

Burp Suite: The Basics

Task 1 Introduction (Görev 1 Giriş)

Burp Suite Basics'e hoş geldiniz!

Bu özel oda, Burp Suite web uygulaması güvenlik testi çerçevesinin temellerini anlamayı amaçlamaktadır. Odak noktamız aşağıdaki temel hususlar etrafında dönecektir:

- 1- Burp Suite'e kapsamlı bir giriş.
- 2- Çerçeve içinde mevcut olan çeşitli araçlara kapsamlı bir genel bakış.
- 3- Burp Suite'i sisteminize yükleme süreci hakkında ayrıntılı rehberlik.
- 4- Burp Suite'te gezinme ve yapılandırma.

Ayrıca Burp Suite çerçevesinin çekirdeği olan Burp Proxy'yi de tanıtacağız. Bu odanın öncelikle Burp Suite hakkında bilgi edinmek için temel bir kaynak olarak hizmet ettiğini belirtmek önemlidir. Burp modülündeki sonraki odalar daha pratik bir yaklaşım benimseyecektir. Bu nedenle, bu oda teorik içeriğe daha fazla vurgu yapacaktır. Burp Suite'i henüz kullanmadıysanız, verilen bilgileri dikkatlice okumanız ve araçla aktif olarak etkileşime girmeniz önerilir. Bu çerçevenin temellerini kavramak için deney yapmak şarttır. Burada sunulan bilgileri uygulamalı keşiflerle birleştirmek, çerçeveyi kullanmak için güçlü bir temel oluşturacaktır. Bu, gelecekteki odalarda size önemli ölçüde yardımcı olacaktır.

Başlayalım!

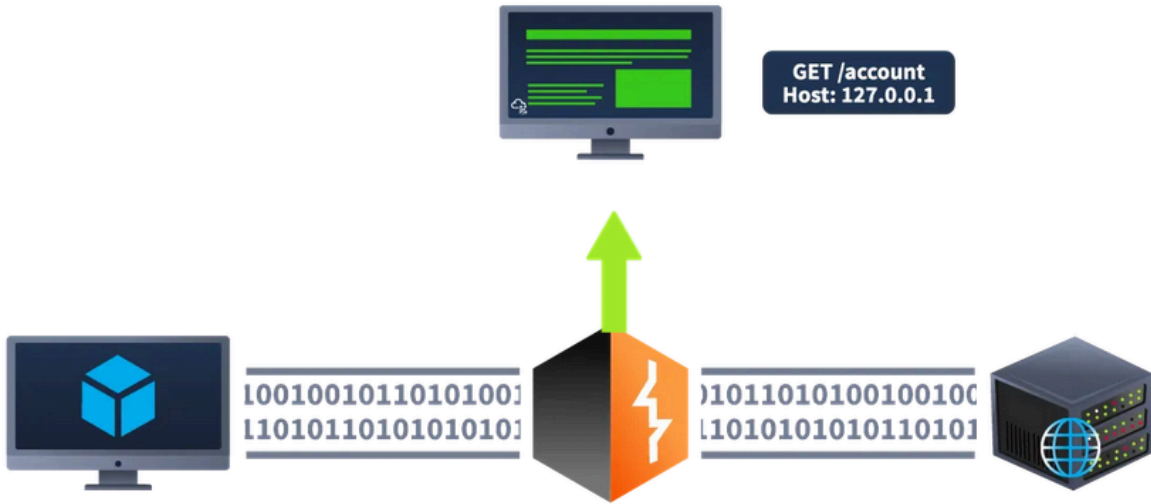
Cevap Gerekmemektedir.

Task 2 What is Burp Suite (Görev 2 Burp Suite nedir)

Özünde Burp Suite, web uygulaması sızma testi yapmak için kapsamlı bir çözüm olarak hizmet etmek üzere tasarlanmış Java tabanlı bir çerçevedir. Uygulama programlama arayüzlerine (API'ler) dayananlar da dahil olmak üzere web ve mobil

uygulamaların uygulamalı güvenlik değerlendirmeleri için endüstri standardı bir araç haline gelmiştir.

Basitçe söylemek gerekirse, Burp Suite bir tarayıcı ile bir web sunucusu arasındaki tüm HTTP/HTTPS trafiğini yakalar ve manipüle edilmesini sağlar. Bu temel yetenek, çerçevenin omurgasını oluşturur. Kullanıcılar, istekleri durdurarak, onları Burp Suite çerçevesi içindeki çeşitli bileşenlere yönlendirme esnekliğine sahip olurlar; bunları ilerleyen bölümlerde inceleyeceğiz. Web isteklerini hedef sunucuya ulaşmadan önce durdurma, görüntüleme ve değiştirme ve hatta tarayıcımız tarafından alınmadan önce yanıtları manipüle etme yeteneği, Burp Suite'i manuel web uygulaması testi için paha biçilmez bir araç haline getirir.



Burp Suite'in farklı sürümleri mevcuttur. Bizim amacımız doğrultusunda, yasal sınırlar içinde ticari olmayan kullanım için ücretsiz olarak erişilebilen Burp Suite Community Edition'a odaklanacağız. Bununla birlikte, Burp Suite'in gelişmiş özelliklerle gelen ve lisanslama gerektiren Professional ve Enterprise sürümleri de sunduğunu belirtmek gerekir:

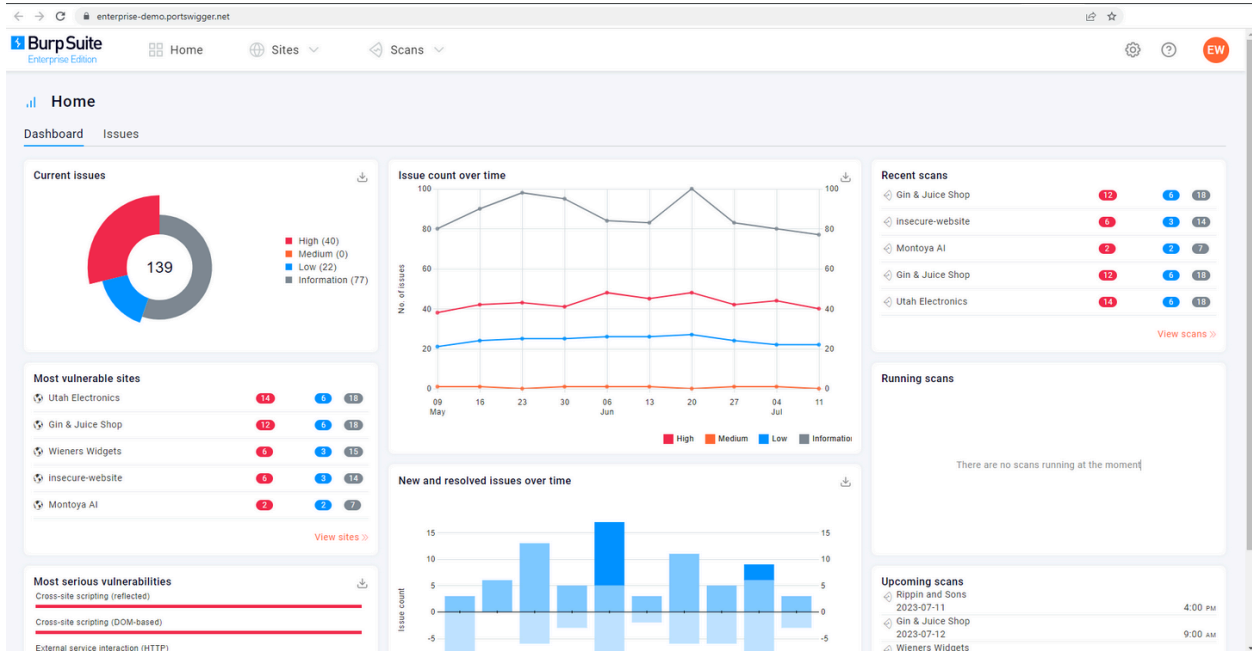
1- Burp Suite Professional, Burp Suite Community'nin kısıtlanmamış bir sürümüdür. Aşağıdakiler gibi özelliklerle birlikte gelir:

- Otomatik bir güvenlik açığı tarayıcısı.
- Hız sınırlaması olmayan bir fuzzer/brute-forcer.
- Gelecekte kullanım ve rapor oluşturma için projeleri kaydetme.

- Diğer araçlarla entegrasyona izin veren yerleşik bir API.
- Daha fazla işlevsellik için yeni uzantılar eklemek için sınırsız erişim.
- Burp Suite Collaborator'a erişim (etkin bir şekilde kendi kendine barındırılan veya Portswigger'a ait bir sunucuda çalışan benzersiz bir istek yakalayıcı sağlar).

Kısacası, Burp Suite Professional son derece güçlü bir araçtır ve bu da onu alandaki profesyoneller için tercih edilen bir seçenek haline getirir.

2- Burp Suite Enterprise, topluluk ve profesyonel sürümlerin aksine, öncelikle sürekli tarama için kullanılır. Nessus gibi araçların otomatik altyapı taraması yapmasına benzer şekilde, web uygulamalarını güvenlik açıkları için periyodik olarak tarayan otomatik bir tarayıcıya sahiptir. Yerel bir makineden manuel saldırılara izin veren diğer sürümlerin aksine, Burp Suite Enterprise bir sunucuda bulunur ve hedef web uygulamalarını potansiyel güvenlik açıklarına karşı sürekli olarak tarar.



Professional ve Enterprise sürümleri için lisans gerektirdiğinden, Burp Suite Community Edition tarafından sağlanan temel özellik setine odaklanacağız.

Not: Sunulan gösterimlerde Windows için Burp Suite kullanılmaktadır. Ancak, işlevsellik AttackBox'ta yüklü olan sürümle tutarlı kalmaktadır.

sorular;

soru⇒ Burp Suite'in hangi sürümü bir sunucuda çalışır ve hedef web uygulamaları için sürekli tarama sağlar?

cevap⇒ **Burp Suite Enterprise**

soru⇒ Burp Suite, web uygulamalarına ve _____ uygulamalarına saldırırken sıklıkla kullanılır.(İpucu Boşluğu doldurun.)

cevap⇒ **Mobile**

Task 3 Features of Burp Community (Görev 3 Burp Topluluğunun Özellikleri)

Burp Suite Community, Professional sürümüne kıyasla daha sınırlı bir özellik seti sunsa da, web uygulama testi için son derece değerli olan etkileyici bir dizi araç sağlar. Şimdi bazı temel özellikleri inceleyelim:

- Proxy: Burp Proxy, Burp Suite'in en ünlü yönüdür. Web uygulamaları ile etkileşim sırasında isteklerin ve yanıtların durdurulmasını ve değiştirilmesini sağlar.
- Repeater: Bir başka iyi bilinen özellik. Tekrarlayıcı, aynı isteği birden çok kez yakalamaya, değiştirmeye ve yeniden göndermeye olanak tanır. Bu işlevsellik özellikle deneme yanılma yoluyla yük oluştururken (örneğin SQLi - Yapılandırılmış Sorgu Dili Enjeksiyonu) veya bir uç noktanın işlevselliğini güvenlik açıkları için test ederken kullanışlıdır.
- Intruder: Burp Suite Community'deki hız sınırlamalarına rağmen, Intruder uç noktalara istek püskürtmeye izin verir. Genellikle kaba kuvvet saldırıları veya uç noktaları bulanıklaştırmak için kullanılır.
- Decoder: Kod çözücü, veri dönüşümü için değerli bir hizmet sunar. Yakalanan bilgilerin kodunu çözebilir veya hedefe göndermeden önce yükleri kodlayabilir. Bu amaç için alternatif hizmetler mevcut olsa da, Burp Suite içindeki Decoder'dan yararlanmak oldukça verimli olabilir.

- Comparer: Adından da anlaşılacağı gibi, Comparer iki veri parçasının kelime veya bayt düzeyinde karşılaştırılmasını sağlar. Burp Suite'e özel olmamakla birlikte, potansiyel olarak büyük veri segmentlerini tek bir klavye kısayoluyla doğrudan bir karşılaştırma aracına gönderme yeteneği süreci önemli ölçüde hızlandırır.
- Sequencer: Sıralayıcı genellikle oturum çerezi değerleri veya rastgele oluşturulduğu varsayılan diğer veriler gibi belirteçlerin rastgeleliğini değerlendirirken kullanılır. Bu değerleri oluşturmak için kullanılan algoritma güvenli rastgelelikten yoksunsa, yıkıcı saldırılar için yollar ortaya çıkarabilir.

