Uygulamalı laboratuvar: Mezmo kullanarak bir Ayrıştırma Şablonu oluşturma

Tahmini Gerekli Süre: **60 dk**

Başlarken

Mezmo kullanarak bir Ayrıştırma Şablonu oluşturma uygulamalı laboratuvarına hoş geldiniz.

Bu laboratuvar, alınan günlük satırlarını nasıl ayrıştıracağınızı öğreneceksiniz. Ayrıştırma ekranı ve ayrıştırma mini haritası hakkında bilgi edineceksiniz. Mevcut bazı ayrıştırma fonksiyonlarını nasıl kullanacağınızı öğreneceksiniz. Üç değerin hepsini nasıl ayrıştıracağınızı veya birini nasıl ayrıştıracağınızı ve şablonları nasıl doğrulayacağınızı öğreneceksiniz.

Mezmo ayrıştırma:

- Mezmo, yaygın günlük türlerini destekler ve satırları sizin için otomatik olarak ayrıştırır. Günlük ayrıştırma, günlük verilerini makine tarafından okunabilir hale getirmek için ortak bir formata dönüştürme sürecidir. Ancak, desteklenen günlük türlerinden birine uymayan bir günlük formatınız varsa, Bir Ayrıştırma Şablonu Oluştur veya Alanları Çıkar kullanarak kendi ayrıştırma kurallarınızı oluşturabilirsiniz.
- Özel Ayrıştırma şablonları, aktif şablonların sırasına göre günlüklerinize uygulanır. Örneğin, aynı günlük satırını hedefleyen iki aktif şablonunuz varsa, şablonlar Yönetim Ayrıştırma sayfasındaki sıraya göre uygulanır.

  -Şablon Bir
  -Şablon İki

  Öncelikle, Şablon Bir gelen günlükler üzerine uygulanacaktır; eğer Şablon İki'de eşleşen bir günlük satırı varsa, o zaman uygulanacaktır. Aktif şablonların sırasını Yönetim Ayrıştırma sayfasında sürükleyerek değiştirebilirsiniz.

Öğrenme Hedefleri:

Bu laboratuvar çalışmasında, standart olmayan günlük formatlarını düzenlemek ve günlükleriniz üzerinde özel dönüşümler gerçekleştirmek için adım adım sihirbazı kullanacaksınız. Bu sayede daha önce erişilemeyen günlük satırlarını kolayca arayabilir ve grafikleyebilirsiniz.

Bu basit bir üç adımlı süreçtir:
-Arama
-Çıkarma
-Doğrulama

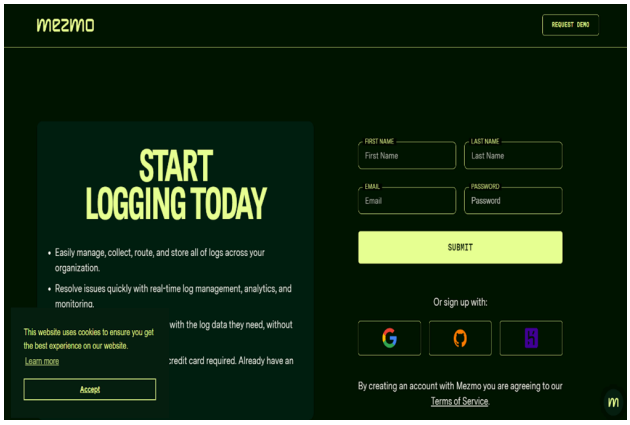
Çoğu durumda, otomatik ayrıştırma ihtiyacınız olan tek şey olabilir, özellikle günlükleriniz yaygın formatlarda ise.

Bu laboratuvarı tamamladıktan sonra:

- Bir dizeyi nasıl ayrıştıracağınızı gösterin.
- Bir zaman damgasını nasıl ayrıştıracağınızı gösterin.
- Bir sayıyı nasıl ayrıştıracağınızı gösterin.
- Şablonları nasıl doğrulayacağınızı sergileyin.

