Burp Suite: Intruder

Task 1 Introduction (Görev 1 Giriş)

Burp Suite Davetsiz Misafir odasına hoş geldiniz!

Bu odada, Burp Suite'in otomatik istek manipülasyonu sunan ve fuzzing ve brute-forcing gibi görevleri mümkün kılan Intruder modülünü keşfedeceğiz. Burp Suite'in Proxy ve Repeater işlevlerine aşina değilseniz, devam etmeden önce en azından Burp Basics odasını tamamlamanız önerilir.

Burp Suite'in Intruder modülü, otomatik ve özelleştirilebilir saldırılara olanak tanıyan güçlü bir araçtır. Bir isteğin belirli bölümlerini değiştirme ve girdi verilerinin varyasyonları ile tekrarlayan testler gerçekleştirme yeteneği sağlar. Intruder, bir hedefe karşı farklı değerlerin test edilmesi gereken fuzzing ve brute-forcing gibi görevler için özellikle yararlıdır.

Yeşil Makineyi Başlat düğmesine basarak bu göreve bağlı hedef sanal makineyi dağıtın. Ayrıca, kendi makinenizi kullanmıyorsanız, bu odanın üst kısmındaki mavi Start AttackBox düğmesine basarak AttackBox'ı başlatın. Ardından Burp'ü başlatın ve sonraki görevleri takip edin.

Hadi başlayalım!

Cevap Gerekmemektedir.

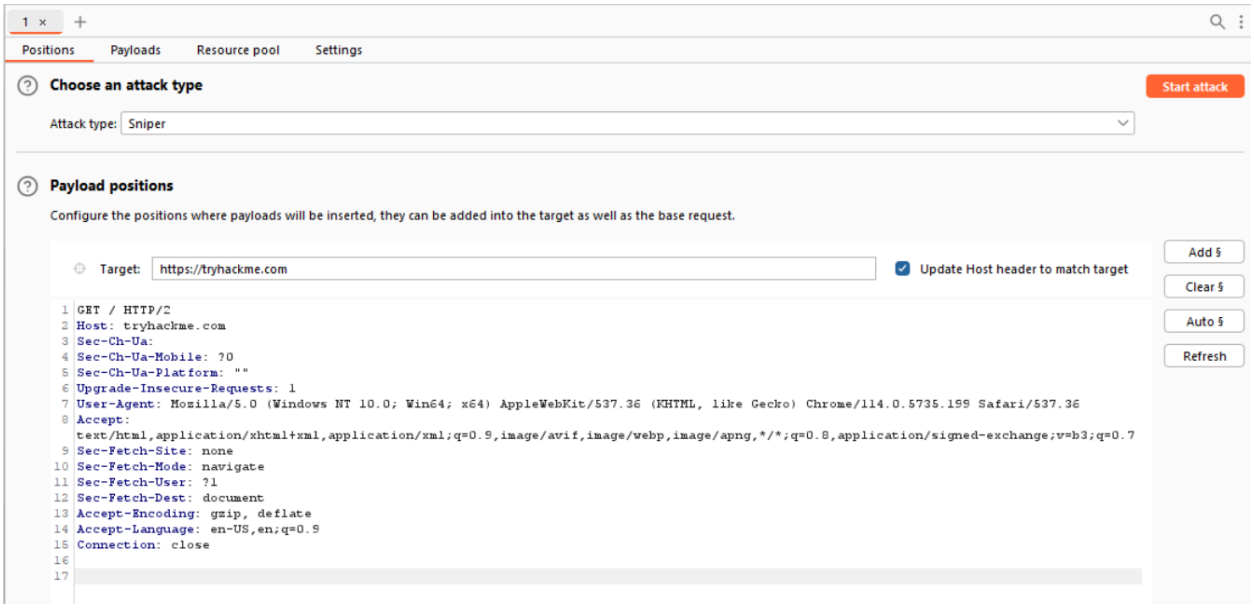
Task 2 What is Intruder (Görev 2 Intruder nedir)

Intruder, Burp Suite'in otomatik istek modifikasyonuna ve girdi değerlerindeki varyasyonlarla tekrarlayan testlere olanak tanıyan yerleşik bulanıklaştırma aracıdır. Intruder, yakalanan bir isteği (genellikle Proxy modülünden) kullanarak, kullanıcı tanımlı yapılandırmalara dayalı olarak biraz değiştirilmiş değerlerle birden fazla istek gönderebilir. Kullanıcı adı ve parola alanlarını bir kelime listesindeki değerlerle değiştirerek oturum açma formlarını kaba kuvvetle zorlamak veya alt dizinleri, uç

noktaları veya sanal ana bilgisayarları test etmek için kelime listelerini kullanarak bulanıklaştırma saldırıları gerçekleştirmek gibi çeşitli amaçlara hizmet eder. Intruder'ın işlevselliği Wfuzz veya ffuf gibi komut satırı araçlarıyla karşılaştırılabilir.

Bununla birlikte, Intruder'ın Burp Community Edition ile kullanılabilmesine rağmen, Burp Professional'a kıyasla hızını önemli ölçüde düşüren hız sınırlı olduğunu belirtmek önemlidir. Bu sınırlama genellikle güvenlik uygulayıcılarının fuzzing ve brute-forcing için diğer araçlara güvenmesine neden olur. Bununla birlikte, Intruder değerli bir araç olmaya devam etmektedir ve nasıl etkili bir şekilde kullanılacağını öğrenmeye değer.

Intruder arayüzünü keşfedelim:



Intruder'ın ilk görünümü hedefimizi seçebileceğimiz basit bir arayüz sunar. Proxy'den bir istek gönderildiyse bu alan zaten doldurulmuş olacaktır (Ctrl + I kullanılarak veya sağ tıklayıp "Davetsiz Misafir'e Gönder" seçilerek).

Davetsiz Misafir içinde dört alt sekme vardır:

- **Positions (**Pozisyonlar): Bu sekme, bir saldırı türü seçmemize (gelecekteki bir görevde ele alacağız) ve yüklerimizi istek şablonunda nereye eklemek istediğimizi yapılandırmamıza olanak tanır.
- **Payloads** (Yükler): Burada, Pozisyonlar sekmesinde tanımlanan pozisyonlara eklenecek değerleri seçebiliriz. Bir kelime listesinden öğeler yüklemek gibi

çeşitli yük seçeneklerimiz vardır. Bu yüklerin şablona eklenme şekli, Pozisyonlar sekmesinde seçilen saldırı türüne bağlıdır. Payloads sekmesi ayrıca her bir payload için ön işleme kuralları tanımlamak gibi Intruder'ın payload'larla ilgili davranışını değiştirmemizi sağlar (örneğin, bir önek veya sonek ekleme, eşleştirme ve değiştirme gerçekleştirme veya tanımlanmış bir regex'e dayalı olarak payload'ları atlama).

- **Resource Pool (**Kaynak Havuzu): Bu sekme Burp Community Edition'da özellikle kullanışlı değildir. Burp Professional'daki çeşitli otomatik görevler arasında kaynak tahsisine izin verir. Bu otomatik görevlere erişim olmadan, bu sekmenin önemi sınırlıdır.
- **Settings** (Ayarlar): Bu sekme saldırı davranışını yapılandırmamızı sağlar. Öncelikle Burp'ün sonuçları ve saldırının kendisini nasıl ele aldığı ile ilgilidir. Örneğin, belirli bir metin içeren istekleri işaretleyebilir veya Burp'un yönlendirme (3xx) yanıtlarına vereceği yanıtı tanımlayabiliriz.

Not: "Fuzzing" terimi, bir parametreye bir dizi veri uygulayarak işlevselliği veya varlığı test etme sürecini ifade eder. Örneğin, bir web uygulamasındaki uç noktalar için bulanıklaştırma, bir kelime listesindeki her bir kelimeyi alıp sunucunun yanıtını gözlemlemek için bir istek URL'sine (ör. http://MACHINE_IP/WORD_GOES_HERE) eklemeyi içerir

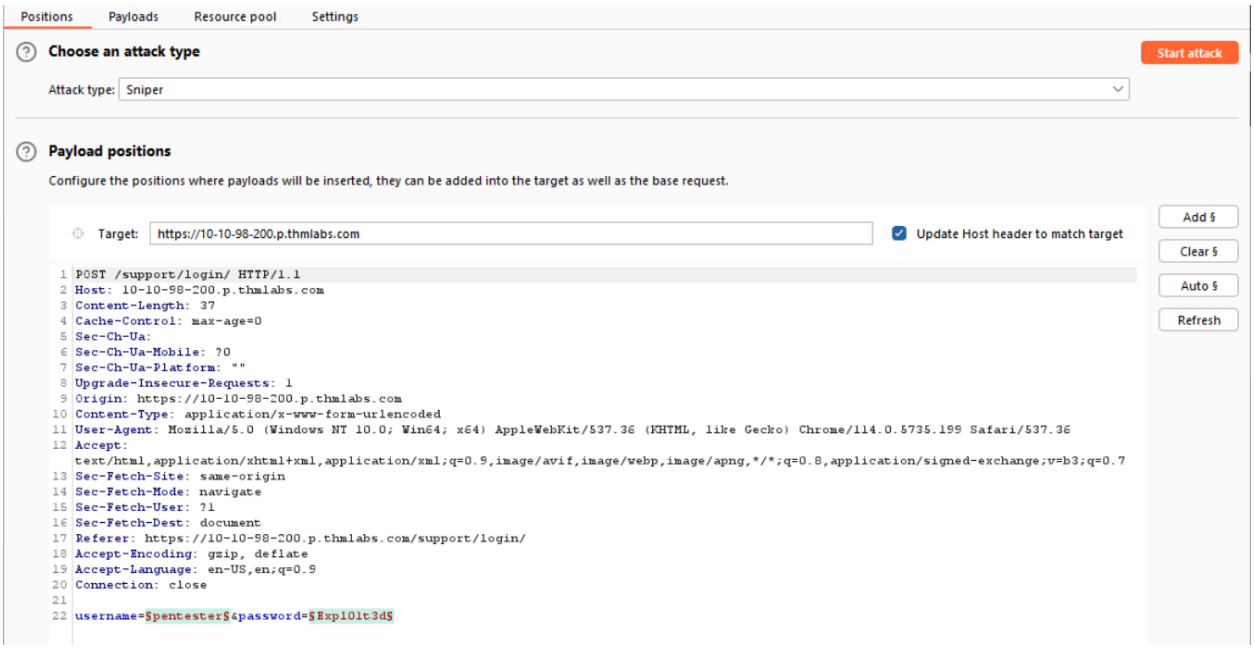
soru ⇒ Planladığımız saldırı için "Saldırı türünü" hangi Saldırgan sekmesinde tanımlayabiliriz?

