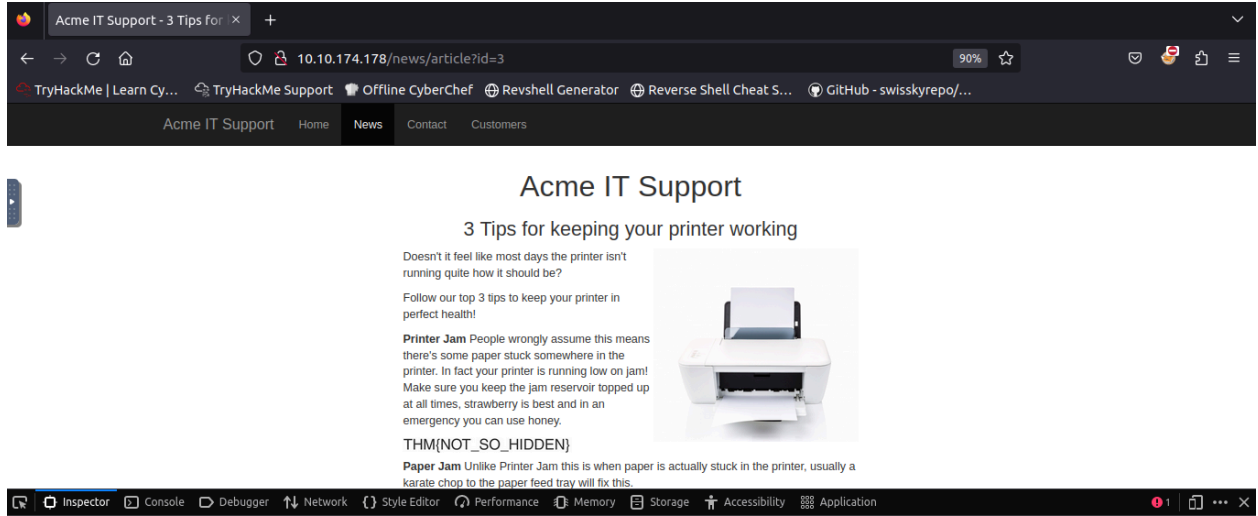
düzenlendiğini ve yenileme tuşuna bastığınızda her şeyin normale döneceğini unutmayın.

soru

Ödeme duvarının arkasındaki bayrak nedir? (İPUCU ⇒ <https://assets.tryhackme.com/additional/walkinganapplication/updating-html-css.gif>)

⇒ THM{NOT_SO_HIDDEN}





Task 5 Developer Tools - Debugger (Geliştirici Araçları - Hata Ayıklayıcı)

Geliştirici Araçları - Hata Ayıklayıcı

Geliştirici araçlarındaki bu panel JavaScript'te hata ayıklamak için tasarlanmıştır ve yine bir şeyin neden çalışmadığını anlamak isteyen web geliştiricileri için mükemmel bir özelliktir. Ancak sızma testçileri olarak bize JavaScript kodunun derinliklerine inme seçeneği sunar. Firefox ve Safari'de bu özelliğin adı Debugger'dır, ancak Google Chrome'da Sources olarak adlandırılır.

Acme IT Support web sitesinde, iletişim sayfasına tıklayın, sayfa her yüklendiğinde, ekranda hızlı bir kırmızı yanıp sönme fark edebilirsiniz. Bu kırmızı flaşın ne olduğunu ve ilginç bir şey içerip içermediğini anlamak için Hata Ayıklayıcı'yı kullanacağız. Kırmızı bir noktayı ayıklamak gerçek dünyada bir sızma testçisi olarak yapacağınız bir şey değildir, ancak bu özelliği kullanmamıza ve Hata Ayıklayıcı'ya alışmamıza olanak tanır.

Her iki tarayıcıda da sol tarafta, geçerli web sayfasının kullandığı tüm kaynakların bir listesini görürsünüz. Varlıklar klasörüne tıklarsanız flash.min.js adında bir dosya görürsünüz. Bu dosyaya tıkladığınızda JavaScript dosyasının içeriği görüntülenir.

Çoğu zaman javascript dosyalarını görüntülerken, her şeyin tek bir satırda olduğunu fark edersiniz, bunun nedeni dosyanın küçültülmüş olmasıdır, yani dosyayı küçültmek için tüm biçimlendirmeler (sekmeler, boşluklar ve yeni satırlar)

kaldırılmıştır. Bu dosya da buna bir istisna değildir ve aynı zamanda diğer geliştiriciler tarafından kolayca kopyalanamaması için okunmasını kasıtlı olarak zorlaştıran obfuscation edilmiştir.

Biraz daha okunabilir hale getirmek için iki parantez `{ }` gibi görünen "Pretty Print" seçeneğini kullanarak bazı biçimlendirmeleri döndürebiliriz, ancak karmaşıklık nedeniyle dosyada neler olup bittiğini anlamak hala zordur. Eğer flash.min.js dosyasının en altına doğru ilerlerseniz, şu satırı göreceksiniz: `flash.remove ;`