Yerleşik özelliklerin ötesinde, Burp Suite'in Java kod tabanı, çerçevenin işlevselliğini geliştirmek için uzantıların geliştirilmesini kolaylaştırır. Bu uzantılar Java, Python (Java Jython yorumlayıcısı kullanılarak) veya Ruby (Java JRuby yorumlayıcısı kullanılarak) dillerinde yazılabilir. Burp Suite Extender modülü, uzantıların çerçeveye hızlı ve kolay bir şekilde yüklenmesini sağlarken, BApp Store olarak bilinen pazar yeri, üçüncü taraf modüllerin indirilmesine olanak tanır. Bazı uzantılar entegrasyon için profesyonel lisans gerektirse de, Burp Community için hala önemli sayıda uzantı mevcuttur. Örneğin, Logger++ modülü Burp Suite'in yerleşik günlük tutma işlevini genişletebilir.

sorular;

soru⇒ Hangi Burp Suite özelliği kendimiz ve hedef arasındaki istekleri engellememizi sağlar?

cevap ⇒ Proxy

soru ⇒ Bir giriş formunu kaba kuvvetle doldurmak için hangi Burp aracını kullanırız?

cevap ⇒ intruder

Task 4 Installation (Görev 4 Kurulum)

Burp Suite, web veya mobil uygulama değerlendirmeleri, pentesting, bug bounty avcılığı ve hatta web uygulaması geliştirmedeki özelliklerde hata ayıklama için

sahip olunması çok yararlı olan araçlardan biridir. İşte Burp Suite'i farklı platformlara yükleme rehberi:

Not: AttackBox kullanıyorsanız, Burp Suite zaten yüklüdür, bu nedenle bu adımı atlayabilirsiniz.

İndirmeler

Burp Suite'in diğer sistemler için en son sürümünü indirmek için, indirme sayfasına gitmek üzere bu düğmeyi tıklayabilirsiniz.

Kali Linux: Burp Suite, Kali Linux ile önceden yüklenmiş olarak gelir. Kali kurulumunuzda eksik olması durumunda, Kali apt depolarından kolayca yükleyebilirsiniz.

Linux, macOS ve Windows: Diğer işletim sistemleri için PortSwigger, Burp Suite indirmeleri sayfasında Burp Suite Community ve Burp Suite Professional için özel yükleyiciler sağlar. Açılır menüden işletim sisteminizi seçin ve Burp Suite Community Edition'ı seçin. Ardından, indirme işlemini başlatmak için İndir düğmesine tıklayın.

Burp Suite Releases



Professional / Community 2023.7

Early Adopter

Released Thursday, 6 July 2023

Burp Suite Professional

Windows (64-bit)

DOWNLOAD

view checksums

This release introduces the ability to easily customize the layout of Burp Suite's top-level tabs. We've also made some other improvements and fixed a few bugs.

Usage of this software is subject to the [licence agreement](#).

read more

Kurulum

İşletim sisteminiz için uygun yöntemi kullanarak Burp Suite'i yükleyin. Windows'ta çalıştırılabilir dosyayı çalıştırın, Linux'ta ise betiği terminalden çalıştırın (sudo ile veya sudo olmadan). Linux'ta kurulum sırasında sudo kullanmamayı seçerseniz,

Burp Suite ~/BurpSuiteCommunity/BurpSuiteCommunity adresindeki ev dizininize kurulacak ve PATH'inize eklenmeyecektir.

Kurulum sihirbazı açık talimatlar sunar ve varsayılan ayarları kabul etmek genellikle güvenlidir. Ancak, yükleyicinin her zaman dikkatlice incelenmesi önerilir.

Burp Suite başarıyla yüklendikten sonra artık uygulamayı başlatabilirsiniz. Bir sonraki görevde, ilk kurulum ve yapılandırmayı inceleyeceğiz.

sorular;

soru⇒ AttackBox'ı kullanmamayı seçtiyseniz, devam etmeden önce Burp Suite'in bir kopyasının kurulu olduğundan emin olun.

cevap ⇒ **Cevap Gerekmemektedir.**

Task 5 The Dashboard (Görev 5 Gösterge Tablosu)

AttackBox'ımızda önceden yüklenmiş Burp Suite Community Edition'ı kullanabilirsiniz. AttackBox'ı başlatmak için bu sayfanın üst kısmındaki Start AttackBox düğmesine tıklayın.

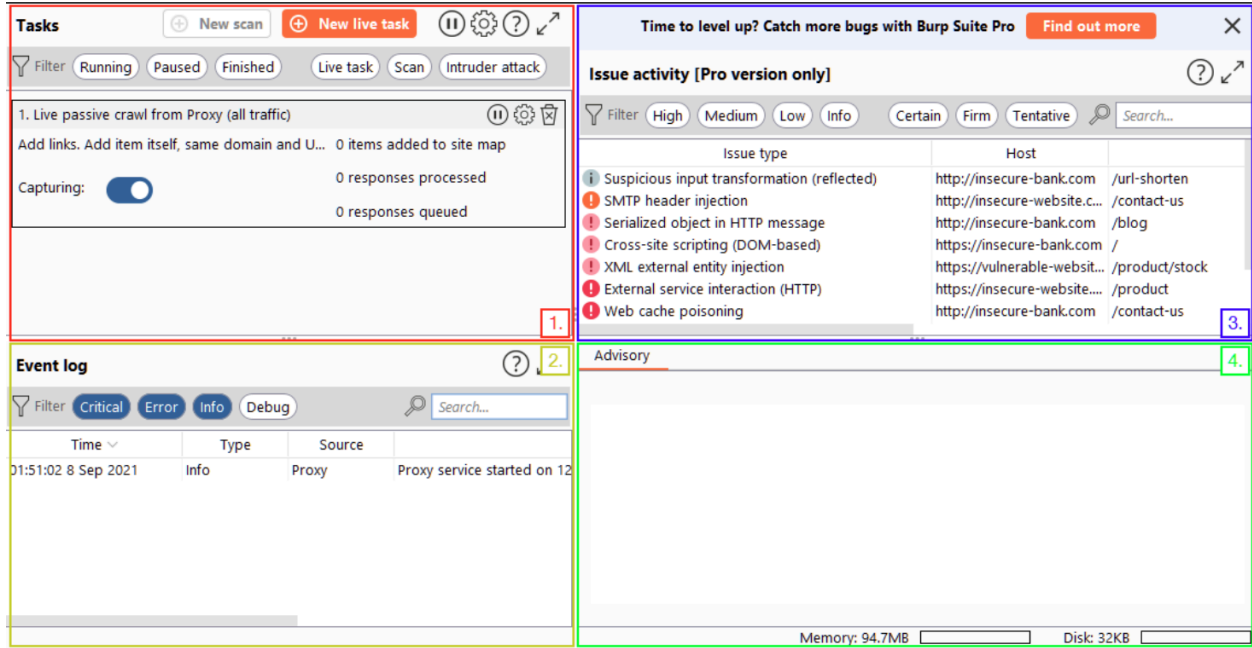
Burp Suite'i başlatıp hüküm ve koşulları kabul ettiğinizde, bir proje türü seçmeniz istenecektir. Burp Suite Community'de seçenekler sınırlıdır ve devam etmek için İleri'ye tıklayabilirsiniz.

Bir sonraki pencere Burp Suite için yapılandırmayı seçmenizi sağlar. Genellikle çoğu durum için uygun olan varsayılan ayarların korunması tavsiye edilir. Ana Burp Suite arayüzünü açmak için Burp'ü Başlat'a tıklayın.

Burp Suite'i ilk kez açtığınızda, eğitim seçeneklerini içeren bir ekranla karşılaşabilirsiniz. Zamanınız olduğunda bu eğitim materyallerini gözden geçirmeniz şiddetle tavsiye edilir.

Eğitim ekranını görmezseniz (veya sonraki oturumlarda), ilk başta bunaltıcı görünebilecek Burp Dashboard ile karşılaşacaksınız. Ancak, kısa süre içinde tanıdık gelecektir.

Burp Gösterge Paneli, sol üstten başlayarak saat yönünün tersine sırayla etiketlendiği gibi dört çeyreğe ayrılmıştır:



1- **Tasks** (Görevler): Görevler menüsü, siz uygulamayı kullanırken Burp Suite'in gerçekleştireceği arka plan görevlerini tanımlamanıza olanak tanır. Burp Suite Community'de, ziyaret edilen sayfaları otomatik olarak günlüğe kaydeden varsayılan "Live Passive Crawl" görevi bu modüldeki amaçlarımız için yeterlidir. Burp Suite Professional, isteğe bağlı taramalar gibi ek özellikler sunar.

2- **Event log**(Olay günlüğü): Olay günlüğü, proxy'nin başlatılması gibi Burp Suite tarafından gerçekleştirilen eylemlerin yanı sıra Burp aracılığıyla yapılan bağlantılarla ilgili ayrıntılar hakkında bilgi sağlar.

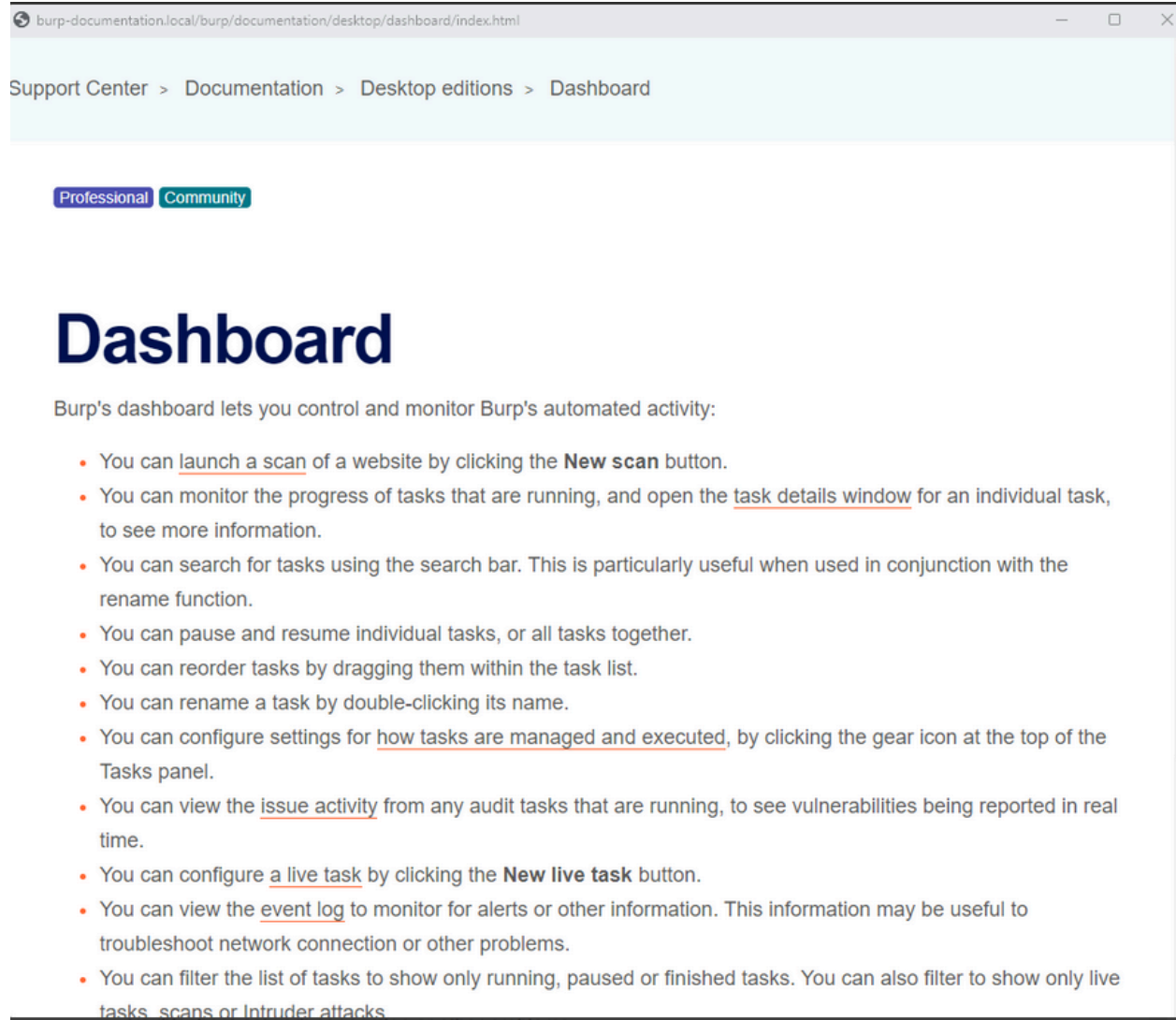
3- **Issue Activity**(Sorun Etkinliği): Bu bölüm Burp Suite Professional'a özeldir. Otomatik tarayıcı tarafından tespit edilen, önem derecesine göre sıralanan ve güvenlik açığının kesinliğine göre filtrelenebilen güvenlik açıklarını görüntüler.