Cevap ⇒ Positions

Task 3 Positions (Görev 3 Pozisyonları)

Bir saldırı gerçekleştirmek için Burp Suite Intruder'ı kullanırken, ilk adım, yüklerimizi eklemek istediğimiz istek içindeki konumları incelemektir. Bu konumlar, Intruder'a yüklerimizin ekleneceği konumlar hakkında bilgi verir (ilerleyen görevlerde inceleyeceğimiz gibi).

Pozisyonlar sekmesine gidelim:

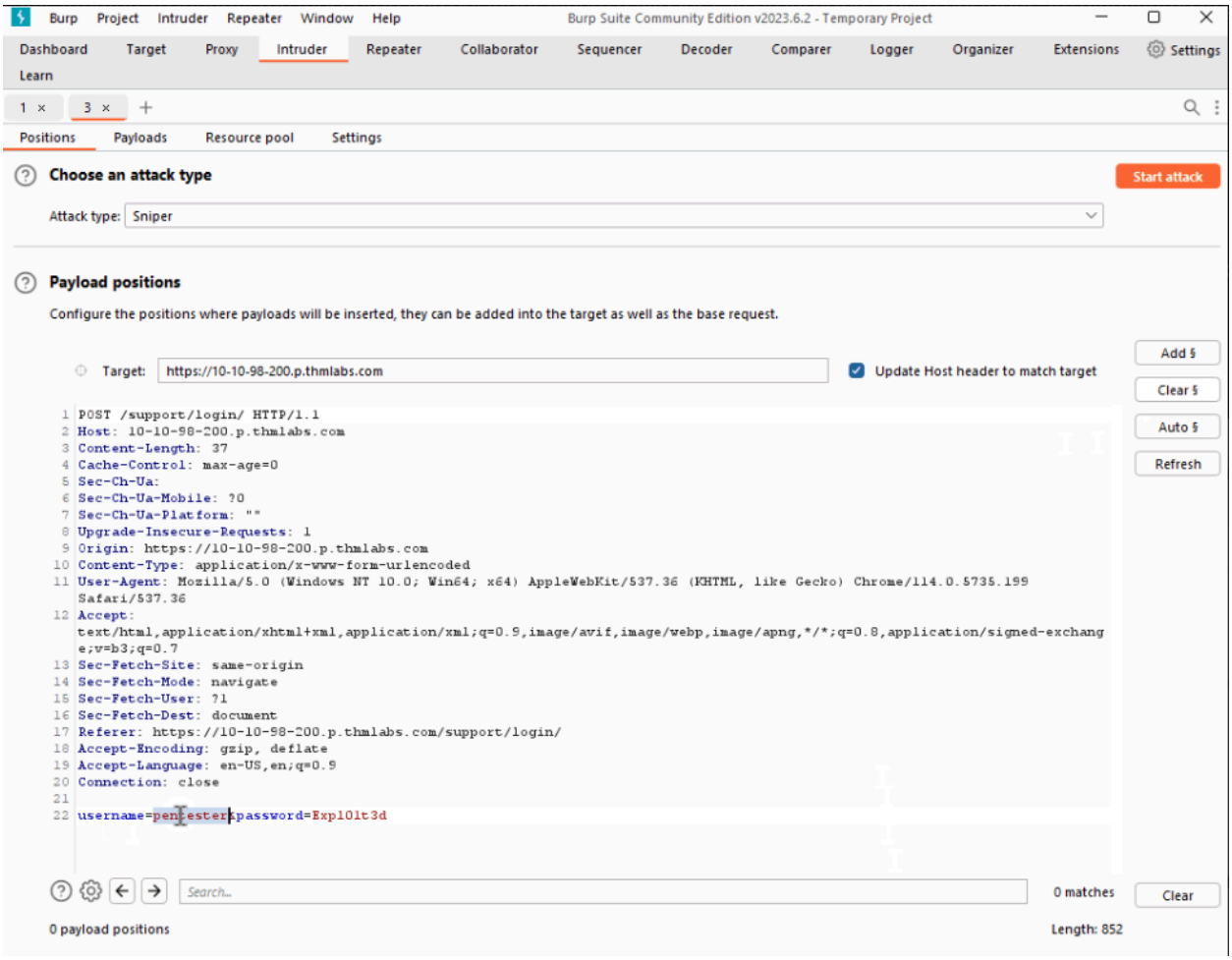


Burp Suite'in otomatik olarak faydalı yüklerin yerleştirilebileceği en olası konumları belirlemeye çalıştığına dikkat edin. Bu konumlar yeşil renkle vurgulanmış ve bölüm işaretleriyle (§) çevrelenmiştir.

Arayüzün sağ tarafında aşağıdaki düğmeleri buluyoruz: Ekle §, Temizle § ve Otomatik §:

- Add § düğmesi, istek düzenleyicide vurgulayarak ve ardından düğmeye tıklayarak yeni pozisyonları manuel olarak tanımlamamıza olanak tanır.
- Clear § düğmesi tüm tanımlı pozisyonları kaldırarak kendi pozisyonlarımızı tanımlayabileceğimiz boş bir tuval sağlar.
- Otomatik § düğmesi, talebe göre en olası konumları otomatik olarak belirlemeye çalışır. Bu özellik, daha önce varsayılan konumları temizlediysek ve bunları geri istiyorsak faydalıdır.

Aşağıdaki GIF pozisyon ekleme, silme ve otomatik olarak yeniden seçme işlemlerini göstermektedir:



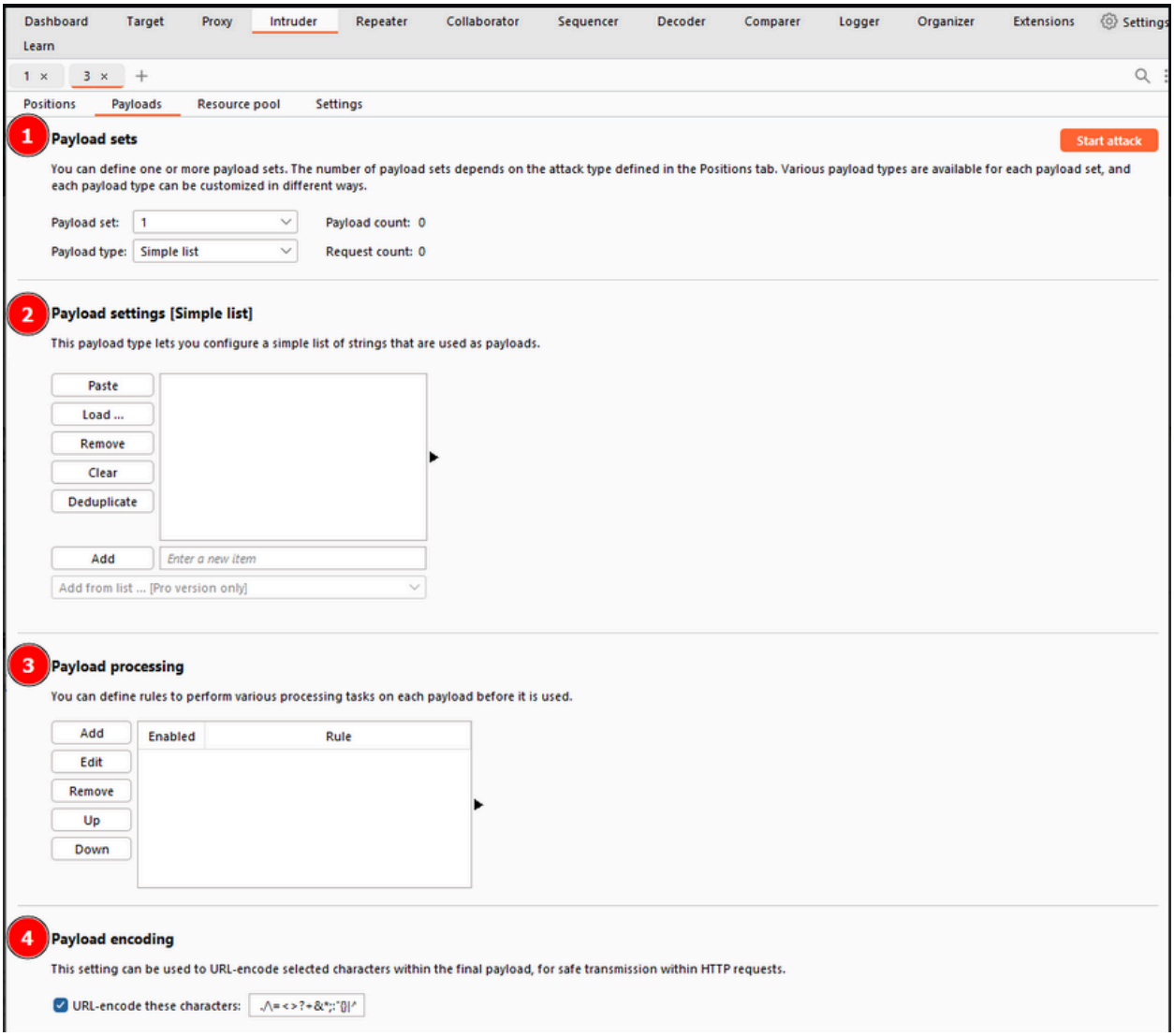
Burp Suite Intruder arayüzünü kullanarak pozisyon ekleme, silme ve otomatik seçme işlemlerine alışmak için biraz zaman ayırın.

soru ⇒ Bir yük pozisyonunun başlangıcını ve sonunu hangi sembol tanımlar?