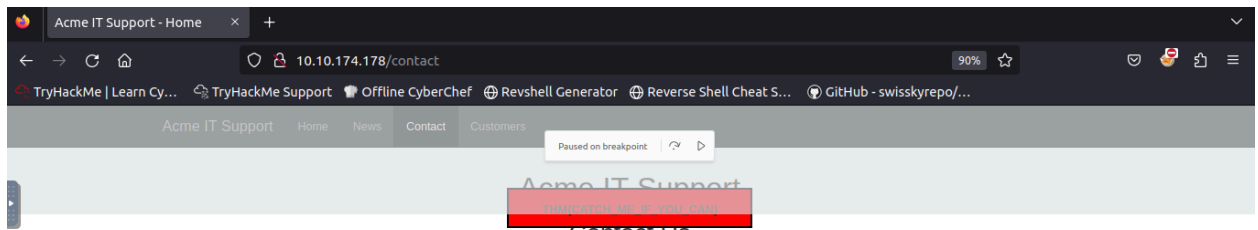
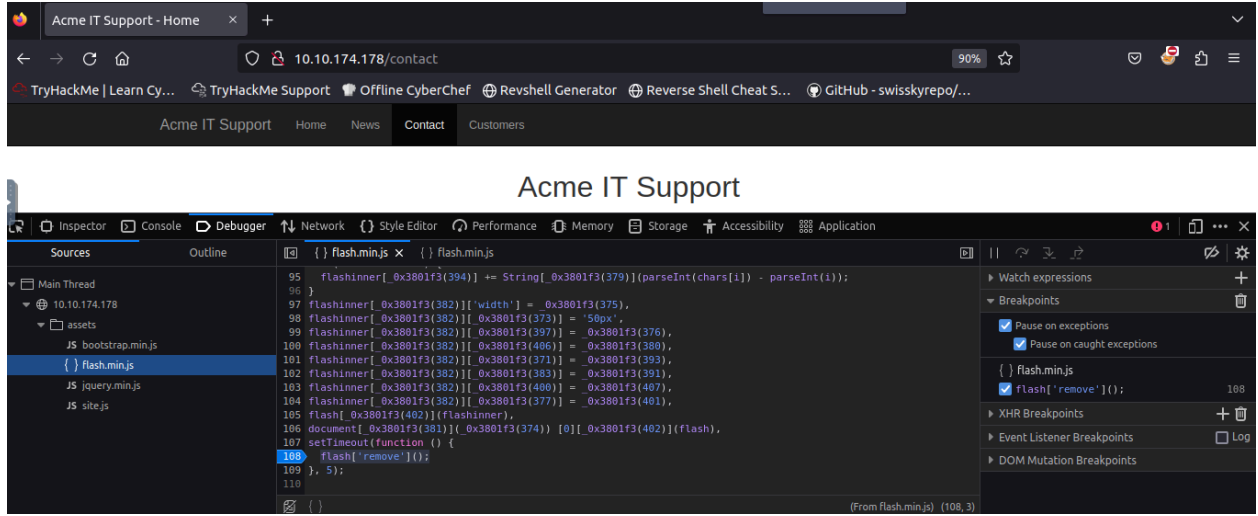
Bu küçük JavaScript parçası, kırmızı açılır pencereyi sayfadan kaldıran şeydir. Hata ayıklayıcının kesme noktaları adı verilen başka bir özelliğini kullanabiliriz. Bunlar kodda tarayıcıyı JavaScript'i işlemeyi durdurmaya ve mevcut yürütmeyi duraklatmaya zorlayabileceğimiz noktalardır.

Yukarıdaki kodu içeren satır numarasına tıklarsanız, maviye döndüğünü fark edeceksiniz; artık bu satıra bir kesme noktası eklediniz. Şimdi sayfayı yenilemeyi deneyin; kırmızı kutunun kaybolmak yerine sayfada kaldığını ve bir bayrak içerdiğini göreceksiniz.

soru

Kırmızı kutudaki bayrak nedir? (İPUCU ⇒ Hata ayıklayıcı araçları Firefox/Chrome üzerinde farklı çalışabilir. JavaScript flash.min.js dosyasını bulmak, güzelleştirmek, "flash.remove" satırını bulmak ve sayfa yüklendiğinde kırmızı mesajın kaybolmasını durdurmak için bir JavaScript kesme noktası eklemek için görevdeki adımları izleyin.)

⇒ `THM{CATCH_ME_IF_YOU_CAN}`



Task 6 Developer Tools - Network (Geliştirici Araçları - Ağ)

Geliştirici Araçları - Ağ

Geliştirici araçlarındaki ağ sekmesi, bir web sayfasının yaptığı her harici isteği takip etmek için kullanılabilir. Ağ sekmesine tıklar ve ardından sayfayı yenilerseniz, sayfanın talep ettiği tüm dosyaları görürsünüz.

Bunu iletişim sayfasında yapmayı deneyin; liste biraz kalabalıklaşırsa silmek için çöp kutusu simgesine basabilirsiniz.

Ağ sekmesi açıkken, iletişim formunu doldurmayı ve Mesaj Gönder düğmesine basmayı deneyin. Ağ sekmesinde bir olay göreceksiniz ve bu, formun AJAX adı verilen bir yöntem kullanılarak arka planda gönderilmesidir. AJAX, geçerli web sayfasını değiştirerek müdahale etmeden bir web uygulamasının arka planında ağ verilerini göndermek ve almak için kullanılan bir yöntemdir.

İletişim formunun oluşturduğu ağ sekmesindeki yeni girişi inceleyin ve bir bayrağı ortaya çıkarmak için verilerin gönderildiği sayfayı görüntüleyin.

soru

Contact-msg ağ talebinde gösterilen bayrak nedir? (İPUCU⇒ Contact-msg talebini bulduğunuzda, talebin yanıtını göstermek için üzerine tıkladığınızdan emin olun (tıkladığınızda gösterilen bir yanıt sekmesi olabilir).)

⇒ THM{GOT_AJAX_FLAG}