4- **Advisory**(Danışma): Danışma bölümü, referanslar ve önerilen düzeltmeler de dahil olmak üzere tanımlanan güvenlik açıkları hakkında daha ayrıntılı bilgi sağlar. Bu bilgiler bir rapora aktarılabilir. Burp Suite Community'de bu bölüm herhangi bir güvenlik açığı göstermeyebilir.

Burp Suite'in çeşitli sekmeleri ve pencereleri boyunca soru işareti simgeleri (soru işareti simgesi) göreceksiniz.

Bu simgelere tıklandığında, söz konusu bölüme özgü yararlı bilgiler içeren yeni bir pencere açılır. Bu yardım simgeleri, belirli bir özellik hakkında yardıma veya

açıklamaya ihtiyaç duyduğunuzda çok değerlidir, bu nedenle bunları etkili bir şekilde kullandığınızdan emin olun.



Burp Suite'in farklı sekmelerini ve işlevlerini keşfederek, yavaş yavaş yeteneklerine aşina olacaksınız.

sorular;

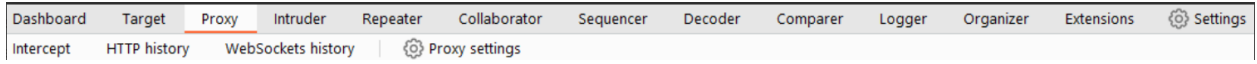
soru⇒ Proxy'yi başlatmak gibi Burp Suite tarafından gerçekleştirilen eylemler ve Burp aracılığıyla yapılan bağlantılarla ilgili ayrıntılar hakkında bilgi sağlayan menü hangisidir?

cevap ⇒ **Event Log**

Task 6 Navigation (Görev 6 Navigasyon)

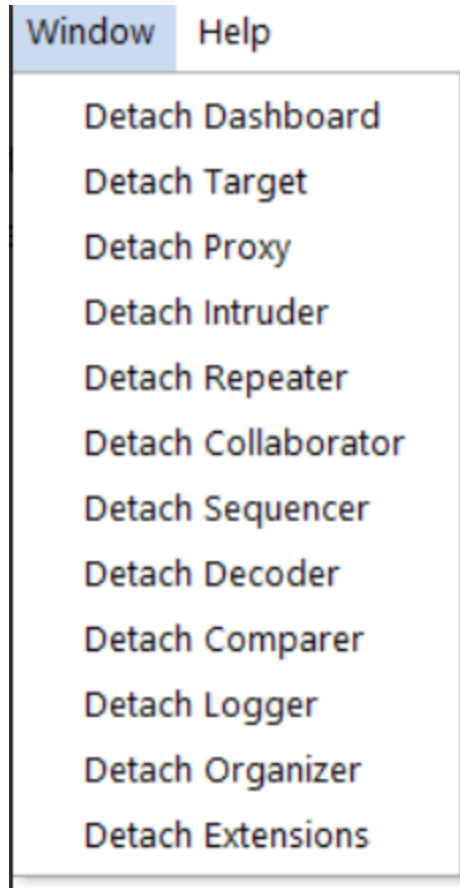
Burp Suite'te varsayılan gezinme, öncelikle modüller arasında geçiş yapmanıza ve her modül içindeki çeşitli alt sekmelere erişmenize olanak tanıyan üst menü çubukları aracılığıyla yapılır. Alt sekmeler, ana menü çubuğunun hemen altındaki ikinci bir menü çubuğunda görünür.

1- Module Selection (Modül Seçimi): Menü çubuğunun en üst satırında Burp Suite'teki mevcut modüller görüntülenir. Modüller arasında geçiş yapmak için her bir modüle tıklayabilirsiniz. Örneğin, aşağıdaki resimde Burp Proxy modülü seçilidir.



2-Sub-Tabs (Alt Sekmeler): Seçili bir modülün birden fazla alt sekmesi varsa, bunlara ana menü çubuğunun hemen altında görünen ikinci menü çubuğundan erişilebilir. Bu alt sekmeler genellikle modüle özgü ayarlar ve seçenekler içerir. Örneğin, yukarıdaki resimde Burp Proxy modülü içinde Proxy Intercept alt sekmesi seçilidir.

3 - Detaching Tabs (Sekmeleri Ayırma): Birden fazla sekmeyi ayrı ayrı görüntülemeyi tercih ederseniz, bunları ayrı pencerelere ayırabilirsiniz. Bunu yapmak için, Modül Seçim çubuğunun üzerindeki uygulama menüsünde Pencere seçeneğine gidin. Buradan "Ayr" seçeneğini seçin ve seçilen sekme ayrı bir pencerede açılacaktır. Ayrılan sekmeler aynı yöntem kullanılarak yeniden eklenebilir.



Burp Suite ayrıca önemli sekmelerde hızlı gezinme için klavye kısayolları sağlar. Varsayılan olarak aşağıdaki kısayollar mevcuttur:

Shortcut	Tab
Ctrl + Shift + D	Dashboard
Ctrl + Shift + T	Target tab
Ctrl + Shift + P	Proxy tab
Ctrl + Shift + I	Intruder tab
Ctrl + Shift + R	Repeater tab

sorular;

soru⇒ Ctrl + Shift + P bizi hangi sekmeye geçirecek?

cevap⇒ Proxy tab

Task 7 Options (Görev 7 Seçenekler)

Burp Proxy'ye dalmadan önce, Burp Suite'i yapılandırmak için mevcut seçenekleri inceleyelim. İki tür ayar vardır: Global ayarlar (Kullanıcı ayarları olarak da bilinir) ve Proje ayarları.

- Global Settings (Genel Ayarlar): Bu ayarlar tüm Burp Suite kurulumunu etkiler ve uygulamayı her başlattığınızda uygulanır. Burp Suite ortamınız için temel bir yapılandırma sağlarlar.
- Project Settings (Proje Ayarları): Bu ayarlar mevcut projeye özeldir ve yalnızca oturum sırasında geçerlidir. Ancak, Burp Suite Community Edition'ın projeleri kaydetmeyi desteklemediğini, bu nedenle Burp'u kapattığınızda projeye özgü seçeneklerin kaybolacağını lütfen unutmayın.

Ayarlara erişmek için üst gezinti çubuğundaki Ayarlar düğmesine tıklayın. Bu ayrı bir ayarlar penceresi açacaktır.

The screenshot shows the Burp Suite Settings window. The left sidebar has a search bar and tabs for 'All', 'User', and 'Project'. The 'Tools' section is expanded, showing 'Proxy' as the selected tool. The main area is divided into two sections: 'Proxy listeners' and 'Request interception rules'.

Proxy listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

	Running	Interface	Invisible	Redirect	Certificate	TLS Protocols	Support
<input type="button" value="Add"/>	<input checked="" type="checkbox"/>	127.0.0.1:8080			Per-host	Default	<input checked="" type="checkbox"/>
<input type="button" value="Edit"/>							
<input type="button" value="Remove"/>							

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in or another installation of Burp.

Request interception rules

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☒ Intercept requests based on the following rules: *Master interception is turned off*

	Enabled	Operator	Match type	Relationship	Condition
<input type="button" value="Add"/>	<input checked="" type="checkbox"/>		File extension	Does not match	(^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$ ^ico\$...
<input type="button" value="Edit"/>	<input type="checkbox"/>	Or	Request	Contains parameters	(get post)
<input type="button" value="Remove"/>	<input type="checkbox"/>	Or	HTTP method	Does not match	(get post)
<input type="button" value="Up"/>	<input type="checkbox"/>	And	URL	Is in target scope	
<input type="button" value="Down"/>					

☐ Automatically fix missing or superfluous new lines at end of request

☒ Automatically update Content-Length header when the request is edited

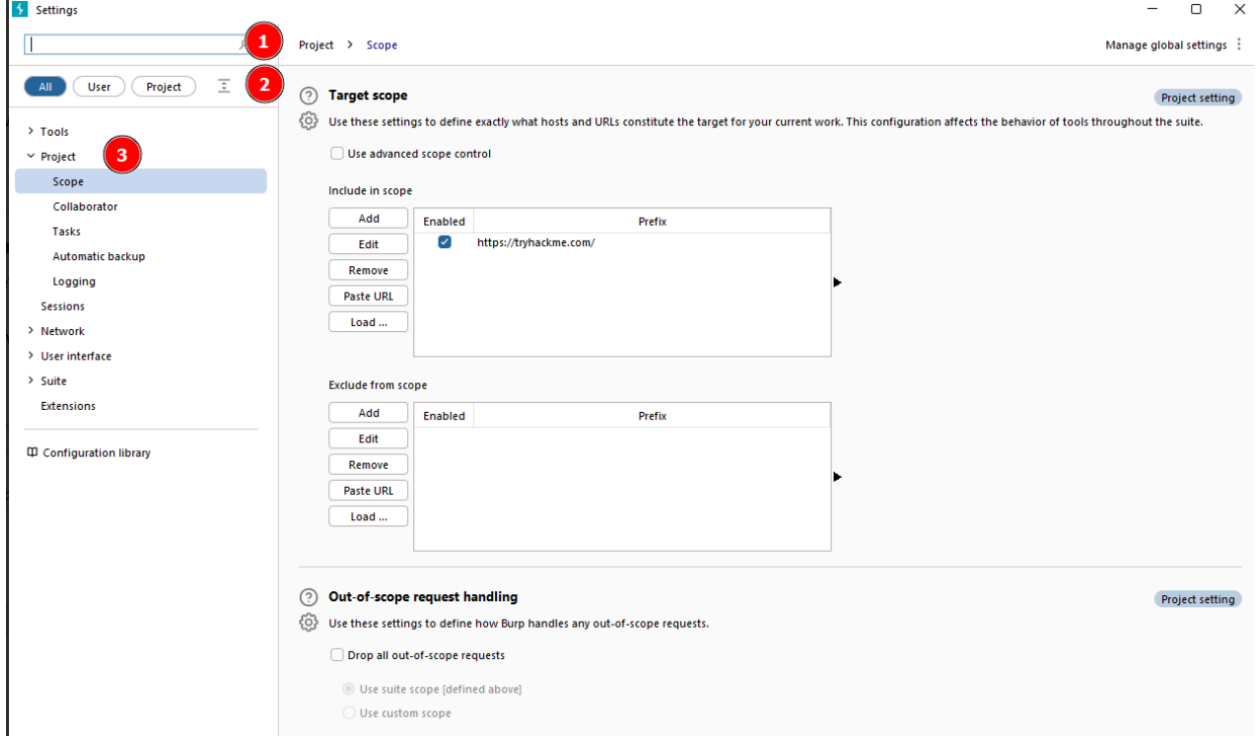
Ayarlar penceresinde, sol tarafta bir menü bulacaksınız. Bu menü, aşağıdakiler de dahil olmak üzere farklı ayar türleri arasında geçiş yapmanızı sağlar:

1- **Search (Arama):** Anahtar kelimeleri kullanarak belirli ayarların aranmasını sağlar.

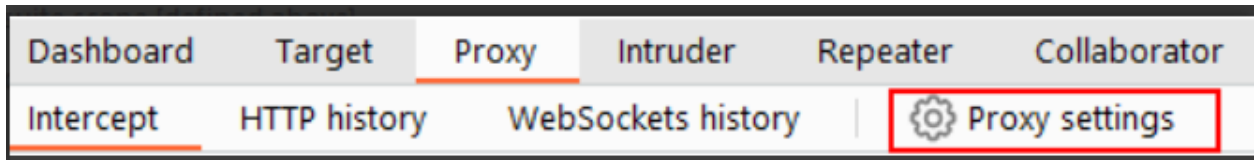
2- **Type filter** (Tip filtresi): Kullanıcı ve Proje seçenekleri için ayarları filtreler.

- **User settings** (Kullanıcı ayarları): Burp Suite kurulumunun tamamını etkileyen ayarları gösterir.
- **Project settings**(Proje ayarları): Geçerli projeye özgü ayarları görüntüler.

3- **Categories** (Kategoriler): Ayarların kategoriye göre seçilmesini sağlar.



Burp Suite içindeki birçok aracın belirli ayar kategorilerine kısayollar sağladığını belirtmek gerekir. Örneğin, Proxy modülü, ayarlar penceresini doğrudan ilgili proxy bölümüne açan bir Proxy ayarları düğmesi içerir.



Ayarlar sayfasındaki arama özelliği, anahtar kelimeleri kullanarak ayarları hızlı bir şekilde aramanıza olanak tanıyan değerli bir eklentidir.