Cevap⇒ §

Task 4 Payloads (Görev 4 Faydalı Yükler)

Burp Suite Intruder'ın Payloads sekmesinde, saldırımız için payload'lar oluşturabilir, atayabilir ve yapılandırabiliriz. Bu alt sekme dört bölüme ayrılmıştır:



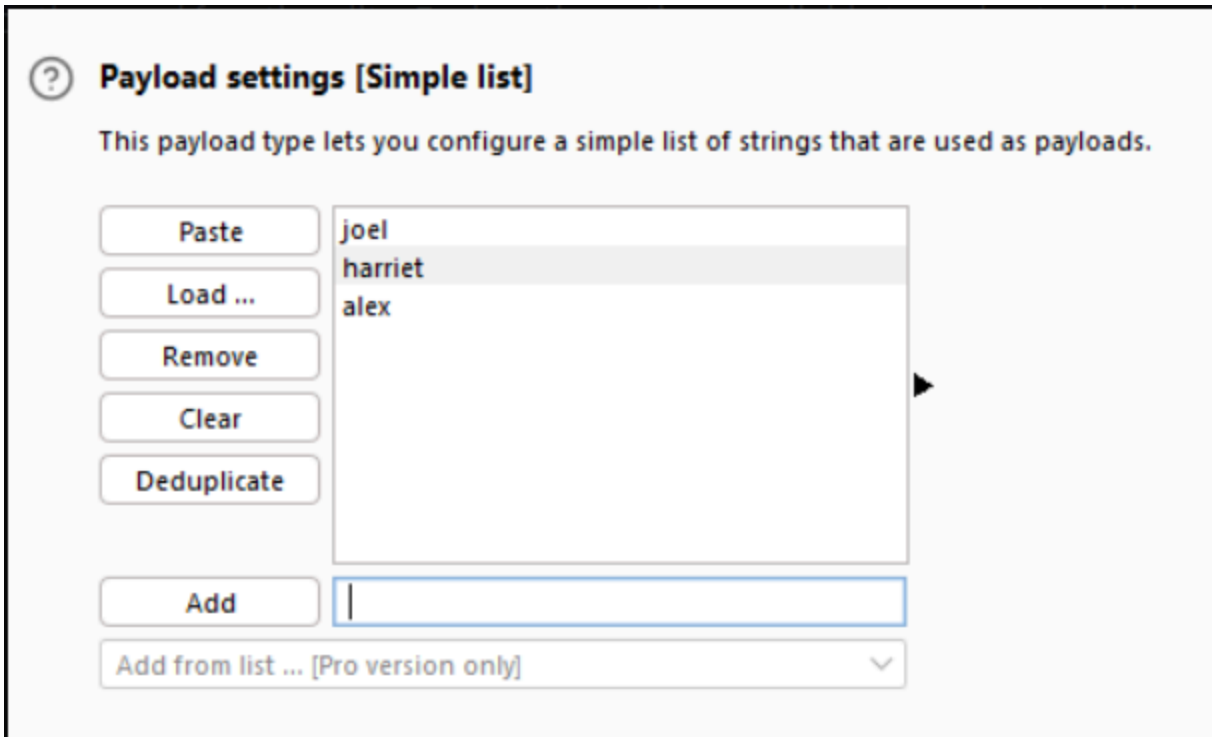
1. **Payload sets (Yük Setleri:)**

- Bu bölüm, bir yük setini yapılandırmak istediğimiz konumu seçmemize ve kullanmak istediğimiz yük türünü seçmemize olanak tanır.
- Yalnızca tek bir yük setine izin veren saldırı türlerini kullanırken (Keskin Nişancı veya Koçbaşı), "Yük Seti" açılır menüsünde tanımlı konum sayısına bakılmaksızın yalnızca bir seçenek olacaktır.
- Birden fazla yük seti gerektiren saldırı türleri kullanırsak (Pitchfork veya Cluster Bomb), açılır menüde her konum için bir öğe olacaktır.
- Not: Birden fazla pozisyon için "Payload Set" açılır menüsünde numaralar atarken, yukarıdan aşağıya, soldan sağa bir sıra izleyin. Örneğin, iki konumla

(username=§pentester§&password=§Expl01ted§), payload set açılır menüsündeki ilk öğe kullanıcı adı alanına, ikinci öğe ise parola alanına karşılık gelecektir.

2. **Payload Settings (Payload ayarları:)**

- Bu bölüm, geçerli yük seti için seçilen yük tipine özgü seçenekler sunar.
- Örneğin, "Basit liste" yükü türünü kullanırken, Ekle metin kutusunu, Satırları yapıştır veya Bir dosyadan yük yükle düğmelerini kullanarak yükleri kümeye manuel olarak ekleyebilir veya kümeden kaldırabiliriz. Kaldır düğmesi o anda seçili olan satırı kaldırır ve Temizle düğmesi tüm listeyi temizler. Burp'ün çökmesine neden olabileceğinden, büyük listeler yüklerken dikkatli olun.
- Her yük tipinin kendine özgü seçenekleri ve işlevleri olacaktır. Olasılıklar yelpazesini anlamak için mevcut seçenekleri keşfedin.



3. **Payload Processing(Yük İşleme:)**:

- Bu bölümde, hedefe gönderilmeden önce setteki her bir yüke uygulanacak kuralları tanımlayabiliriz.

- Örneğin, her kelimeyi büyük harfle yazabilir, bir regex deseniyle eşleşen yükleri atlayabilir veya başka dönüşümler ya da filtrelemeler uygulayabiliriz.
- Bu bölümü sık kullanmasanız da, saldırınız için belirli bir yük işleme gerektiğinde oldukça değerli olabilir.

4. **Payload Encoding (Yük Kodlaması):**

- Bu bölüm, yüklerimiz için kodlama seçeneklerini özelleştirmemize olanak tanır.
- Varsayılan olarak Burp Suite, yüklerin güvenli bir şekilde iletilmesini sağlamak için URL kodlaması uygular. Ancak, kodlama davranışını ayarlamak istediğimiz durumlar olabilir.
- Kodlanacak karakterlerin listesini değiştirerek veya "URL-encode these characters" onay kutusunun işaretini kaldırarak varsayılan URL kodlama seçeneklerini geçersiz kılabiliriz.

Bu bölümlerden yararlanarak, saldırılarımızın özel gereksinimlerine uyacak şekilde yük setleri oluşturabilir ve özelleştirebiliriz. Bu kontrol seviyesi, etkili test ve istismar için yüklerimizi hassas bir şekilde ayarlamamıza olanak tanır.

Soru ⇒ Kümedeki her bir yükün sonuna karakter eklemek için hangi Yük işleme kuralını kullanabiliriz?

Cevap ⇒ Add suffix

Task 5 Introduction to Attack Types (Görev 5 Saldırı Türlerine Giriş)

Burp Suite Intruder'ın Pozisyonlar sekmesinde saldırı türünü seçmek için bir açılır menü vardır. Intruder, her biri belirli bir amaca hizmet eden dört saldırı türü sunar. Şimdi her birini inceleyelim:

1. **Sniper** (Keskin Nişancı): Sniper saldırı türü varsayılan ve en yaygın kullanılan seçenektir. Her seferinde bir yükü istekte tanımlanan her konuma ekleyerek yükler arasında geçiş yapar. Sniper saldırıları, tüm yükleri doğrusal bir şekilde yineleyerek hassas ve odaklanmış testlere olanak tanır.
2. **Battering ram** (Koçbaşı): Koçbaşı saldırı türü, Sniper'dan farklı olarak tüm yükleri aynı anda gönderir ve her yük kendi konumuna yerleştirilir. Bu saldırı

türü, yarış koşullarını test ederken veya yüklerin eşzamanlı olarak gönderilmesi gerektiğinde kullanışlıdır.

3. **Pitchfork** (Pitchfork): Pitchfork saldırı türü, farklı yüklerle birden fazla konumun aynı anda test edilmesini sağlar. Test edenin, her biri istekte belirli bir konumla ilişkilendirilmiş birden fazla yük seti tanımlamasına olanak tanır. Pitchfork saldırıları, ayrı ayrı test edilmesi gereken farklı parametreler olduğunda etkilidir.
4. **Cluster bomb (**Salkım bombası): Salkım bombası saldırı türü Sniper ve Pitchfork yaklaşımlarını birleştirir. Her pozisyona Sniper benzeri bir saldırı gerçekleştirir ancak aynı anda her kümedeki tüm yükleri test eder. Bu saldırı türü, birden fazla konumun farklı yükleri olduğunda ve hepsini birlikte test etmek istediğimizde kullanışlıdır.

Her saldırı türünün avantajları vardır ve farklı test senaryoları için uygundur. Aralarındaki farkları anlamak, test hedeflerine göre uygun saldırı türünü seçmemize yardımcı olur.

Soru ⇒ Hangi saldırı türü, istekte tanımlanan her konuma bir seferde bir yük ekleyerek yükler arasında geçiş yapar?

Cevap ⇒ Sniper

Task 6 Sniper (Görev 6 Keskin Nişancı)

Sniper saldırı türü, Burp Suite Intruder'da varsayılan ve en yaygın kullanılan saldırı türüdür. Özellikle API uç noktaları için parola kaba kuvvet veya fuzzing gibi tek konumlu saldırılar için etkilidir. Bir Sniper saldırısında, bir kelime listesi veya sayı aralığı olabilen bir dizi yük sağlarız ve Intruder her bir yükü istekte tanımlanan her konuma ekler.

Daha önce kullandığımız örnek şablona geri dönelim:

Example Positions

```
POST /support/login/ HTTP/1.1
Host: MACHINE_IP
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
Origin: http://MACHINE_IP
Connection: close
Referer: http://MACHINE_IP/support/login/
Upgrade-Insecure-Requests: 1

username=§pentester§&password=§Expl01ted§
```

Bu örnekte, kullanıcı adı ve parola gövde parametreleri için tanımlanmış iki konumumuz vardır. Bir Sniper saldırısında, Saldırgan her bir yükü yük setinden alır ve sırayla tanımlanan her bir konuma yerleştirir.

Üç kelimelik bir kelime listemiz olduğunu varsayarsak: burp, suite ve intruder, Intruder altı istek oluşturacaktır:

Request Number	Request Body
1	username=burp&password=Expl01ted
2	username=suite&password=Expl01ted
3	username=intruder&password=Expl01ted
4	username=pentester&password=burp
5	username=pentester&password=suite
6	username=pentester&password=intruder

Intruder'ın ilk pozisyonla (kullanıcı adı) nasıl başladığını ve her bir yükü bu pozisyonla nasıl değiştirdiğini, ardından ikinci pozisyona (şifre) nasıl geçtiğini ve yüklerle aynı değiştirmeyi nasıl gerçekleştirdiğini gözlemleyin. Intruder Sniper tarafından yapılan toplam istek sayısı, requests = numberOfWords * numberOfPositions olarak hesaplanabilir.