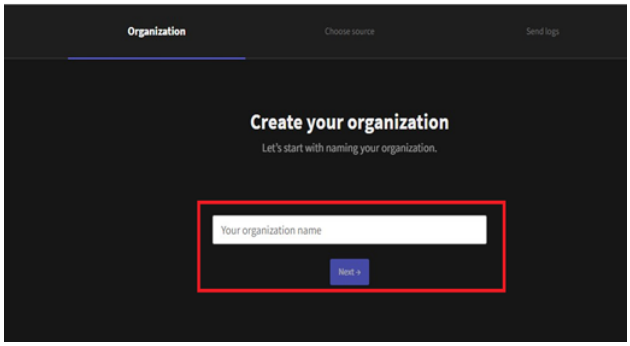
Kurulum : Mezmo ile Kaydolun

1. Kaydolun bağlantısına tıklayın ve açın.
2. Kaydolma sayfasına yönlendirileceksiniz.

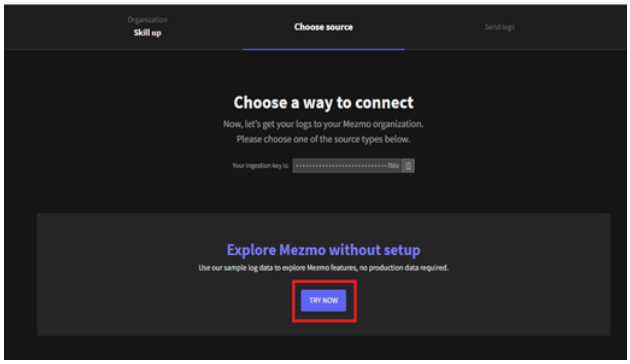


3. Bilgilerinizi girin ve **Gönder** butonuna tıklayın.

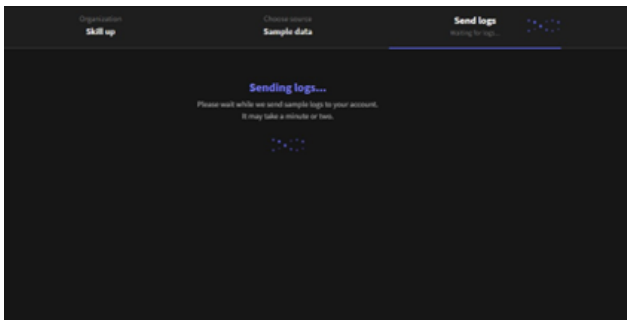
4. E-posta adresinizin geçerliliğini sağlamak için, Mezmo sağladığınız adrese bir doğrulama e-postası gönderecektir. Doğrulama kodunu girin.
5. Aşağıda gösterildiği gibi **organizasyon adınızı** girin.



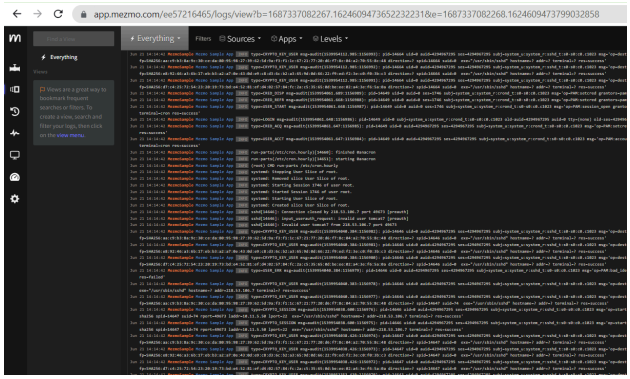
6. **Şimdi dene** butonuna tıklayın.



7. Örneklenen günlük gönderilirken birkaç saniye bekleyin.



8. Artık Mezmo hesabınızın **kontrol paneline** veya **ana sayfasına** yönlendirileceksiniz.



Not: Mezmo'nun ücretsiz deneme süresi yalnızca 14 gündür. Lütfen laboratuvarı ücretsiz deneme süresi içinde tamamlayın.

Günlük bilgileri:

Örnek günlük satırını ele alalım; bu satırda IP adresi, zaman damgası, yanıt bilgisi ve kullanılan web tarayıcıları bulunmaktadır:

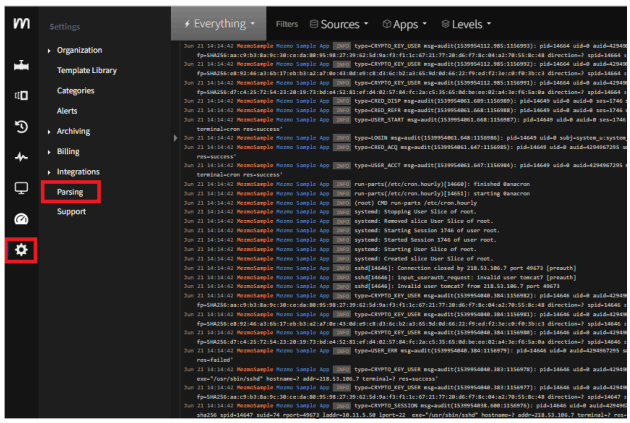
```
103.93.21.233 - - [15/Nov/2018:18:31:24 +0000] "GET / HTTP/1.1" 200 745 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36"
```