Burp Suite'teki yapılandırılabilir seçenekler yelpazesini tanımak için biraz zaman ayırın. Kendinizi rahat hissettiğinizde, Burp Suite ayarlarının yapılandırılmasıyla ilgili alıştırmalara devam edebilirsiniz.

sorular;

soru⇒ Hangi kategoride "Kurabiye kavanozu" ile ilgili bir referans bulabilirsiniz?

cevap ⇒ **sessions**

soru⇒ Burp Suite güncelleme davranışını kontrol eden "Güncellemeler" alt kategorisini hangi temel kategoride bulabilirsiniz(İpucu Bu soruya cevabınız "Çeşitli" ise, Burp Suite'in eski bir sürümünü kullanıyorsunuz demektir. En son sürüme güncelleyin, ardından ayarlar penceresinde yanıtı arayın.)?

cevap ⇒ **suite**

soru ⇒ Burp Suite'te kısayollar için tuş atamalarını değiştirmenizi sağlayan alt kategorinin adı nedir?

cevap ⇒ **hotkeys**

soru ⇒ İstemci Tarafı TLS sertifikaları yüklediysek, bunları proje bazında geçersiz kılabilir miyiz (evet/hayır)(İpucu "İstemci TLS Sertifikaları" için arama yapın, ardından bölüm başlığının sağında verilen kapsamlara bakın.)?

cevap ⇒ **yea**

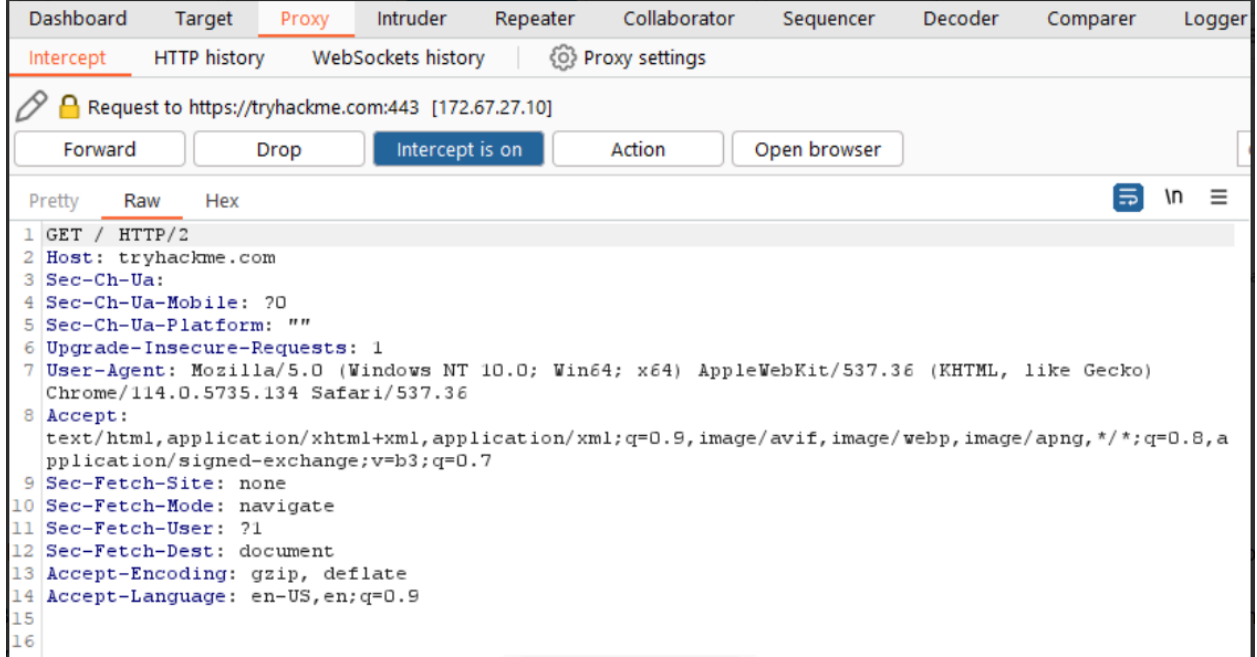
Task 8 Introduction to the Burp Proxy (Görev 8 Burp Proxy'ye Giriş)

Burp Proxy, Burp Suite içinde temel ve önemli bir araçtır. Kullanıcı ile hedef web sunucusu arasındaki istek ve yanıtların yakalanmasını sağlar. Yakalanan bu trafik manipüle edilebilir, daha fazla işlem için diğer araçlara gönderilebilir veya açıkça hedefine devam etmesine izin verilebilir.

Burp Proxy Hakkında Anlaşılması Gereken Önemli Noktalar

Intercepting Requests (İstekleri Engelleme): İstekler Burp Proxy aracılığıyla yapıldığında, durdurulur ve hedef sunucuya ulaşmaları engellenir. İstekler Proxy sekmesinde görünür ve iletme, bırakma, düzenleme veya diğer Burp modüllerine

gönderme gibi diğer eylemlere izin verir. Engellemeyi devre dışı bırakmak ve isteklerin kesintisiz olarak proxy'den geçmesine izin vermek için **Intercept is on** (Engelleme açık) düğmesine tıklayın.



- **Taking Control** (Kontrolü Ele Almak): İstekleri engelleme yeteneği, test uzmanlarının web trafiği üzerinde tam kontrol sahibi olmalarını sağlayarak web uygulamalarını test etmek için paha biçilmez hale getirir.
- **Capture and Logging** (Yakalama ve Günlükleme): Burp Suite, durdurma kapalı olsa bile varsayılan olarak proxy üzerinden yapılan istekleri yakalar ve günlüğe kaydeder. Bu günlük tutma işlevi, daha sonraki analizler ve önceki taleplerin gözden geçirilmesi için yararlı olabilir.
- **WebSocket Support** (WebSocket Desteği): Burp Suite ayrıca WebSocket iletişimini yakalayıp günlüğe kaydederek web uygulamalarını analiz ederken ek yardım sağlar.
- **Logs and History** (Günlükler ve Geçmiş): Yakalanan istekler HTTP geçmişi ve WebSockets geçmişi alt sekmelerinde görüntülenebilir, böylece geriye dönük analiz yapılabilir ve istekler gerektiğinde diğer Burp modüllerine gönderilebilir.

Dashboard	Target	Proxy	Intruder	Repeater	Collaborator	Sequencer	Decoder	Comparer	Logger	Organizer	Extensions	Settings
Intercept	HTTP history	WebSockets history	Proxy settings									
Filter: Hiding CSS, image and general binary content												
#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title		
8	https://assets.tryhackme.com	GET	/js/popper.min.js			200	34557	script	js			
10	https://assets.tryhackme.com	GET	/js/jquery.min.js?v=3.5.1	✓		200	128920	script	js			
18	https://assets.tryhackme.com	GET	/js/bootstrap431.min.js			200	93752	script	js			
19	https://assets.tryhackme.com	GET	/js/script.js?v=3.11	✓		200	21758	script	js			
20	https://assets.tryhackme.com	GET	/js/validation.js			200	1935	script	js			
40	https://tryhackme.com	GET	/assets/pace/pace.js			200	28469	script	js			
42	https://cdnjs.cloudflare.com	GET	/ajax/libs/cookieconsent2/3.0.3/cookie...			200	20784	script	js			
43	https://kenwheelers.github.io	GET	/slick/slick/slick.js			200	84960	script	js			
44	https://tryhackme.com	GET	/cdn-cgi/scripts/5c5dd728/cloudflare...			200	1624	script	js			
45	https://assets.tryhackme.com	GET	/js/path.js?v=1.3	✓		200	8891	script	js			

Proxy'ye özgü seçeneklere Proxy ayarları düğmesine tıklayarak erişilebilir. Bu seçenekler Proxy'nin davranışı ve işlevselliği üzerinde kapsamlı kontrol sağlar. Burp Proxy kullanımınızı optimize etmek için bu seçeneklere aşina olun.

Proxy Ayarlarındaki Bazı Önemli Özellikler

- **Response Interception (Yanıt Engelleme):** Varsayılan olarak proxy, istek başına açıkça istenmediği sürece sunucu yanıtlarını engellemez. "Yanıtları aşağıdaki kurallara göre engelle" onay kutusu, tanımlanan kurallarla birlikte daha esnek bir yanıt engelleme olanağı sağlar.

Response interception rules

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

☒ Intercept responses based on the following rules: *Master interception is turned off*

	Enabled	Operator	Match type	Relationship	Condition
Add	<input checked="" type="checkbox"/>		Content type header	Matches	text
Edit	<input type="checkbox"/>	Or	Request	Was modified	
Remove	<input checked="" type="checkbox"/>	Or	Request	Was intercepted	
Up	<input type="checkbox"/>	And	Status code	Does not match	^304\$
Down	<input type="checkbox"/>	And	URL	Is in target scope	

☒ Automatically update Content-Length header when the response is edited

- **Match and Replace (Eşleştir ve Değiştir):** Proxy ayarlarındaki "Eşleştir ve Değiştir" bölümü, gelen ve giden istekleri değiştirmek için düzenli ifadelerin (regex) kullanılmasını sağlar. Bu özellik, kullanıcı aracısının değiştirilmesi veya çerezlerin manipüle edilmesi gibi dinamik değişikliklere olanak tanır.

Proxy seçeneklerini keşfetmek ve denemek için zaman ayırın, çünkü bu, araçla ilgili anlayışınızı ve yeterliliğinizi artıracaktır.

sorular;

soru⇒ Bir sonraki göreve geçmek için bana tıklayın.

cevap ⇒ **Cevap Gerekmektedir.**

Task 9 Connecting through the Proxy (FoxyProxy) (Görev 9 Proxy üzerinden bağlanma (FoxyProxy))

Aşağıdaki Makineyi Başlat düğmesine tıklayarak makineyi başlatın.

Burp Suite Proxy'yi kullanmak için yerel web tarayıcımızı trafiği Burp Suite üzerinden yönlendirecek şekilde yapılandırmamız gerekir. Bu görevde, Firefox'taki FoxyProxy uzantısını kullanarak proxy'yi yapılandırmaya odaklanacağız.

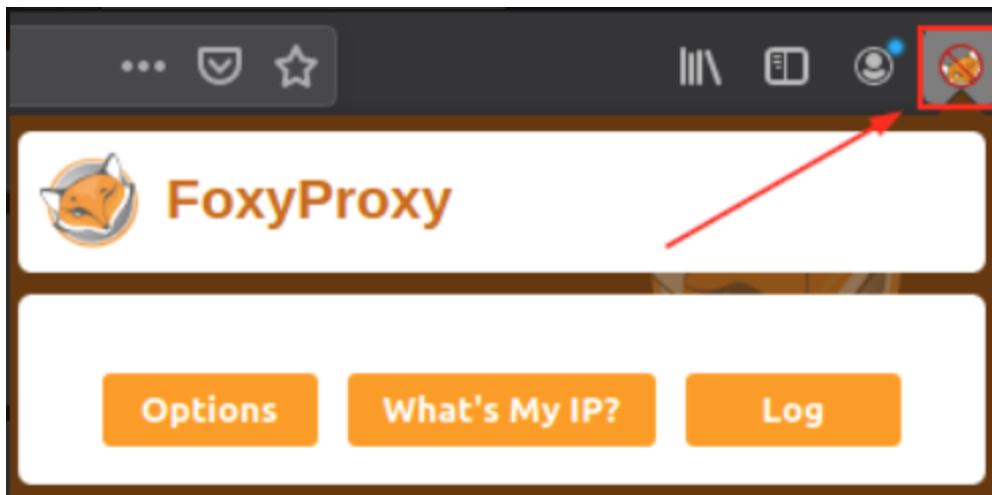
Lütfen verilen talimatların Firefox'a özel olduğunu unutmayın. Farklı bir tarayıcı kullanıyorsanız, alternatif yöntemler bulmanız veya TryHackMe AttackBox'ı kullanmanız gerekebilir.