Sniper saldırı türü, her pozisyon için farklı faydalı yükler kullanarak tek pozisyonlu saldırılarla testler yapmak istediğimizde faydalıdır. Farklı faydalı yük

varyasyonlarının hassas bir şekilde test edilmesine ve analiz edilmesine olanak tanır.

Sorular;

Soru ⇒ Sniper'ı 100 kelime içeren bir kelime listesine sahip bir istekte üç parametreyi bulanıklaştırmak için kullanıyor olsaydınız, Burp Suite'in saldırıyı tamamlamak için kaç istek göndermesi gerekirdi?

Cevap ⇒ 300

Soru ⇒ Sniper bir saldırı gerçekleştirmek için kaç yük setini kabul edecek?

Cevap ⇒ 1

Task 7 Battering Ram (Görev 7 Koçbaşı)

Burp Suite Intruder'daki koçbaşı saldırı türü, her bir yükü sırayla her bir konuma yerleştirmek yerine aynı yükü her konuma aynı anda yerleştirmesi bakımından Sniper'dan farklıdır.

Önceki örnek şablonumuza geri dönelim:

Example Positions

```
POST /support/login/ HTTP/1.1
    Host: MACHINE_IP
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
    Accept-Language: en-US,en;q=0.5
    Accept-Encoding: gzip, deflate
    Content-Type: application/x-www-form-urlencoded
    Content-Length: 37
    Origin: http://MACHINE_IP
    Connection: close
    Referer: http://MACHINE_IP/support/login/
    Upgrade-Insecure-Requests: 1

    username=§pentester§&password=§Expl01ted§
```

Öncekiyle aynı kelime listesiyle (burp, suite ve intruder) Battering Ram saldırı türünü kullanan Intruder üç istek oluşturacaktır:

Request Number	Request Body
1	username=burp&password=burp
2	username=suite&password=suite
3	username=intruder&password=intruder

Tabloda gösterildiği gibi, kelime listesindeki her yük, yapılan her istek için her konuma eklenir. Koçbaşı saldırısında, aynı yük tanımlanan her konuma aynı anda atılır ve test için kaba kuvvet benzeri bir yaklaşım sağlar.

Battering Ram saldırı türü, aynı yükü sıralı ikameye gerek kalmadan aynı anda birden fazla pozisyona karşı test etmek istediğimizde kullanışlıdır.

Gelecek görevlerde, Saldırganın Koçbaşı saldırı türüyle ilgili diğer yapılandırmaları ve ayarları keşfedeceğiz ve farklı senaryolardaki uygulamalarını inceleyeceğiz.

Varsayımsal bir soru olarak: Yukarıdaki örnek talebe bir Koçbaşı İzinsiz Giriş saldırısı gerçekleştirmeniz gerekiyor.

İçinde iki kelime (admin ve Guest) olan bir kelime listeniz varsa ve istek şablonundaki konumlar aşağıdaki gibi görünüyorsa:

`username=§pentester§&password=§Expl01ted§`

Soru ⇒ Burp Suite'in gönderdiği ilk isteğin gövde parametreleri ne olmalıdır(İpucu ⇒ Cevabınızı şu şekilde gönderin: username=PAYLOAD&password=PAYLOAD)?

Cevap ⇒ username=admin&password=admin

Task 8 Pitchfork (Görev 8 Pitchfork)

Burp Suite Intruder'daki Pitchfork saldırı türü, aynı anda çalışan birden fazla Sniper saldırısına benzer. Sniper tüm pozisyonları aynı anda test etmek için bir yük seti kullanırken, Pitchfork pozisyon başına bir yük seti kullanır (maksimum 20'ye kadar) ve hepsini aynı anda yineler.

Pitchfork'u daha iyi anlamak için kaba kuvvet örneğimizi tekrar ele alalım, ancak bu kez iki kelime listesi kullanalım:

1. İlk kelime listesi kullanıcı adlarını içerir: joel, harriet ve alex.
2. İkinci kelime listesi şifreleri içerir: J03l, Emma1815 ve Sk1ll.

Bu iki listeyi oturum açma formuna bir Pitchfork saldırısı gerçekleştirmek için kullanabiliriz. Saldırı sırasında yapılan her istek şu şekilde görünecektir:

Request Number	Request Body
1	username=joel&password=J03l
2	username=harriet&password=Emma1815
3	username=alex&password=Sk1ll

Tabloda gösterildiği gibi, Pitchfork her listeden ilk öğeyi alır ve her pozisyon için bir tane olmak üzere bunları istekle değiştirir. Daha sonra bu işlemi her listeden ikinci öğeyi alıp şablona yerleştirerek bir sonraki istek için tekrarlar. Intruder bu yinelemeyi listelerden birinde veya tümünde öğe kalmayana kadar sürdürür. Intruder'ın listelerden biri tamamlanır tamamlanmaz testi durdurduğuna dikkat etmek önemlidir. Bu nedenle, Pitchfork saldırılarında, yük setlerinin aynı uzunlukta olması idealdir. Yük setlerinin uzunlukları farklıysa, Saldırgan yalnızca kısa liste tükenene kadar istekte bulunacak ve uzun listede kalan öğeler test edilmeyecektir.

Pitchfork saldırı türü özellikle kimlik bilgisi doldurma saldırıları gerçekleştirirken veya birden fazla pozisyon ayrı yük setleri gerektirdiğinde kullanışlıdır. Farklı yüklerle birden fazla pozisyonun aynı anda test edilmesine olanak tanır.

Gelecek görevlerde, Intruder'ın Pitchfork saldırı türüyle ilgili diğer yapılandırmaları ve ayarları inceleyeceğiz ve kimlik bilgisi doldurma saldırıları da dahil olmak üzere farklı senaryolardaki uygulamalarını keşfedeceğiz.

Soru ⇒ Pitchfork modunda Intruder'a yükleyebileceğimiz maksimum yük seti sayısı nedir?

Cevap ⇒ 20

Task 9 Cluster Bomb (Görev 9 Misket Bombası)

Burp Suite Intruder'daki Cluster bomb saldırı türü, her pozisyon için bir tane olmak üzere birden fazla faydalı yük seti seçmemize olanak tanır (maksimum 20'ye kadar). Tüm faydalı yük setlerinin aynı anda test edildiği Pitchfork'un aksine, Cluster bomb her faydalı yük setini ayrı ayrı yineleyerek olası her faydalı yük kombinasyonunun test edilmesini sağlar.

Salkım bombası saldırı türünü göstermek için, daha önce olduğu gibi aynı kelime listelerini kullanalım:

- Kullanıcı adları: Joel, Harriet ve Alex.
- Şifreler: J03l, Emma1815, ve Sk1ll.

Bu örnekte, hangi parolanın hangi kullanıcıya ait olduğunu bilmediğimizi varsayalım. Üç kullanıcımız ve üç parolamız var, ancak eşleştirmeler bilinmiyor. Bu durumda, her değer kombinasyonunu denemek için bir Cluster bomb saldırısı kullanabiliriz. Kullanıcı adı ve şifre pozisyonlarımız için istek tablosu aşağıdaki gibi görünecektir:

Request Number	Request Body
1	`username=joel&password=J03l`
2	`username=harriet&password=J03l`
3	`username=alex&password=J03l`
4	`username=joel&password=Emma1815`
5	`username=harriet&password=Emma1815`
6	`username=alex&password=Emma1815`
7	`username=joel&password=Sk1ll`
8	`username=harriet&password=Sk1ll`
9	`username=alex&password=Sk1ll`

Tabloda gösterildiği gibi, Küme bombası saldırı türü, sağlanan yük setlerinin her kombinasyonunu yineler. Her bir yük kümesindeki her bir değeri istekte karşılık gelen konuma yerleştirerek her olasılığı test eder.

Küme bombası saldırıları her kombinasyonu test ettiği için önemli miktarda trafik oluşturabilir. Bir Küme bombası saldırısı tarafından yapılan istek sayısı, her bir yük kümesindeki satır sayısı çarpılarak hesaplanabilir. Bu saldırı türünü kullanırken, özellikle de büyük yük setleriyle uğraşırken dikkatli olmak önemlidir. Ek olarak, Burp Topluluğu ve Intruder hız sınırlaması kullanıldığında, orta büyüklükte bir yük setine sahip bir Cluster bomb saldırısının yürütülmesi önemli ölçüde daha uzun sürebilir.

Küme bombası saldırı türü, kullanıcı adları ve parolalar arasındaki eşlemenin bilinmediği kimlik bilgisi zorlama senaryoları için özellikle kullanışlıdır.

Gelecek görevlerde, Intruder'ın Küme bombası saldırı türüyle ilgili daha fazla yapılandırma ve ayar keşfedeceğiz ve farklı senaryolardaki uygulamalarını

inceleyeceğiz.

Üç yük setimiz var. İlk set 100 satır, ikincisi 2 satır ve üçüncüsü 30 satır içeriyor.

Soru ⇒ Intruder bir Misket bombası saldırısında bu yük setlerini kullanarak kaç talepte bulunacaktır(İpucu ⇒ Her bir yük setindeki satır sayısını birbiriyle çarpın. Çok küçük sayıların ne kadar hızlı toplanabildiğini görüyor musunuz?)?

Cevap ⇒ 6000

Task 10 Practical Example (Görev 10 Uygulama Örneği)

Teorik bilgilerimizi uygulamaya koymak için http://MACHINE_IP/support/login adresinde bulunan destek portalına erişim sağlamaya çalışacağız. Bu portal tipik bir giriş yapısını takip etmektedir ve kaynak kodunu incelediğimizde hiçbir koruyucu önlemin uygulanmadığını görüyoruz:

Support Login Form Source Code

```
---
<form method="POST">
    <div class="form-floating mb-3">
        <input class="form-control" type="text" name=username  placeholder="Username" required>
        <label for="username">Username</label>
    </div>
    <div class="form-floating mb-3">
        <input class="form-control" type="password" name=password  placeholder="Password" required>
        <label for="password">Password</label>
    </div>
    <div class="d-grid"><button class="btn btn-primary btn-lg" type="submit">Login!</button></div>
</form>
---
```

Koruyucu önlemlerin yokluğu göz önüne alındığında, bu formdan yararlanmak için kimlik bilgilerini kaba kuvvetle zorlamak için bir küme bombası saldırısı da dahil olmak üzere birçok seçeneğimiz var. Ancak, elimizde daha kolay bir yaklaşım var.