- **ip_address:** 103.93.21.233
- **timestamp:** 15/Kas/2018:18:31:24 +0000
- **response:** 200

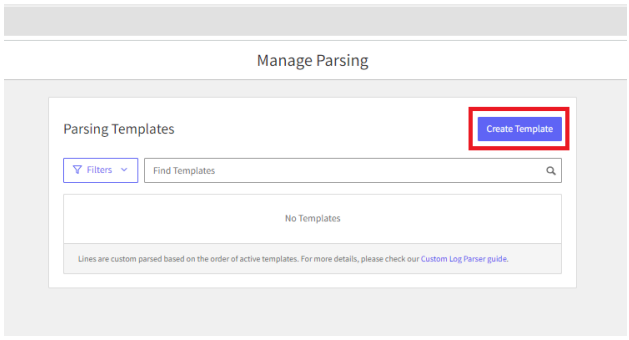
Görev 1: Dizeyi Ayrıştır

Log satırından 111.00.11.10'u ayrıştıracaksınız.

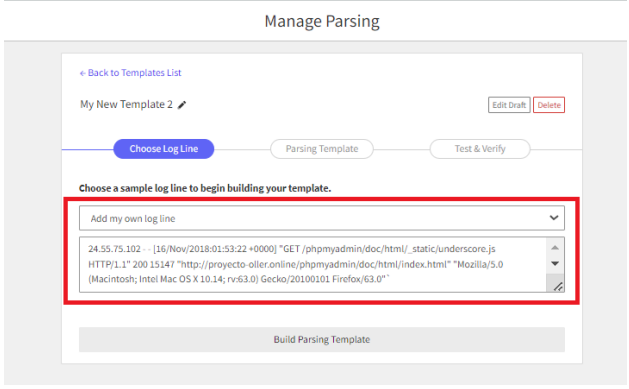
1. **Ayarlar** simgesine tıklayın ve **Ayrıştırma** seçeneğine tıklayın. Sonraki sayfada **Şablon Oluştur** butonuna tıklayın.



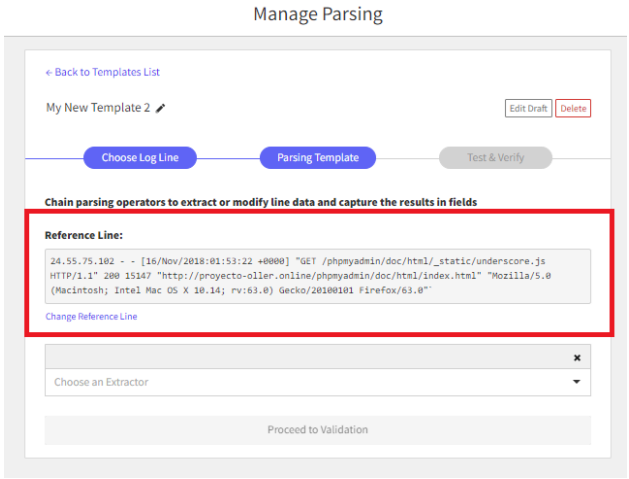
2. Sonraki sayfada **Şablon Oluştur** butonuna tıklayın.



3. Log Satırı Seçin kısmında **Kendi log satırımı ekle** seçeneğini seçin. Girişteki log satırını kullanacaksınız.



4. **Ayrıştırma Şablonu Oluştur** butonuna tıklayın. Girdiğiniz satırı Referans Satırı olarak göreceksiniz.