Burp Suite Proxy'yi FoxyProxy ile yapılandırmak için gerekli adımları aşağıda bulabilirsiniz:

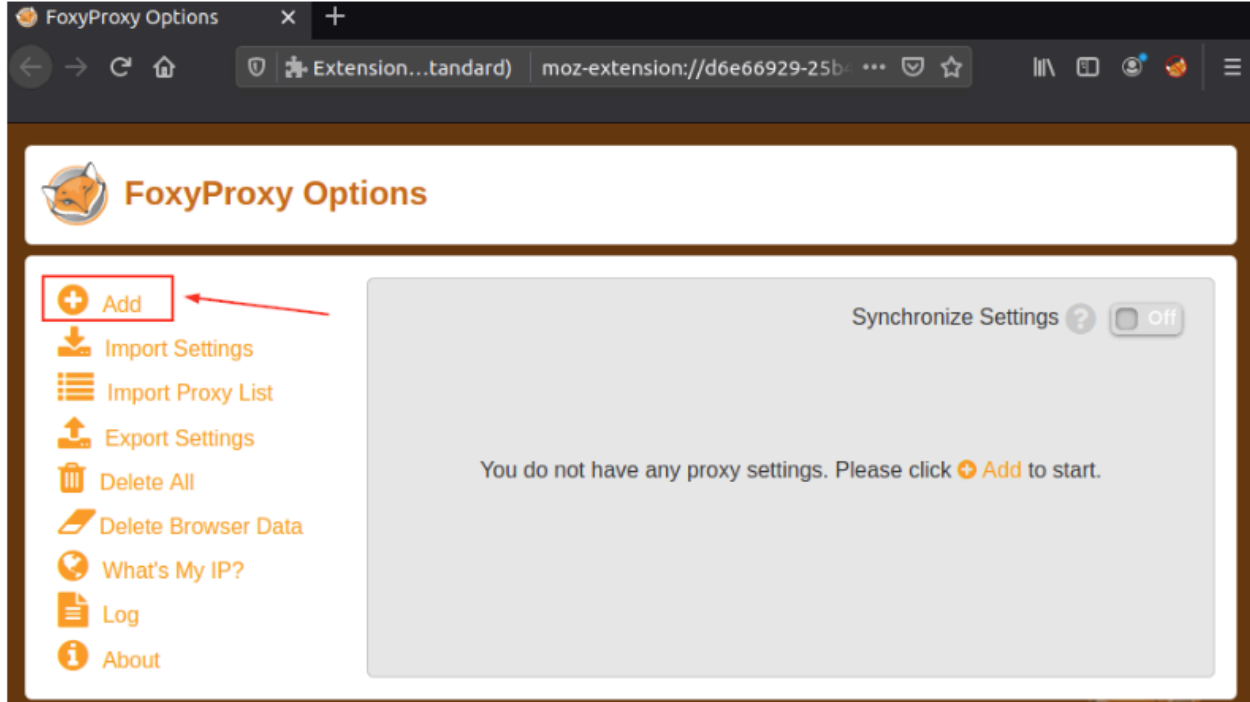
1- FoxyProxy'yi yükleyin: FoxyProxy Basic uzantısını indirin ve yükleyin.

Not: FoxyProxy zaten AttackBox üzerinde yüklüdür.

2- FoxyProxy Seçeneklerine erişin: Kurulduktan sonra, Firefox tarayıcısının sağ üst köşesinde bir düğme belirecektir. FoxyProxy seçenekleri açılır penceresine erişmek için FoxyProxy düğmesine tıklayın.

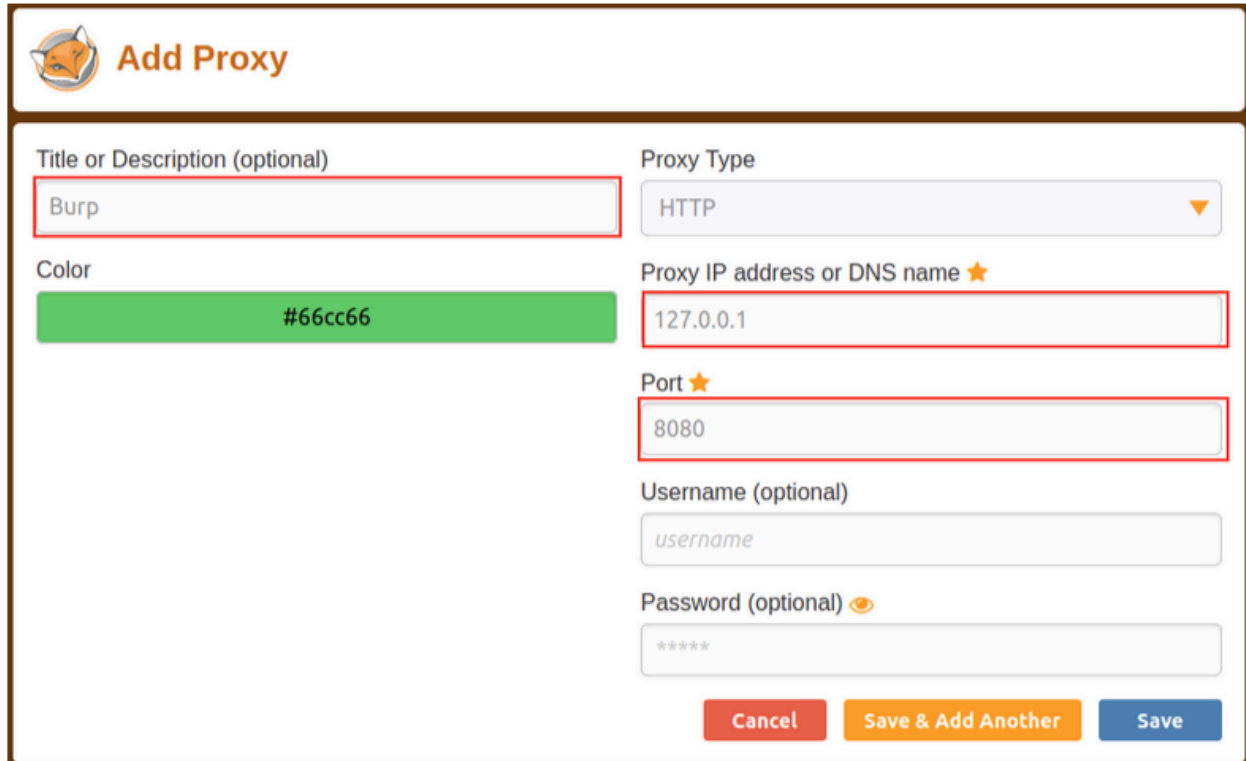


3- Burp Proxy Yapılandırması Oluşturun: FoxyProxy seçenekleri açılır penceresinde Seçenekler düğmesine tıklayın. Bu, FoxyProxy konfigürasyonlarını içeren yeni bir tarayıcı sekmesi açacaktır. Yeni bir proxy yapılandırması oluşturmak için Ekle düğmesine tıklayın.



Proxy Ayrıntılarını Ekleyin: "Proxy Ekle" sayfasında aşağıdaki değerleri doldurun:

- Title: **Burp** (or any preferred name)
- Proxy IP: **127.0.0.1**
- Port: **8080**



The image shows the 'Add Proxy' dialog box in FoxyProxy. It has a title bar with the FoxyProxy logo and the text 'Add Proxy'. The dialog is divided into two columns. The left column contains a 'Title or Description (optional)' text box with 'Burp' entered, a 'Color' dropdown menu showing '#66cc66', and a 'Proxy Type' dropdown menu showing 'HTTP'. The right column contains a 'Proxy IP address or DNS name' text box with '127.0.0.1' entered, a 'Port' text box with '8080' entered, a 'Username (optional)' text box with 'username' entered, and a 'Password (optional)' text box with '*****' entered. At the bottom right, there are three buttons: 'Cancel', 'Save & Add Another', and 'Save'.

Add Proxy

Title or Description (optional)
Burp


Color
#66cc66

Proxy Type
HTTP

Proxy IP address or DNS name ★
127.0.0.1

Port ★
8080

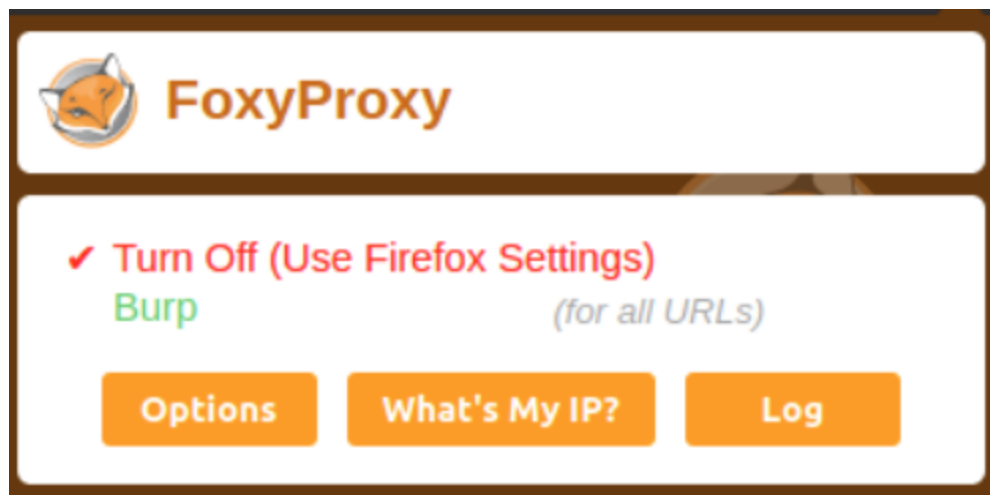
Username (optional)
username

Password (optional) 

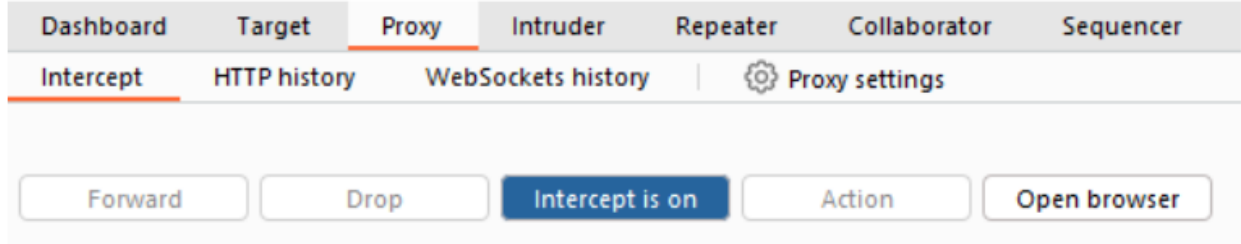
Cancel Save & Add Another Save

5- Yapılandırmayı Kaydet: Burp Proxy yapılandırmasını kaydetmek için Kaydet'e tıklayın.

6- Proxy Yapılandırmasını Etkinleştirin: Firefox tarayıcısının sağ üst köşesindeki FoxyProxy simgesine tıklayın ve Burp yapılandırmasını seçin. Bu, tarayıcı trafiğinizi 127.0.0.1:8080 üzerinden yönlendirecektir. Bu yapılandırma etkinleştirildiğinde tarayıcınızın istekte bulunabilmesi için Burp Suite'in çalışıyor olması gerektiğini unutmayın.



7- Burp Suite'te Proxy Intercept'i etkinleştirin: Burp Suite'e geçin ve Proxy sekmesinde Intercept'in açık olduğundan emin olun.



8- Proxy'yi test edin: Firefox'u açın ve <http://10.10.46.19/> ana sayfası gibi bir web sitesine erişmeyi deneyin. Tarayıcınız kilitlenecek ve proxy HTTP isteği ile dolacaktır. Tebrikler, ilk isteğinizi başarıyla yakaladınız!

Şunları unutmayın:

- Proxy yapılandırması etkin olduğunda ve Burp Suite'te engelleme açık olduğunda, bir istekte bulunduğunuzda tarayıcınız askıda kalacaktır.
- Tarayıcınızın herhangi bir istekte bulunmasını engelleyebileceğinden, engellemeyi istemeden açık bırakmamaya dikkat edin.
- Burp Suite'te bir isteğe sağ tıklamak, iletme, bırakma, diğer araçlara gönderme veya sağ tıklama menüsünden seçenekleri belirleme gibi çeşitli eylemler gerçekleştirmenize olanak tanır.

Not: Hedef VM'den istek yerine bazı WebSocket istekleri alacağınızdan, durdurmayı etkinleştirmeden önce AttackBox tarayıcısındaki diğer sekmeleri kapatmayı düşünün.

sorular;

soru ⇒ Bir sonraki göreve geçmek için bana tıklayın.

cevap ⇒ **Cevap Gerekmemektedir.**

Task 10 Site Map and Issue Definitions (Görev 10 Site Haritası ve Sorun Tanımları)

Burp Suite'teki Hedef sekmesi, testimizin kapsamı üzerinde kontrolden daha fazlasını sağlar. Üç alt sekmeden oluşur:

1- **Site map** (Site haritası): Bu alt sekme, hedeflediğimiz web uygulamalarını bir ağaç yapısında haritalandırmamızı sağlar. Proxy aktifken ziyaret ettiğimiz her sayfa site haritasında görüntülenecektir. Bu özellik, sadece web uygulamasına göz atarak otomatik olarak bir site haritası oluşturmamızı sağlar. Burp Suite Professional'da, site haritasını hedefin otomatik taramasını gerçekleştirmek, sayfalar arasındaki bağlantıları keşfetmek ve sitenin mümkün olduğunca çoğunu haritalamak için de kullanabiliriz. Burp Suite Community ile bile, ilk numaralandırma adımlarımız sırasında veri toplamak için site haritasını kullanabiliriz. Web uygulaması tarafından erişilen tüm API uç noktaları site haritasında yakalanacağından, API'leri haritalamak için özellikle yararlıdır.