Yaklaşık üç ay önce Bastion Hosting, çalışanların kullanıcı adlarını, e-posta adreslerini ve düz metin şifrelerini ele geçiren bir siber saldırının kurbanı oldu. Etkilenen çalışanlara şifrelerini derhal değiştirmeleri talimatı verilmiş olsa da, bazılarının bu tavsiyeyi dikkate almamış olma ihtimali vardır.

Her birine karşılık gelen bir parolanın eşlik ettiği bilinen kullanıcı adlarının bir listesine sahip olduğumuz için, basit bir kaba kuvvet yerine bir kimlik bilgisi doldurma saldırısından yararlanabiliriz. Bu yöntem, özellikle Intruder'ın hız sınırlı sürümünü kullanırken avantajlı ve önemli ölçüde daha hızlıdır. Sızdırılan kimlik bilgilerine erişmek için, AttackBox'ta aşağıdaki komutu kullanarak dosyayı hedef makineden indirin: wget http://MACHINE_IP:9999/Credentials/BastionHostingCreds.zip

Tutorial

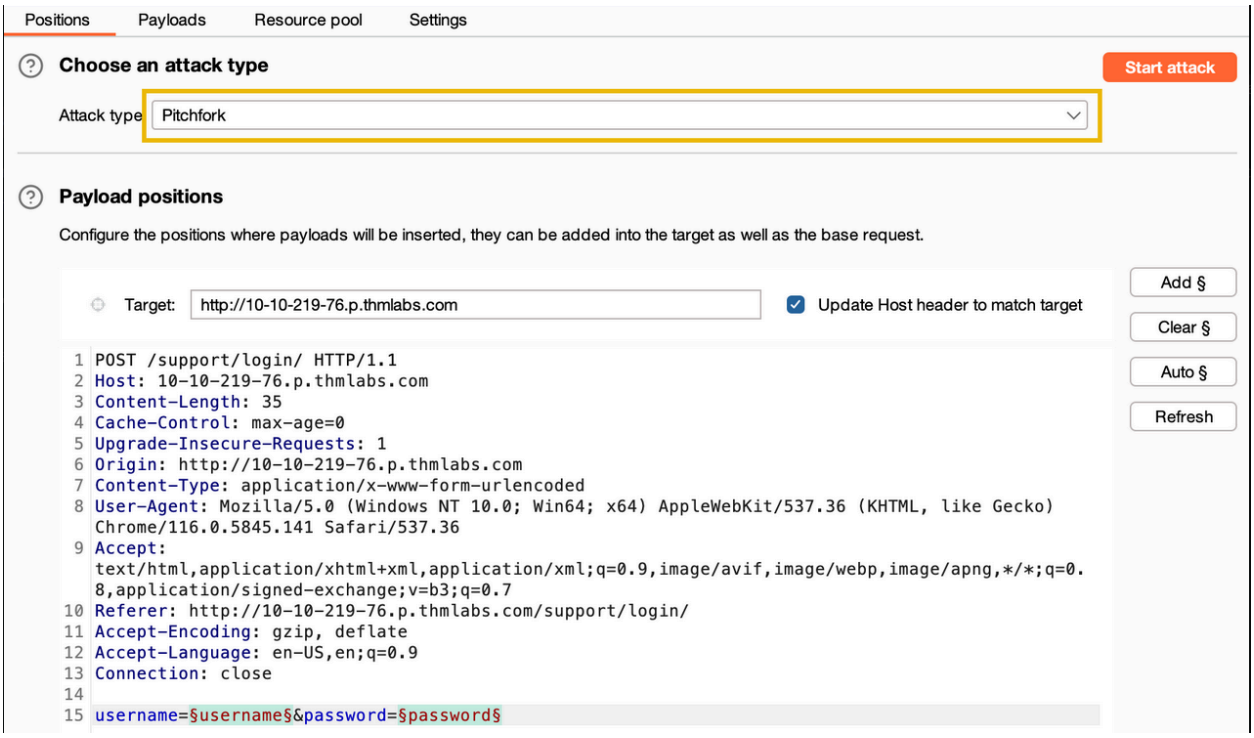
Bu örneği çözmek için Burp Makroları ile bir kimlik bilgisi doldurma saldırısı gerçekleştirmek üzere aşağıdaki adımları izleyin:

1. Kelime Listelerini İndirin ve Hazırlayın:

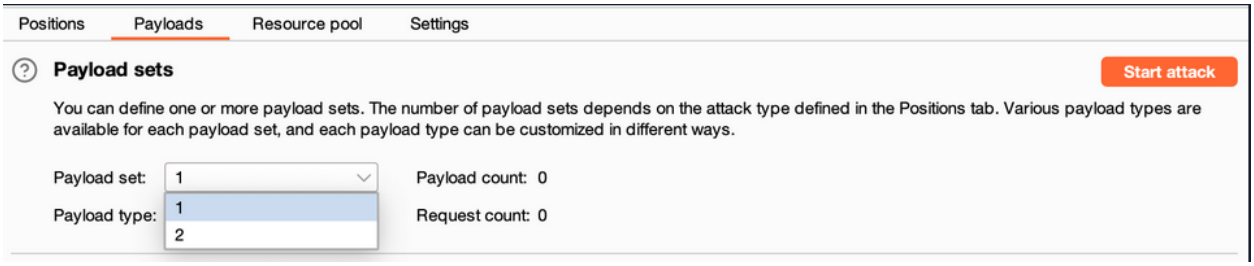
- emails.txt
- usernames.txt
- passwords.txt
- combined.txt

Bunlar sırasıyla sızdırılan e-postaların, kullanıcı adlarının ve şifrelerin listelerini içerir. Son liste birleştirilmiş e-posta ve parola listelerini içerir. Biz usernames.txt ve passwords.txt listelerini kullanacağız.

2. Tarayıcınızda http://MACHINE_IP/support/login adresine gidin. Burp Proxy'yi etkinleştirin ve proxy'nizdeki isteği yakalayarak oturum açmaya çalışın. Bu adım için herhangi bir kimlik bilgisinin yeterli olacağını unutmayın.
3. Proxy'den yakalanan isteği sağ tıklayıp "Davetsiz Misafir'e Gönder "i seçerek veya Ctrl + I kullanarak Davetsiz Misafir'e gönderin.
4. "Pozisyonlar" alt sekmesinde, yalnızca kullanıcı adı ve parola parametrelerinin seçili olduğundan emin olun. Oturum çerezleri gibi tüm ek seçimleri temizleyin.
5. Saldırı türünü "Pitchfork" olarak ayarlayın.

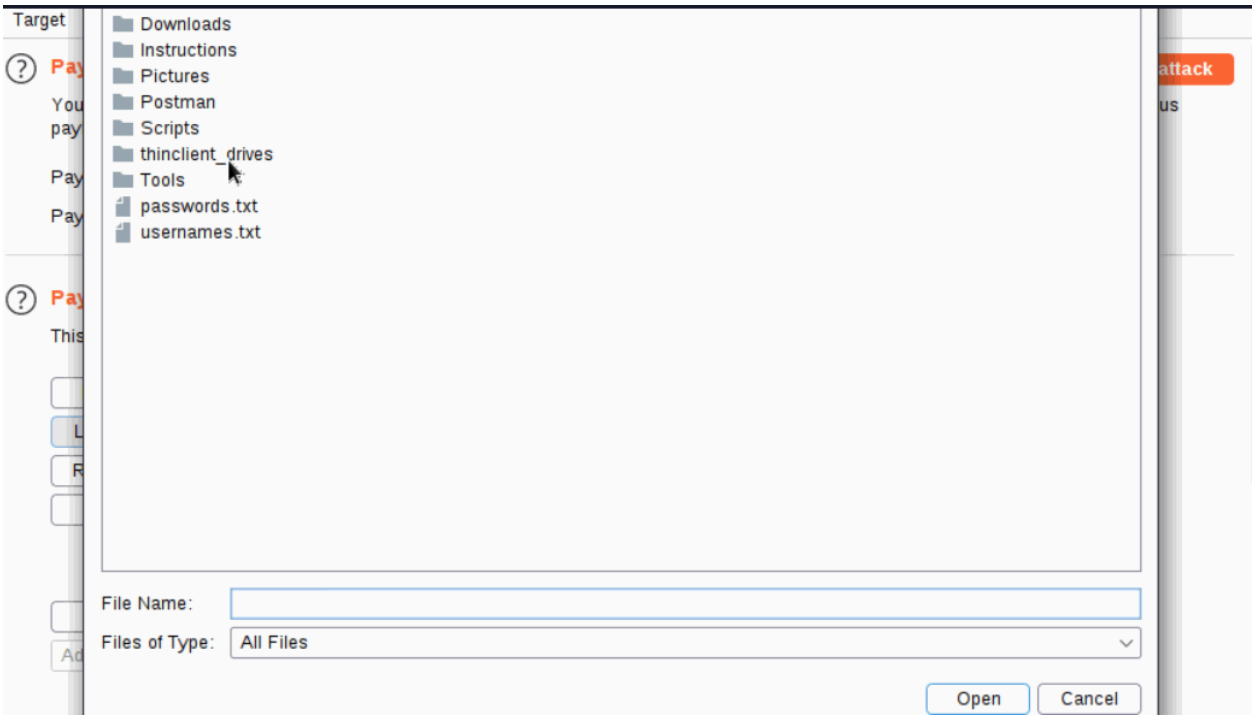


6. "Payloads" alt sekmesine gidin. Kullanıcı adı ve şifre alanları için iki yük seti bulacaksınız.



7. İlk yük setinde (kullanıcı adları için), "Yük Seçenekleri "ne gidin, "Yükle "yi seçin ve usernames.txt listesini seçin.