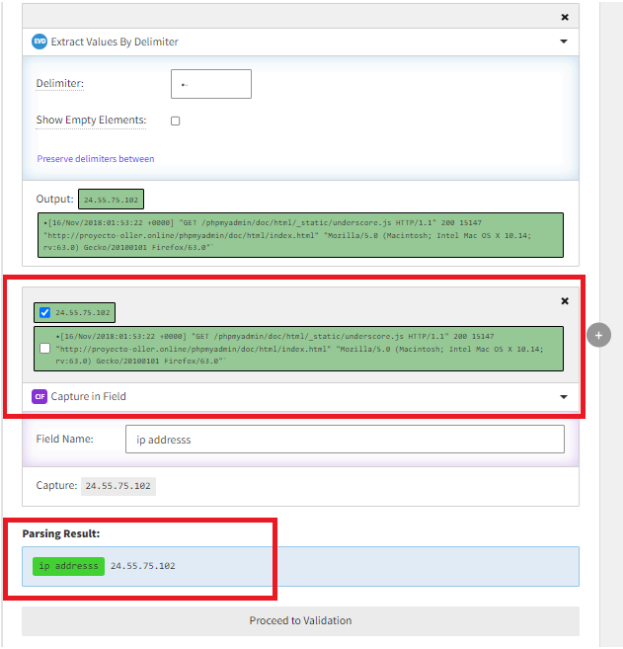
5. Öncelikle, metni daha küçük parçalara ayıracaksınız, böylece istediğiniz parçayı kullanabilirsiniz. Extractor Seçin kısmında **Ayırıcı ile Değer Çıkart** seçeneğini seçin.

6. **boşluk** ve ardından bir **tire** girin.

7. Artık **24.55.75.102**'yi ayrıştırılan satırların bir parçası olarak görmelisiniz.

8. **24.55.75.102**'yi seçin ve **Alanda Yakala** operatörünü seçin. Bir etiket veya Alan Adı olarak **ip_address** verin.

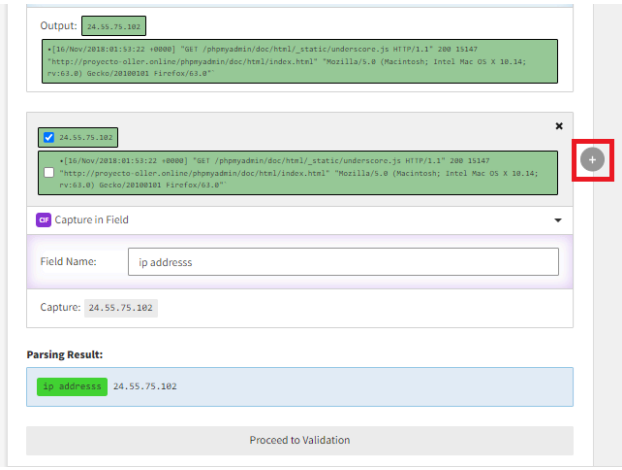
9. Sonuç, ayrıştırma sayfasının altında gösterilmektedir.



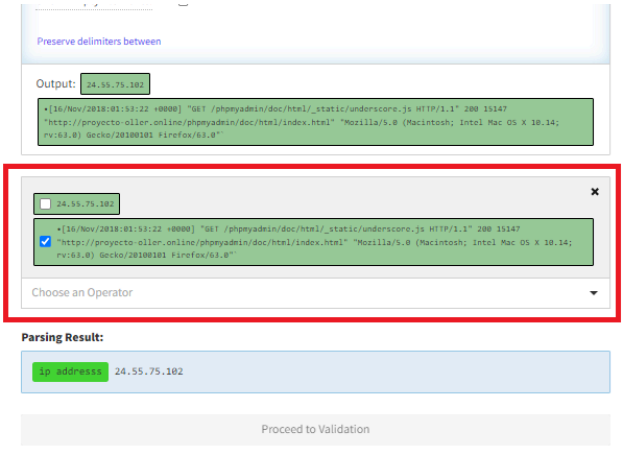
Görev 2: Zaman Damgasını Ayrıştır

Log satırından 16/Nov/2018:01:53:22 +0000 zaman damgasasını ayrıştıracaksınız.

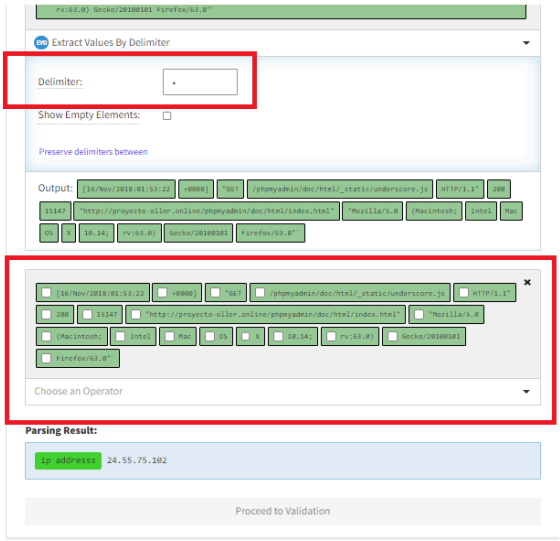
1. Kardeş Operatörü oluşturmak için **artı işareti** olan çemberi seçin.