2- **Issue definitions** (Sorun tanımları): Burp Community, Burp Suite Professional'da bulunan tam güvenlik açığı tarama işlevselliğini içermese de, tarayıcının aradığı tüm güvenlik açıklarının bir listesine erişebiliyoruz. Sorun tanımları bölümü, açıklamaları ve referansları ile birlikte web güvenlik açıklarının kapsamlı bir listesini sunar. Bu kaynak, raporlardaki güvenlik açıklarına atıfta bulunmak veya manuel test sırasında tespit edilmiş olabilecek belirli bir güvenlik açığını tanımlamaya yardımcı olmak için değerli olabilir.

3- **(Scope settings)** Kapsam ayarları: Bu ayar, Burp Suite'teki hedef kapsamı kontrol etmemizi sağlar. Testimizin kapsamını tanımlamak için belirli etki alanlarını/IP'leri dahil etmemizi veya hariç tutmamızı sağlar. Kapsamı yöneterek, özellikle hedeflediğimiz web uygulamalarına odaklanabilir ve gereksiz trafiği yakalamaktan kaçınabiliriz.

Genel olarak, Hedef sekmesi kapsam belirlemenin ötesinde özellikler sunarak web uygulamalarının haritasını çıkarmamıza, hedef kapsamımızda ince ayar yapmamıza ve referans amaçlı kapsamlı bir web güvenlik açıkları listesine erişmemize olanak tanır.

Challenge

<http://10.10.46.19/> adresindeki siteye bir göz atın - modül boyunca bunu çok kullanacağız. Ana sayfada bağlantı verilen diğer tüm sayfaları ziyaret edin, ardından site haritanızı kontrol edin - bir uç nokta çok sıra dışı olarak göze çarpmalıdır!

Tarayıcınızda bunu ziyaret edin (veya bu uç nokta için site haritası girişinin "Yanıt" bölümünü kullanın)

sorular;

soru ⇒ Olağandışı uç noktayı ziyaret ettikten sonra aldığınız bayrak nedir (İpucuBir dizi rastgele harf ve rakamdan oluşan bir isme sahip şüpheli bir sayfa arıyorsunuz.)?

cevap ⇒ **THM{NmNIZTliNGE1MWU1ZTQzMzgZnmFiNWVk}**

Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Length	MIME type	Title	Notes	Status code	Time requested
http://10.10.145.194	GET	/		6807	HTML	Bastion Hosting		200	16:11:51 20 D...
http://10.10.145.194	GET	/assets/favicon.ico							
http://10.10.145.194	GET	/assets/css/bootstrap-ico...							
http://10.10.145.194	GET	/assets/css/styles.css							
http://10.10.145.194	GET	/assets/css/home.css							
http://10.10.145.194	GET	/about/							
http://10.10.145.194	GET	/contact/							
http://10.10.145.194	GET	/ticket/							

Request: GET /about/ HTTP/1.1
Host: 10.10.145.194
Accept-Encoding: gzip, deflate, br
Accept: */*

Response: HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 20 Dec 2024 16:40:57 GMT
Content-Type: text/plain
Content-Length: 37
Connection: keep-alive
Front-End-Https: on
THM{NmNIZTliNGE1MWU1ZTQzMzgZnmFiNWVk}

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time
1	10.10.145.194	GET	/5yR2GLcoGoi22K			200									

Request: GET /5yR2GLcoGoi22K HTTP/1.1
Host: 10.10.145.194
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i

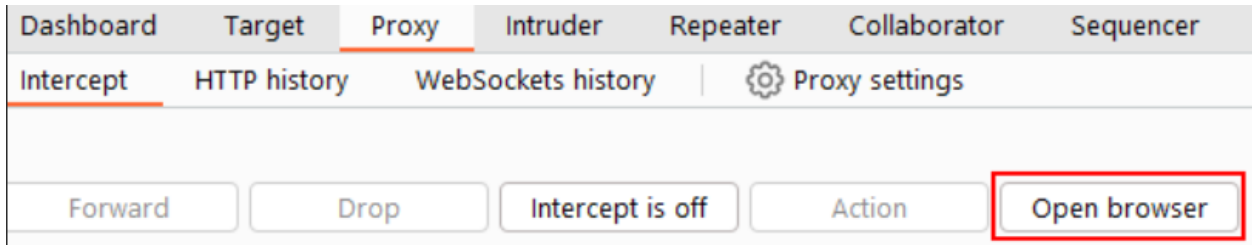
Response: HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 20 Dec 2024 16:40:57 GMT
Content-Type: text/plain
Content-Length: 37
Connection: keep-alive
Front-End-Https: on
THM{NmNIZTliNGE1MWU1ZTQzMzgZnmFiNWVk}

Task 11 The Burp Suite Browser (Görev 11 Burp Suite Tarayıcısı)

Önceki görevler aşırı karmaşık göründüyse, bu konunun çok daha basit olacağından emin olabilirsiniz.

Burp Suite, normal web tarayıcımızı proxy ile çalışacak şekilde değiştirmenin yanı sıra, az önce yapmamız gereken değişikliklerin hiçbiri olmadan proxy'yi kullanmak için önceden yapılandırılmış yerleşik bir Chromium tarayıcı da içerir.

Burp Tarayıcısını başlatmak için proxy sekmesindeki Open Browser düğmesine tıklayın. Bir Chromium penceresi açılacak ve bu tarayıcıda yapılan tüm istekler proxy üzerinden geçecektir.



Not: Proje seçenekleri ve kullanıcı seçenekleri ayarlarında Burp Tarayıcı ile ilgili birçok ayar vardır. Bunları keşfettiğinizden ve gerektiği gibi özelleştirdiğinizden emin olun.

Ancak, Burp Suite'i Linux üzerinde root kullanıcısı olarak çalıştırıyorsanız (AttackBox'ta olduğu gibi), bir sandbox ortamı oluşturulamaması nedeniyle Burp Browser'ın başlamasını engelleyen bir hatayla karşılaşabilirsiniz.

Bunun iki basit çözümü vardır:

1-Smart option (Akıllı seçenek): Yeni bir kullanıcı oluşturun ve Burp Suite'i düşük ayrıcalıklı bir hesap altında çalıştırarak Burp Browser'ın sorunsuz çalışmasını sağlayın.

2-Easy option (Kolay seçenek): Ayarlar → Araçlar → Burp'un tarayıcısı bölümüne gidin ve Burp'un tarayıcısının korumalı alan olmadan çalışmasına izin ver seçeneğini işaretleyin. Bu seçeneğin etkinleştirilmesi, tarayıcının bir sanal alan olmadan başlamasına izin verecektir. Ancak, güvenlik nedeniyle bu seçeneğin varsayılan olarak devre dışı bırakıldığını lütfen unutmayın. Etkinleştirmeyi seçerseniz, tarayıcıyı tehlikeye atmak bir saldırıya tüm makinenize erişim sağlayabileceğinden dikkatli olun. AttackBox'ın eğitim ortamında, bunun önemli bir sorun olması muhtemel değildir, ancak sorumlu bir şekilde kullanın.

sorular;

soru⇒

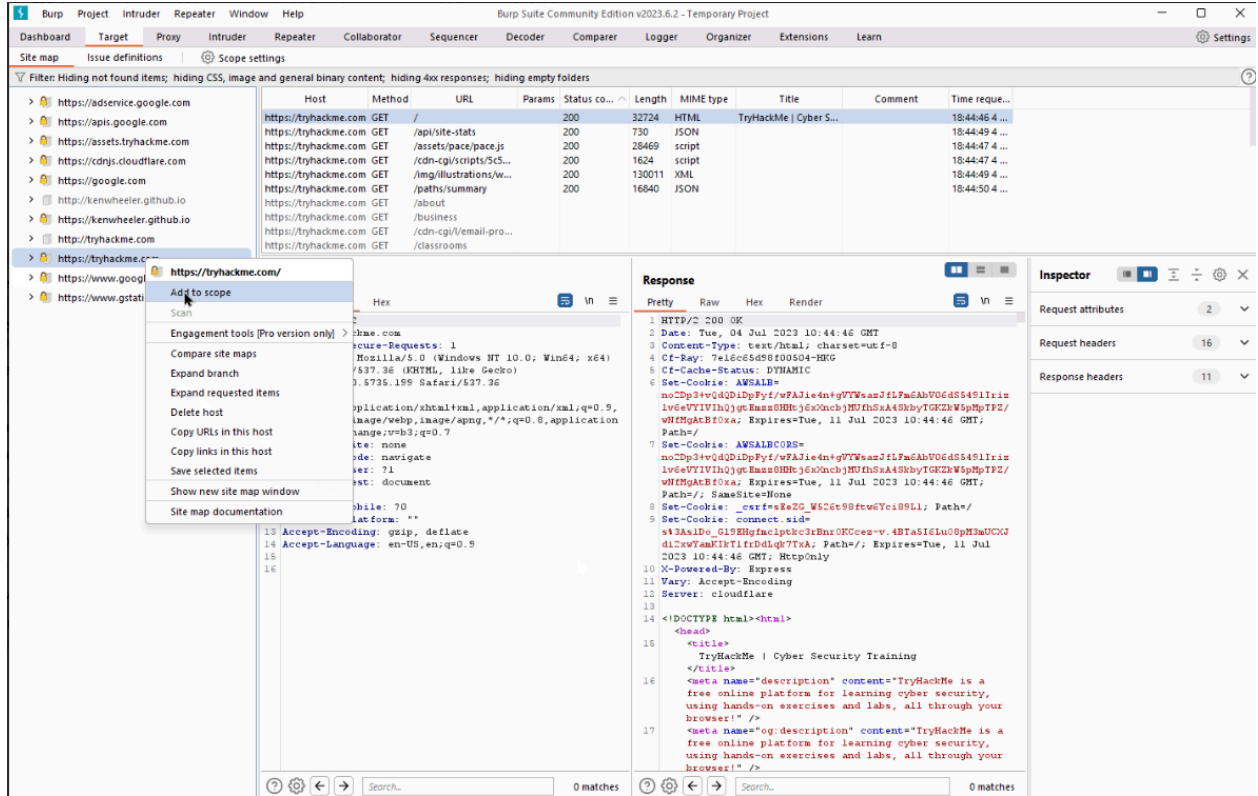
cevap ⇒ **Cevap Gerekmemektedir.**

Task 12 Scoping and Targeting (Görev 12 Kapsam Belirleme ve Hedefleme)

Son olarak, Burp Proxy kullanmanın en önemli yönlerinden birine geliyoruz:**Scoping**. (Kapsam belirleme.)

Tüm trafiği yakalamak ve kaydetmek, özellikle de yalnızca belirli web uygulamalarına odaklanmak istediğimizde, hızla bunaltıcı ve zahmetli hale gelebilir. İşte bu noktada kapsam belirleme devreye girer.