- Aynı işlemi passwords.txt listesini kullanarak ikinci yük seti (parolalar için) için tekrarlayın.
- Tüm süreç aşağıdaki GIF görüntüsünde görülebilir:



8. Kimlik bilgisi doldurma saldırısını başlatmak için Saldırıyı Başlat düğmesine tıklayın. Hız sınırlamasıyla ilgili bir uyarı görünebilir; devam etmek için Tamam'a tıklayın. Saldırının Burp Community'de tamamlanması birkaç dakika sürecektir.
9. Saldırı başladığında, yeni bir pencere isteklerin sonuçlarını gösterecektir. Ancak, Burp 100 istek gönderdiğinden, hangilerinin başarılı olduğunu belirlememiz gerekir.

Yanıt durum kodları başarılı ve başarısız denemeleri ayırt etmediğinden (hepsi 302 yönlendirmesidir), bunları ayırt etmek için yanıt uzunluğunu kullanmamız gerekir.

Request	Payload 1	Payload 2	Status	Error	Timeout	Length
			302	☐	☐	591
0			302	☐	☐	672
1	l.madden	bambam	302	☐	☐	672
2	j.poole	UnitedKingdom123	302	☐	☐	672

Sonuçları bayt uzunluğuna göre sıralamak için "Uzunluk" sütununun başlığına tıklayın. Başarılı bir oturum açma girişimini gösteren daha kısa yanıt uzunluğuna sahip isteği arayın.

10. Başarılı oturum açma denemesini onaylamak için, oturum açmak üzere daha kısa yanıt uzunluğuna sahip istekteki kimlik bilgilerini kullanın.

Soru ⇒ Hangi kullanıcı adı ve parola kombinasyonu başarılı bir oturum açma girişimini gösterir? Cevap formatı "kullanıcı adı:şifre" şeklindedir.

Cevap ⇒ m.rivera:letmein1

Task 11 Practical Challenge (Görev 11 Pratik Zorluk)

Destek sistemine erişim sağladıktan sonra, artık işlevlerini keşfetme ve hangi eylemleri gerçekleştirebileceğimizi görme fırsatına sahibiz.

Ana arayüze eriştiğimizde, çeşitli biletleri gösteren bir tablo ile karşılaşırız. Herhangi bir satıra tıklamak bizi biletin tamamını görüntüleyebileceğimiz bir sayfaya yönlendirir. URL yapısını inceleyerek, bu sayfaların aşağıdaki formatta numaralandırıldığını gözlemliyoruz:

`http://MACHINE_IP/support/ticket/NUMBER`

Numaralandırma sistemi, biletlere karmaşık ve tahmin edilmesi zor kimliklerden ziyade tam sayı tanımlayıcıların atandığını göstermektedir. Bu bilgi önemlidir çünkü iki olası senaryoya işaret etmektedir:

1. **Access Control (**Erişim Kontrolü): Uç nokta, yalnızca mevcut kullanıcımıza atanan destek taleplerine erişimi kısıtlamak için uygun şekilde yapılandırılmış olabilir. Bu durumda, yalnızca hesabımızla ilişkili destek taleplerini görüntüleyebiliriz.
2. **IDOR Vulnerability** (IDOR Güvenlik Açığı): Alternatif olarak, uç nokta uygun erişim kontrollerinden yoksun olabilir ve bu da Güvensiz Doğrudan Nesne Referansları (IDOR) olarak bilinen bir güvenlik açığına yol açabilir. Eğer durum buysa, potansiyel olarak sistemi istismar edebilir ve atanmış kullanıcıdan bağımsız olarak mevcut tüm biletleri okuyabiliriz.

Daha fazla araştırma yapmak için, /support/ticket/NUMBER uç noktasını bulanıklaştırmak için Intruder aracını kullanacağız. Bu yaklaşım, uç noktanın doğru yapılandırılıp yapılandırılmadığını veya bir IDOR güvenlik açığının mevcut olup olmadığını belirlememize yardımcı olacaktır. Fuzzing işlemine devam edelim!

Not: Oturum açmış durumdayken bir talep yakalamanız gerekir.

Sorular;

Soru ⇒ Bu görev için en uygun saldırı türü hangisidir(İpucu⇒ Bulanıklaştırmak için tek bir pozisyonunuz var.)?

Cevap⇒ Sniper

Soru ⇒ Uygun bir konum ve yükü yapılandırın (biletler 1 ile 100 arasındaki değerlerde saklanır), ardından saldırıyı başlatın.

En az beş biletin, var olduklarını belirten 200 durum koduyla döndürüleceğini göreceksiniz.

(İpucu⇒ Bir pozisyona ihtiyacınız olacak (sayısal bilet uç noktası). Yükünüz 1 ile 100 arasında bir sayı listesi olmalıdır -- bunun için sayılar yükü türüne bakın.)

Cevap ⇒ Cevap Gerekmemektedir.

Soru ⇒ Saldırı Sonuçları penceresindeki Yanıt sekmesini kullanarak ya da tarayıcınızda her başarılı (yani 200 kodlu) isteğe manuel olarak bakarak, bayrağı içeren bileti bulun. Bayrak nedir?

Cevap ⇒ THM{MTMxNTg5NTUzMWM0OWRlYzUzMDVjMzJl}

Task 12 Extra Mile Challenge (Görev 12 Ekstra Mil Mücadelesi)

Bu ekstra mil alıştırmasında, daha önce gerçekleştirdiğimiz kimlik bilgisi doldurma saldırısının daha zorlu bir varyantını ele alacağız. Ancak bu kez, kaba zorlamayı daha zor hale getirmek için ek önlemler uygulanmıştır. Burp Makrolarını kullanmakta rahatsanız, aşağıdaki talimatlar olmadan bu zorluğu deneyebilirsiniz. Aksi takdirde, adım adım yaklaşımla devam edelim.

Talebin Yakalanması

http://MACHINE_IP/admin/login/ adresine bir istek göndererek ve yanıtı inceleyerek başlayın. İşte yanıtın bir örneği:

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 20 Aug 2021 22:31:16 GMT
Content-Type: text/html; charset=utf-8
Connection: close
```