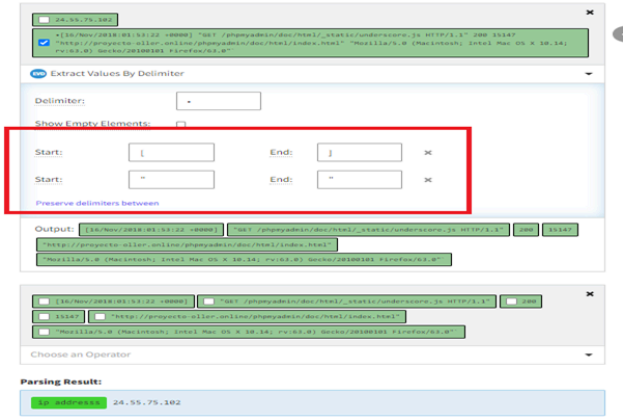
2. Zaman damgasını içeren daha uzun çıktıyı kontrol edin.



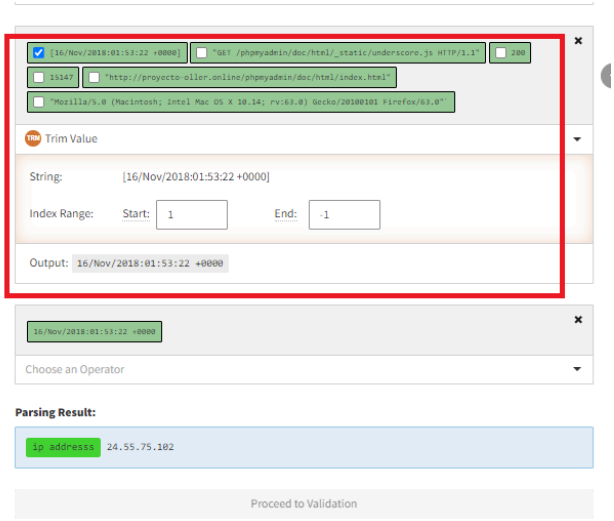
3. Bir operatör seçin > **Ayırıcı ile Değerleri Çıkar**.
4. Ayırıcıya bir **boşluk** girin.
5. Çıktının her şeyi boşlukla ayırdığını, zaman damgasasının bir kısmını da içerdiğini fark edin. Zaman damgasasını düzeltmek için bazı boşlukları korumanız gerekiyor.



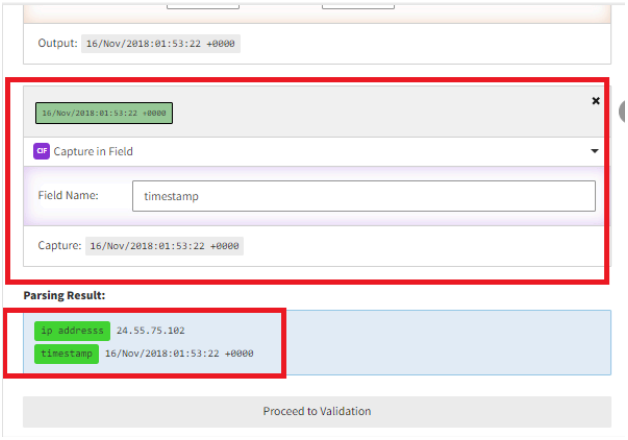
6. **Aralarındaki ayırıcıları koru** seçeneğine tıklayın.
7. Bir sol köşeli parantez [ile başlayın ve bir sağ köşeli parantez] ile bitirin.
8. **Aralarındaki ayırıcıları koru** seçeneğine tekrar tıklayın. Hem başlangıç hem de bitiş için çift tırnak “ kullanın. Zaman damgasasının şimdi temizlendiğini, diğer bazı çıktılarla birlikte göreceksiniz.



9. Şimdi zaman damgasasından köşeli parantezleri kaldırmanız gerekiyor, böylece teşhis koymak daha kolay olur. Zaman damgasasını seçin. [16/Nov/2018:01:53:22 +0000] , operatörü seçin, **Değeri Kısalt**.
10. Kısaltma Değeri 0 bazlıdır. Başlangıç için **1**, bitiş için **-1** girin.
11. Çıktınız zaman damgasası olmalıdır.