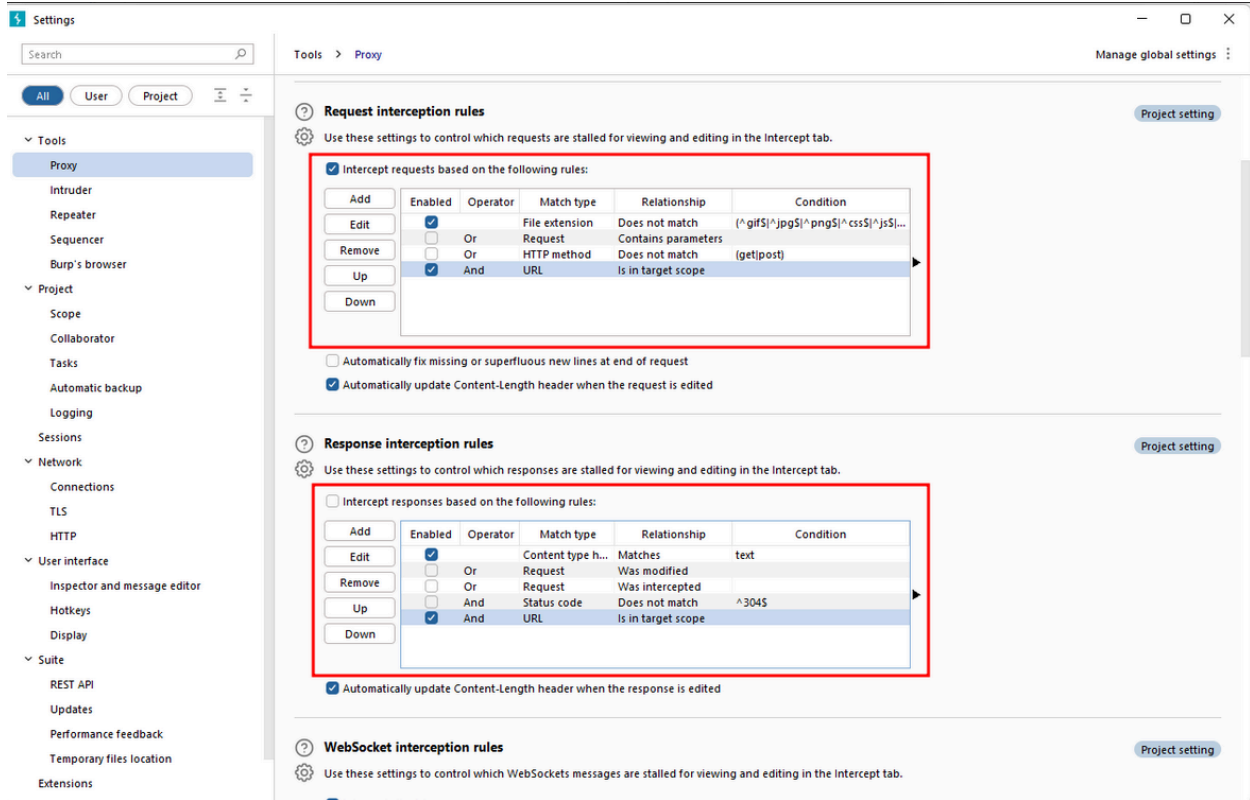
Proje için bir kapsam belirleyerek, Burp Suite'te neyin proxy'leneceğini ve günlüğe kaydedileceğini tanımlayabiliriz. Burp Suite'i yalnızca test etmek istediğimiz belirli web uygulamalarını hedefleyecek şekilde kısıtlayabiliriz. Bunu yapmanın en kolay yolu, Hedef sekmesine geçmek, soldaki listeden hedefimize sağ tıklamak ve Kapsam'a Ekle'yi seçmektir. Burp daha sonra kapsam dahilinde olmayan herhangi bir şeyi günlüğe kaydetmeyi durdurmak isteyip istemediğimizi seçmemizi isteyecektir ve çoğu durumda evet seçeneğini seçmek isteriz.



Kapsamımızı kontrol etmek için Hedef sekmesi içindeki Kapsam ayarları alt sekmesine geçebiliriz.

Kapsam ayarları penceresi, etki alanlarını/IP'leri dahil ederek veya hariç tutarak hedef kapsamımızı kontrol etmemizi sağlar. Bu bölüm güçlüdür ve aşına olmak için zaman harcamaya değer.

Ancak, kapsam dışı trafik için günlük tutmayı devre dışı bıraksak bile, proxy yine de her şeyi engelleyecektir. Bunu önlemek için Proxy ayarları alt sekmesine gitmemiz ve "İstemci İsteklerini Engelle" bölümünden Ve URL Hedef Kapsamında'yı seçmemiz gerekir.



Bu seçeneğin etkinleştirilmesi, proxy'nin tanımlanan kapsam dahilinde olmayan trafiği tamamen yok saymasını sağlayarak Burp Suite'te daha temiz bir trafik görünümü elde edilmesini sağlar.

Kapsamınıza `http://MACHINE_IP/` adresini ekleyin ve proxy ayarlarını yalnızca kapsam içi hedeflere giden trafiği engelleyecek şekilde değiştirin.

Kapsamı sınırlamadan önce ve sonra proxy tarafından yakalanan trafik miktarı arasındaki farka bakın.

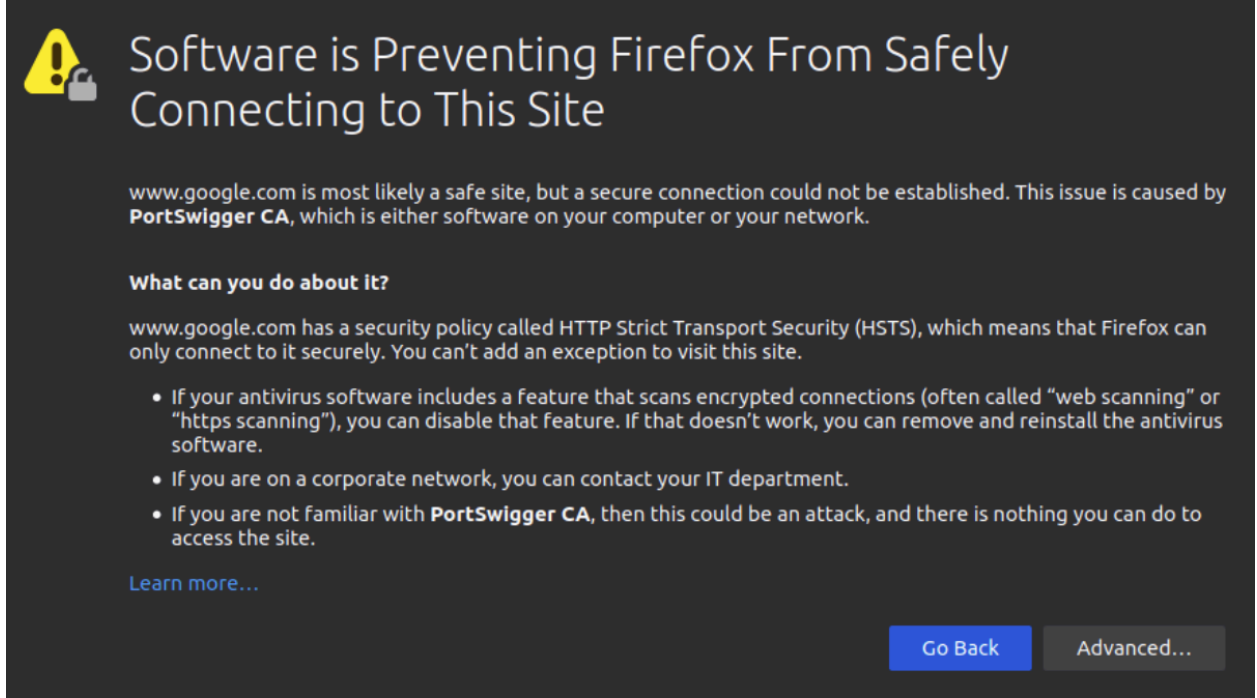
sorular;

Cevap⇒ **Cevap Gerekmemektedir.**

Task 13 Proxying HTTPS (Görev 13 HTTPS Proxyleme)

Not: AttackBox, bu görevde ortaya konan sorunu çözmek için zaten yapılandırılmıştır. AttackBox kullanıyorsanız ve buradaki bilgileri okumak istemiyorsanız, bir sonraki göreve geçebilirsiniz.

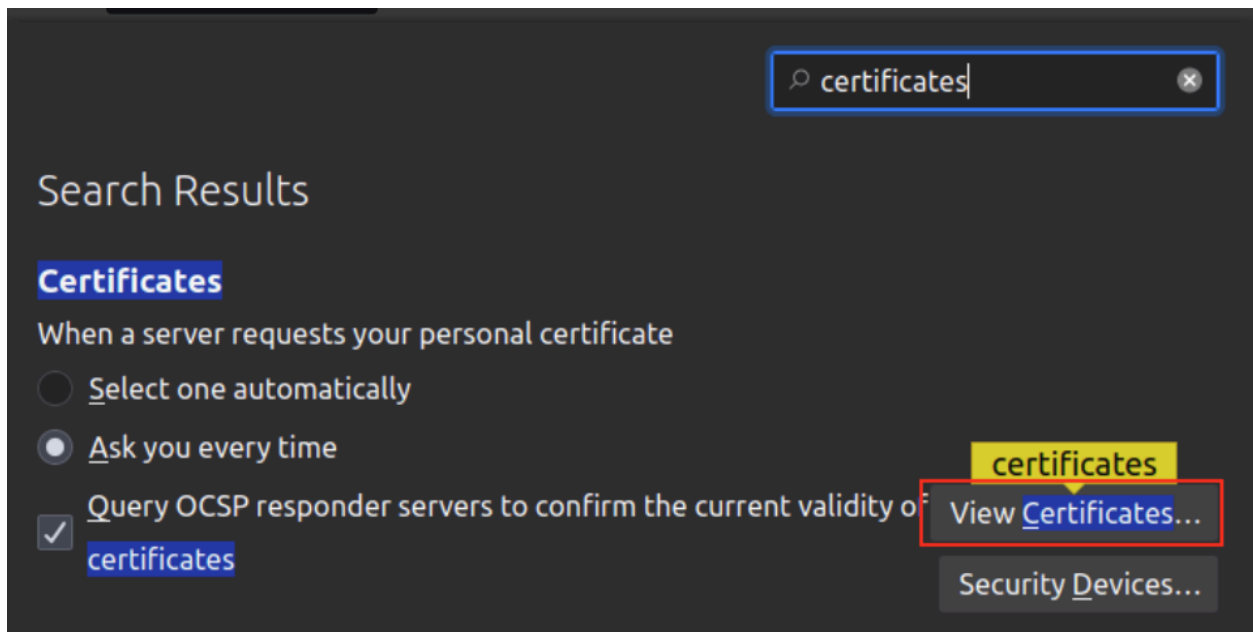
HTTP trafiğini keserken, TLS'nin etkin olduğu sitelerde gezinirken bir sorunla karşılaşabiliriz. Örneğin, <https://google.com/> gibi bir siteye erişirken, PortSwigger Sertifika Yetkilisinin (CA) bağlantıyı güvenli hale getirmek için yetkili olmadığını belirten bir hata alabiliriz. Bunun nedeni tarayıcının Burp Suite tarafından sunulan sertifikaya güvenmemesidir.



Bu sorunun üstesinden gelmek için PortSwigger CA sertifikasını tarayıcımızın güvenilir sertifika yetkilileri listesine manuel olarak ekleyebiliriz. İşte nasıl yapılacağı:

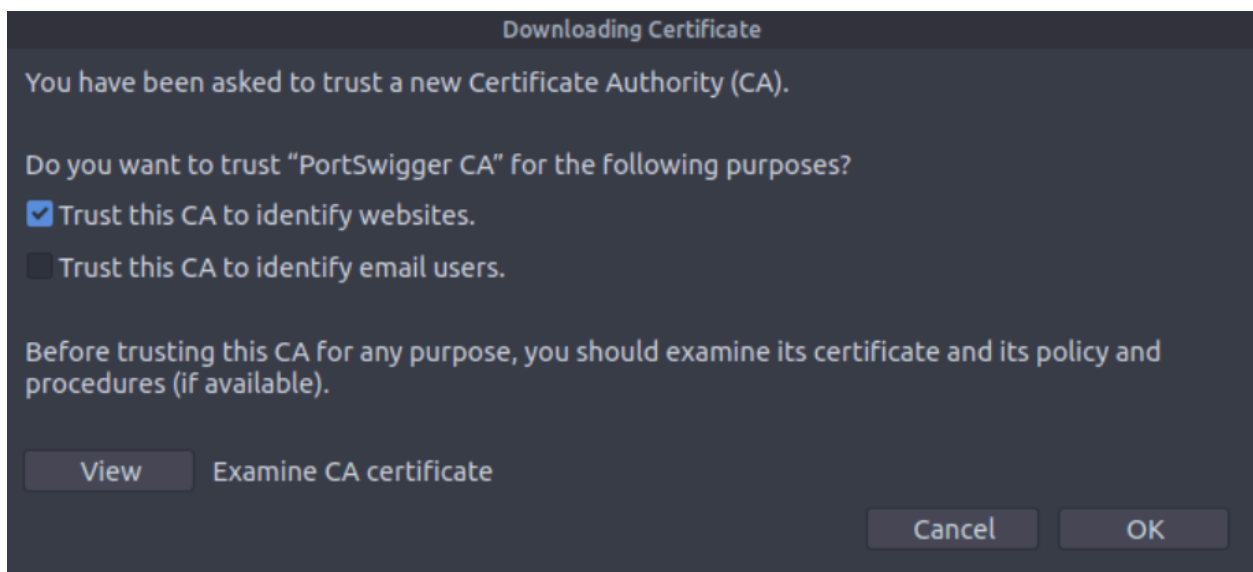
1- **Download the CA Certificate** (CA Sertifikasını indirin): Burp Proxy etkinleştirildiğinde, <http://burp/cert> adresine gidin. Bu, cacert.der adlı bir dosya indirecektir. Bu dosyayı makinenizde bir yere kaydedin.