```
Set-Cookie: session=eyJ0b2tlbklEIjoiMzUyNTQ5ZjgxZDRhOTM5YjVlMTNlMjIz
NmI0ZDlkOGEifQ.YSA-mQ.ZaKKsUnNsIb47sjlyux_LN8Qst0; HttpOnly; Path=/
Vary: Cookie
Front-End-Https: on
Content-Length: 3922
---
<form method="POST">
   <div class="form-floating mb-3">
      <input class="form-control" type="text" name=username  placeholder
="Username" required>
      <label for="username">Username</label>
   </div>
   <div class="form-floating mb-3">
      <input class="form-control" type="password" name=password  placehol
der="Password" required>
      <label for="password">Password</label>
   </div>
   <input type="hidden" name="loginToken" value="84c6358bbf1bd8000b6b
63ab1bd77c5e">
   <div class="d-grid"><button class="btn btn-warning btn-lg" type="submi
t">Login!</button></div>
</form>
```

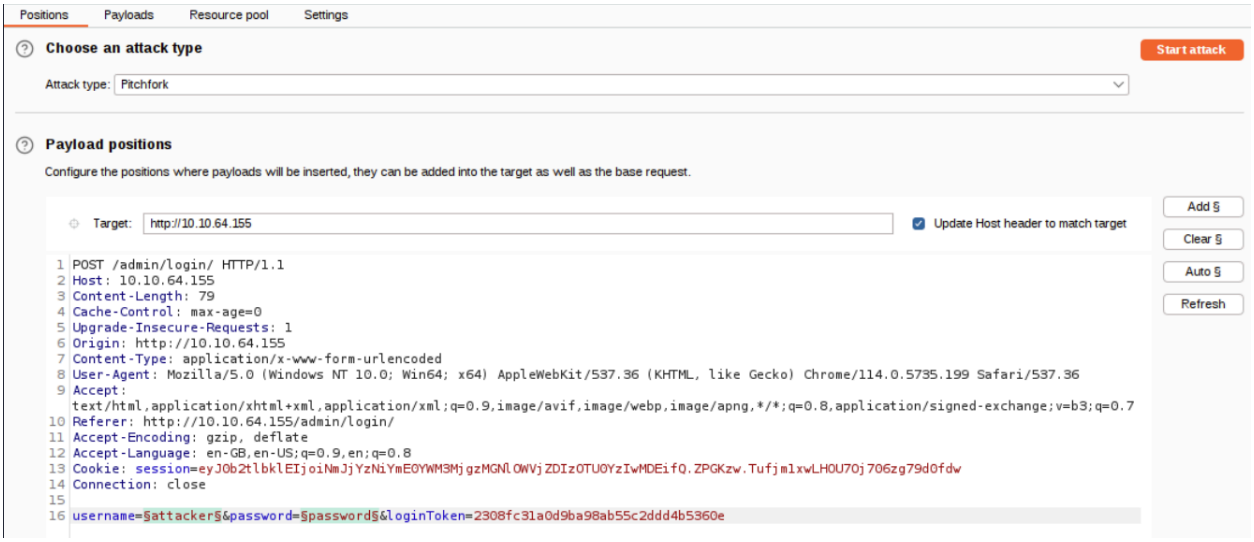
Bu yanıtta, kullanıcı adı ve parola alanlarının yanı sıra artık bir oturum çerezi ayarlandığını ve formda gizli bir alan olarak bir CSRF (Siteler Arası İstek Sahteciliği) belirteci olduğunu fark ediyoruz. Sayfayı yenilediğinizde hem oturum çerezinin hem de loginToken'ın her istekte değiştiğini görürsünüz. Bu, her oturum açma denemesinde hem oturum çerezi hem de loginToken için geçerli değerleri çıkarmamız gerektiği anlamına gelir.

Bunu başarmak için, her istekten önce yürütülecek tekrarlanan bir dizi eylem (makro) tanımlamak için Burp Makrolarını kullanacağız. Bu makro, oturum çerezi ve loginToken için benzersiz değerler çıkaracak ve bunları saldırımızın sonraki her isteğinde değiştirecektir.

Tutorial

1. http://MACHINE_IP/admin/login/ adresine gidin. Proxy modülünde Intercept'i etkinleştirin ve oturum açmaya çalışın. İsteği yakalayın ve Intruder'a gönderin.
2. Konumları, destek girişini zorlamak için yaptığımız gibi yapılandırın:

- Saldırı türünü "Pitchfork" olarak ayarlayın.
- Önceden tanımlanmış tüm konumları temizleyin ve yalnızca kullanıcı adı ve parola form alanlarını seçin. Makromuz diğer iki pozisyonu işleyecektir.



3. Şimdi Payloads sekmesine geçin ve destek oturum açma saldırısı için kullandığımız kullanıcı adı ve parola kelime listelerini yükleyin.

Bu noktaya kadar, Intruder'ı önceki kimlik bilgisi doldurma saldırımızla neredeyse aynı şekilde yapılandırdık; işler burada daha karmaşık hale gelmeye başlıyor.

4. Kullanıcı adı ve parola parametreleri halledildikten sonra, şimdi sürekli değişen loginToken ve oturum çerezini almanın bir yolunu bulmamız gerekiyor. Ne yazık ki, "recursive grep" yönlendirme yanıtı nedeniyle burada çalışmayacaktır, bu nedenle bunu tamamen Intruder içinde yapamayız - bir makro oluşturmamız gerekecek.

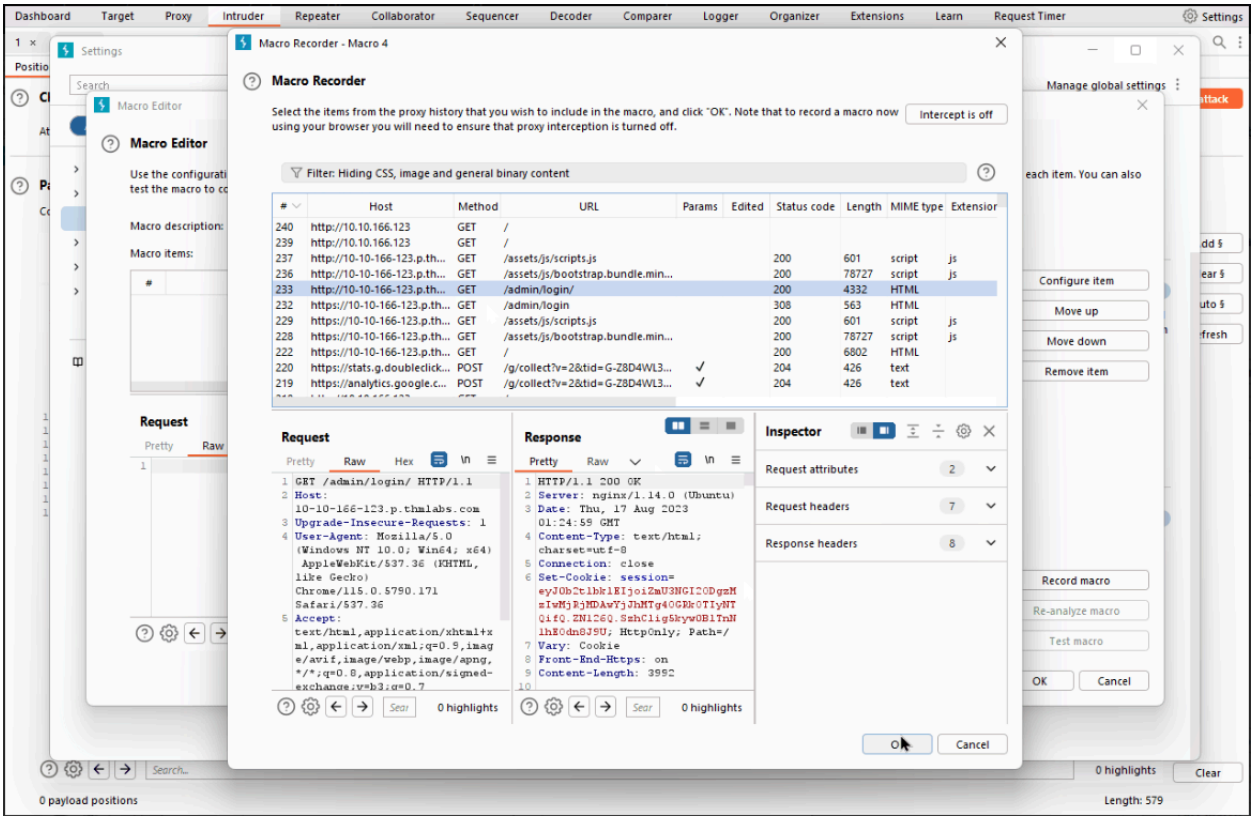
Makrolar aynı eylemleri tekrar tekrar gerçekleştirmemizi sağlar. Bu durumda, basitçe /admin/login/ adresine bir GET isteği göndermek istiyoruz.

Neyse ki, bunu kurmak basit bir işlemdir.

- Burp'ün sağ üst köşesindeki ana "Ayarlar" sekmesine geçin.

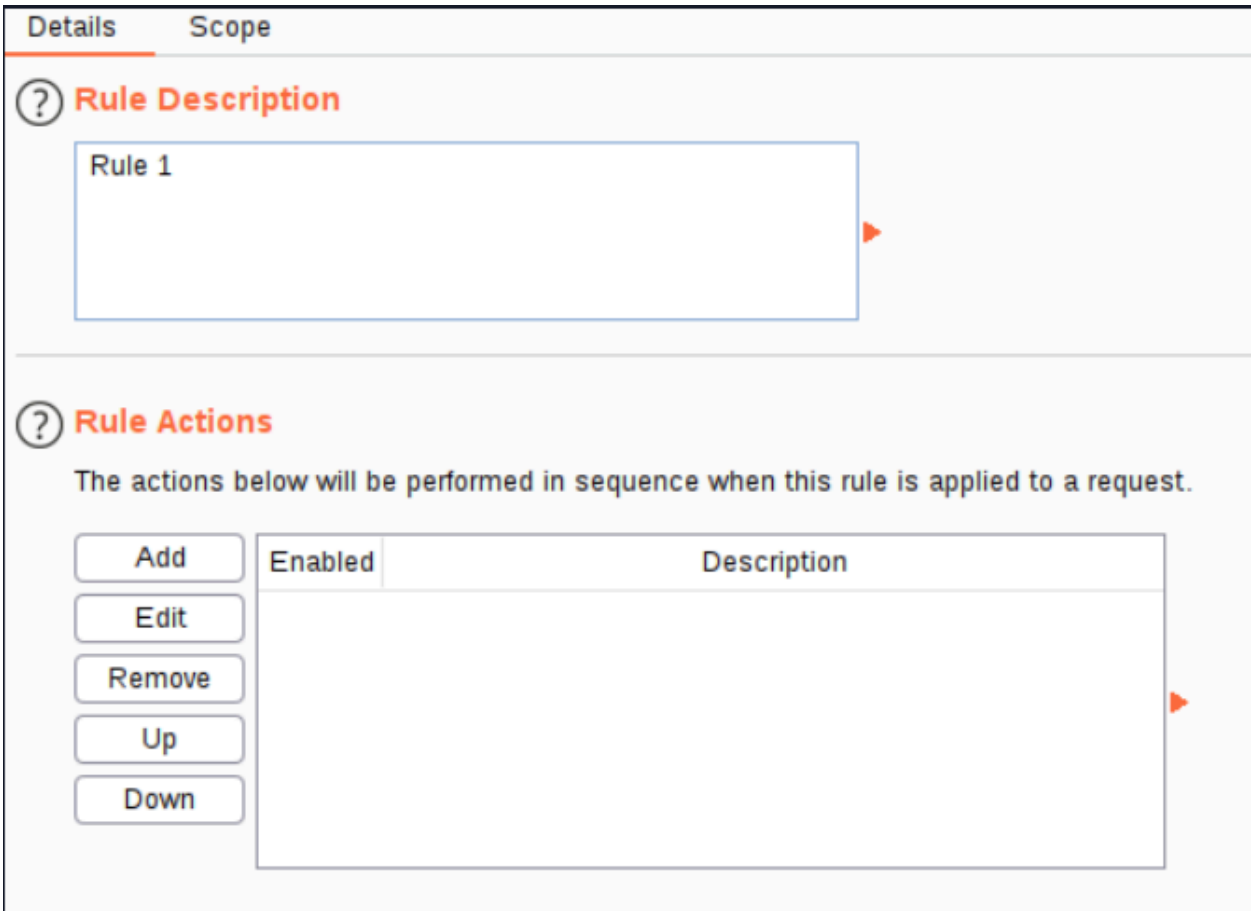
- "Oturumlar" kategorisine tıklayın.
- Kategorinin en altındaki "Makrolar" bölümüne gidin ve Ekle düğmesine tıklayın.
- Görünen menü bize istek geçmişimizi gösterecektir. Listede halihazırda http://MACHINE_IP/admin/login/ adresine bir GET isteği yoksa, tarayıcınızda bu konuma gidin ve listede uygun bir isteğin göründüğünü göreceksiniz.
- Talep seçiliyken Tamam'a tıklayın.
- Son olarak, makroya uygun bir ad verin ve işlemi bitirmek için tekrar Tamam'a tıklayın.

Burada nispeten çok fazla adım vardır, bu nedenle aşağıdaki GIF tüm süreci göstermektedir:

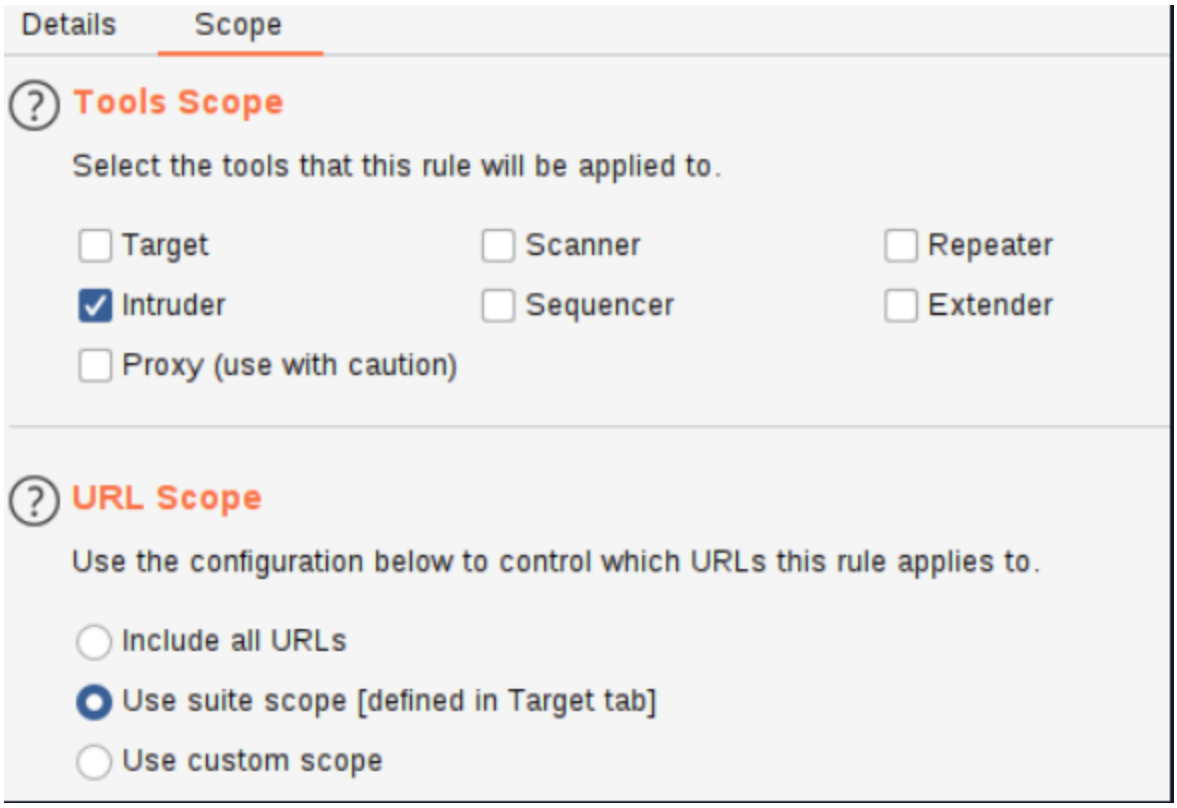


5. Artık bir makro tanımladığımıza göre, makronun nasıl kullanılacağını tanımlayan Oturum İşleme kurallarını belirlememiz gerekir.