2- **Access Firefox Certificate Settings** (Firefox Sertifika Ayarları'na erişin): Firefox URL çubuğuna about:preferences yazın ve Enter tuşuna basın. Bu sizi Firefox ayarları sayfasına götürecektir. Sayfada "sertifikalar" için arama yapın ve Sertifikaları Görüntüle düğmesine tıklayın.



3-Import the CA Certificate (CA Sertifikasını içe aktarın): Sertifika Yöneticisi penceresinde, İçe Aktar düğmesine tıklayın. Bir önceki adımda indirdiğiniz cacert.der dosyasını seçin.

4- Set Trust for the CA Certificate (CA Sertifikası için Güven'i ayarlayın): Daha sonra açılan pencerede "Web sitelerini tanımlamak için bu CA'ya güven" yazan kutuyu işaretleyin ve Tamam'a tıklayın.



Bu adımları tamamlayarak PortSwigger CA sertifikasını güvenilir sertifika yetkilileri listemize eklemiş olduk. Artık TLS özellikli herhangi bir siteyi sertifika hatasıyla karşılaşmadan ziyaret edebilmeliyiz.

Bu talimatları izleyerek, tarayıcınızın PortSwigger CA sertifikasına güvenmesini ve Burp Suite Proxy aracılığıyla TLS özellikli web siteleriyle güvenli bir şekilde iletişim kurmasını sağlayabilirsiniz.

sorular;

AttackBox kullanmıyorsanız, Firefox'u (veya tercih ettiğiniz tarayıcıyı) Burp Proxy üzerinden TLS iletişimi için PortSwigger CA sertifikasını kabul edecek şekilde yapılandırın.

cevap ⇒ **Cevap Gerekmemektedir.**

Task 14 Example Attack (Görev 14 Örnek Saldırı)

Proxy'mizi nasıl kuracağımızı ve yapılandıracağımızı inceledikten sonra, basitleştirilmiş bir gerçek dünya örneği üzerinden gidelim.

İşe `http://MACHINE_IP/ticket/` adresindeki destek formuna göz atarak başlayacağız:

Support

Contact Email:

Type your query here:

Submit Query!

Gerçek dünyadaki bir web uygulaması pentestinde, bunu çeşitli şeyler için test ederiz, bunlardan biri de Siteler Arası Komut Dosyası Yazma (veya XSS) olacaktır. XSS ile henüz karşılaşmadıysanız, bir web sayfasına yürütülecek şekilde istemci tarafında bir komut dosyası (genellikle Javascript) enjekte etmek olarak düşünülebilir. Çeşitli XSS türleri vardır - burada kullandığımız tür, yalnızca web isteğini yapan kişiyi etkilediği için "Yansıtılmış" XSS olarak adlandırılır.

Walkthrough

Yazmayı deneyin: `<script>alert("Succ3ssful XSS")</script>`, "İletişim E-postası" alanına. E-posta adreslerinde izin verilmeyen herhangi bir özel karakter eklemenizi engelleyen bir istemci tarafı filtresi olduğunu göreceksiniz:

Support

Contact Email:

Type your query here:

Submit Query!

Neyse ki istemci tarafı filtreleri atlatmak son derece kolay. Komut dosyasını devre dışı bırakmanın ya da ilk etapta yüklenmesini engellemenin çeşitli yolları vardır.

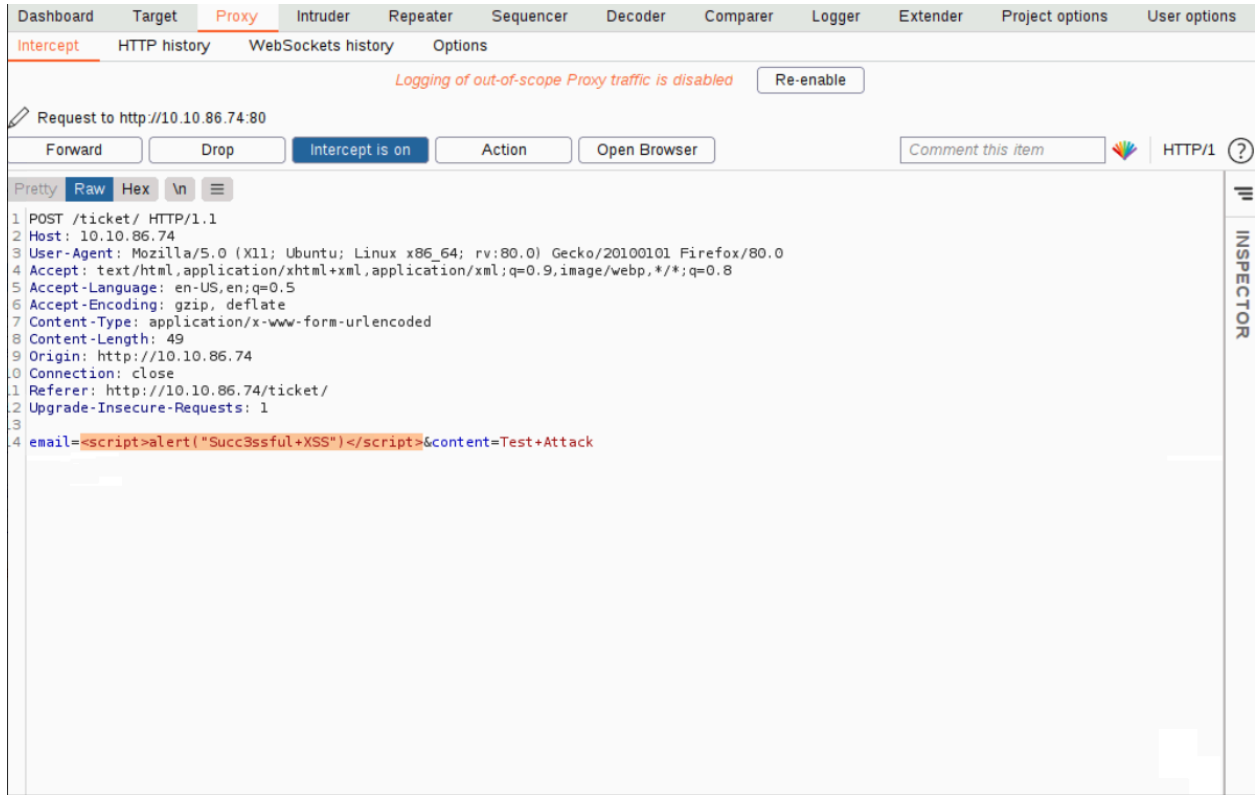
Şimdilik sadece filtreyi atlamaya odaklanalım.

İlk olarak, Burp Proxy'nizin etkin olduğundan ve kesmenin açık olduğundan emin olun.

Şimdi, destek formuna bazı meşru veriler girin. Örneğin: E-posta adresi olarak "pentester@example.thm" ve sorgu olarak "Test Saldırısı".

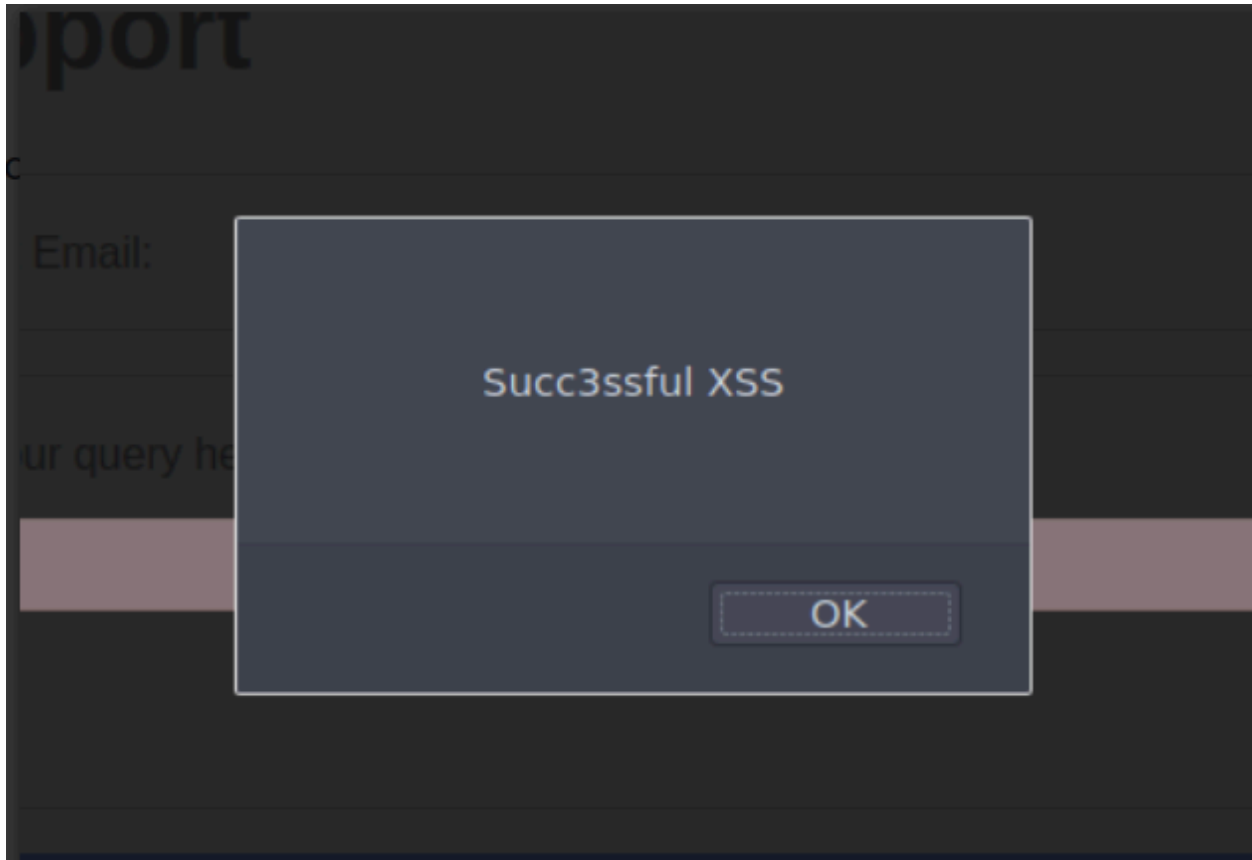
Formu gönderin - istek proxy tarafından durdurulmalıdır.

Proxy'de yakalanan istekle, şimdi e-posta alanını yukarıdaki çok basit yükümüz olacak şekilde değiştirebiliriz: <script>alert("Succ3ssful XSS")</script>. Yükü yapıştırdıktan sonra, onu seçmemiz ve ardından göndermek için güvenli hale getirmek için Ctrl + U kısayoluyla URL kodlamamız gerekir. Bu işlem aşağıdaki GIF'te gösterilmektedir:



Son olarak, talebi göndermek için "İlet" düğmesine basın.

Sitede başarılı bir XSS saldırısını gösteren bir uyarı kutusu bulmalısınız!



sorular;

Soru

cevap⇒ **Cevap Gerekmemektedir.**

Task 15 Conclusion (Görev 15 Sonuç)

Burp Temelleri odasını tamamladığınız için tebrikler! Artık Burp Suite arayüzü, yapılandırma seçenekleri ve Burp Proxy hakkında sağlam bir anlayışa sahipsiniz. Bu beceriler, web ve mobil uygulama sızma testi yolculuğunuza devam ederken çok önemli olacaktır.

Becerilerinizi daha da geliştirmek için Burp Suite ile pratik yapmanızı ve denemeler yapmanızı öneririm. Özelliklerini keşfedin, farklı konfigürasyonlar deneyin ve çeşitli araçlarına aşina olun. Burp Suite'i ne kadar çok kullanırsanız, web

uygulamalarındaki güvenlik açıklarını belirleme ve bunlardan yararlanma konusunda o kadar yetkin hale geleceksiniz.

Modülün bir sonraki odasında, web uygulama isteklerinin manuel olarak test edilmesi ve manipüle edilmesi için bir başka güçlü araç olan Burp Suite Repeater'ı daha derinlemesine inceleyeceğiz. Meraklı kalın ve öğrenmeye devam edin!

Meraklı kalın ve öğrenmeye devam edin!

sorular;

soru

cevap ⇒ **Cevap Gerekmemektedir.**