- Hala ana ayarların "Oturumlar" kategorisinde, "Oturum İşleme Kuralları" bölümüne gidin ve Yeni bir kural ekle'yi seçin.

- İçinde iki sekme bulunan yeni bir pencere açılacaktır: "Ayrıntılar" ve "Kapsam". Varsayılan olarak Ayrıntılar sekmesindeyiz.



- Uygun bir açıklama girin ve ardından Kapsam sekmesine geçin.
- "Araçlar Kapsamı" bölümünde, İzinsiz Giren dışındaki tüm onay kutularının işaretini kaldırın - bu kuralın başka hiçbir yerde uygulanmasına gerek yoktur.
- "URL Kapsamı" bölümünde "Paket kapsamını kullan" seçeneğini seçin; bu, makroyu yalnızca genel kapsama eklenen sitelerde çalışacak şekilde ayarlayacaktır (Burp Temelleri bölümünde tartışıldığı gibi). Genel bir kapsam belirlemediyseniz, "Özel kapsam kullan" seçeneğini varsayılan olarak tutun ve bu bölümdeki kapsama http://MACHINE_IP/ adresini ekleyin.



6. Şimdi Ayrıntılar sekmesine geri dönmemiz ve "Kural Eylemleri" bölümüne bakmamız gerekiyor.

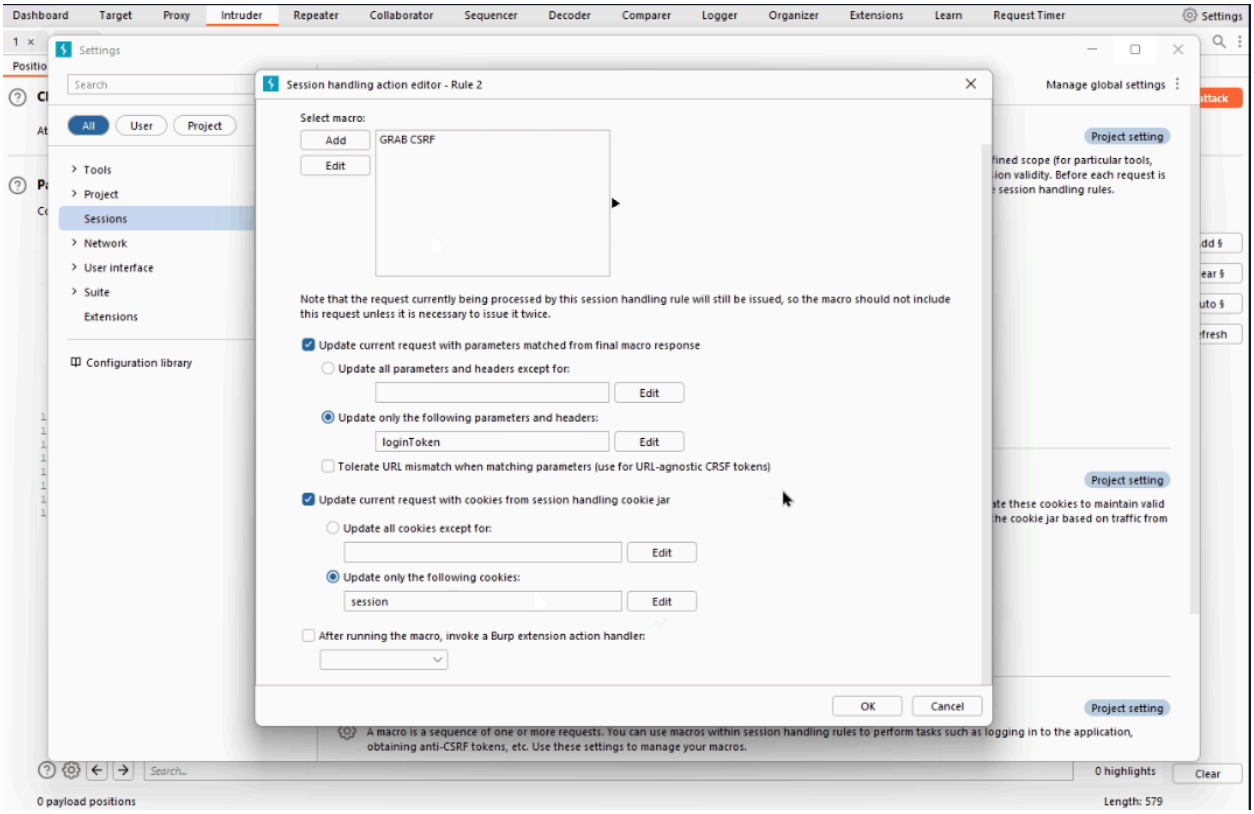
- Ekle düğmesine tıklayın - bu, ekleyebileceğimiz eylemlerin bir listesini içeren bir açılır menünün görünmesine neden olacaktır.
- Bu listeden "Bir Makro Çalıştır" öğesini seçin.
- Görüntülenen yeni pencerede, daha önce oluşturduğumuz makroyu seçin.

Bu haliyle, bu makro artık Intruder isteklerimizdeki tüm parametrelerin üzerine biz onları göndermeden önce yazacaktır; loginTokens ve oturum çerezlerini doğrudan isteklerimize ekleyeceğimiz anlamına geldiği için bu harika bir şeydir. Bununla birlikte, saldırımıza başlamadan önce hangi parametrelerin ve çerezlerin güncelleneceğini kısıtlamalıyız:

- "Yalnızca aşağıdaki parametreleri ve başlıkları güncelle" seçeneğini seçin, ardından radyo düğmesinin altındaki giriş kutusunun yanındaki Düzenle düğmesine tıklayın.

- "Yeni bir öğe girin" metin alanına "loginToken" yazın. Ekle'ye ve ardından Kapat'a basın.
- "Yalnızca aşağıdaki çerezleri güncelle" seçeneğini seçin, ardından ilgili Düzenle düğmesine tıklayın.
- "Yeni bir öğe girin" metin alanına "oturum" girin. Ekle'ye ve ardından Kapat'a basın.
- Son olarak, eylemimizi onaylamak için Tamam düğmesine basın.

Aşağıdaki GIF sürecin bu son aşamasını göstermektedir:



7. Tamam'a tıklayın ve işimiz bitti!
8. Artık CSRF belirtecini ve oturum çerezini yerine koyacak bir makro tanımlamış olmalısınız. Geriye kalan tek şey Intruder'a geri dönmek ve saldırıyı başlatmak!

Not: Bu saldırıdaki her istek için 302 durum kodu yanıtları alıyor olmalısınız. Eğer 403 hatası görüyorsanız, makronuz düzgün çalışmıyor demektir.

9. Gerçekleştirdiğimiz destek girişi kimlik bilgisi doldurma saldırısında olduğu gibi, buradaki yanıt kodlarının hepsi aynıdır (302 Yönlendirmeleri). Bir kez daha, geçerli kimlik bilgilerini bulmak için yanıtları uzunluklarına göre sıralayın. Sonuçlarınız geçen seferki kadar net olmayacaktır - birkaç farklı yanıt uzunluğu göreceksiniz: ancak, başarılı bir oturum açmayı gösteren yanıt yine de önemli ölçüde daha kısa olarak öne çıkmalıdır.
10. Oturum açmak için yeni bulduğunuz kimlik bilgilerini kullanın (kimlik bilgilerini girmeden önce oturum açma sayfasını yenilemeniz gerekebilir).

Soru ⇒ Hangi kullanıcı adı ve parola kombinasyonu başarılı bir oturum açma girişimini gösterir? Cevap formatı "kullanıcı adı:şifre" şeklindedir.

Cevap ⇒ o.bennett:bella1

Task 13 Conclusion (Görev 13 Sonuç)

Burp Suite Intruder odasını tamamladığınız için tebrikler!

Şimdiye kadar, istekleri otomatikleştirmek ve çeşitli saldırı türlerini gerçekleştirmek için Intruder'ı nasıl etkili bir şekilde kullanacağınızı sağlam bir şekilde anlamış olmalısınız.

Modülün bir sonraki odasında Burp Suite'in diğer modüllerinden bazılarına bakacağız!

Cevap Gerekmemektedir.