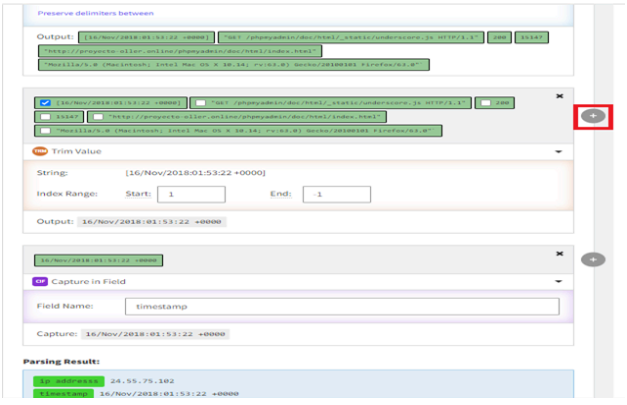
12. Operatörü seçin > **Alanda Yakala** ve etiketini **zaman damgasası** olarak belirleyin.
13. Şimdiye kadar log satırından iki alan yakaladınız.



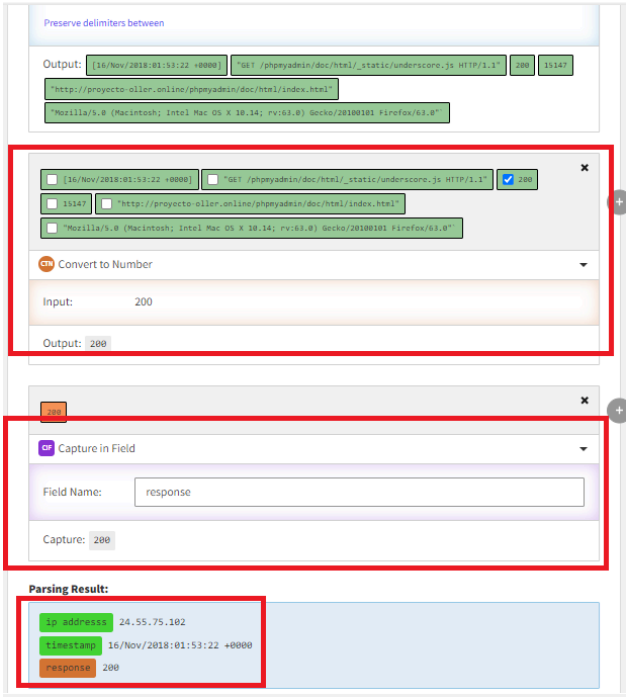
Görev 3: Sayıyı Ayrıştır

Log satırından 200'ü ayrıştıracaksınız.

1. Mini haritayı kullanarak Trim Value'yu seçin. Trim Value turuncudur, mini haritadaki simgelerin üzerine gelerek de bilgi alabilirsiniz. Mini haritayı kullanmak, ayrıştırılan alanlar arasında geçiş yapmanıza olanak tanır. Trim Value'dan başlayarak, 200'ün diğer değerlerden ayrılmış olduğu bir yerden başlayabilir, böylece kullanımı kolaylaşır.
2. **Artı işareti** olan daireye tıklayarak bir Kardeş Operatörü ekleyin.



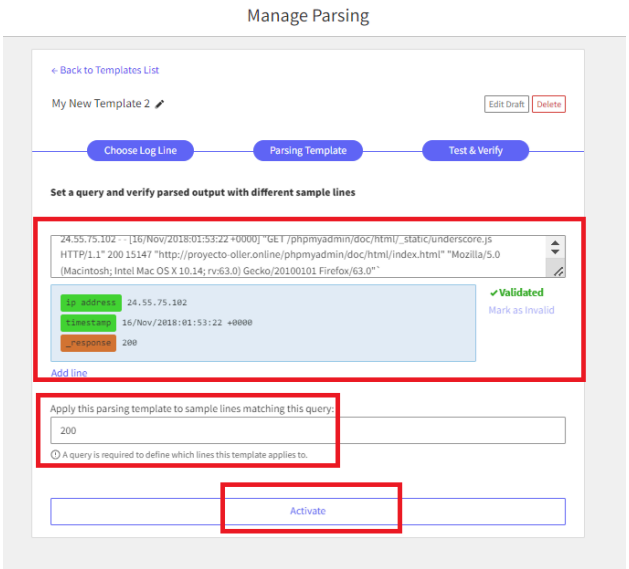
3. **200**'ü seçin.
4. Bir operatör seçin > **Sayıya Dönüştür**.
5. Bir operatör seçin > **Alanda Yakala**. Alan adı **response**.



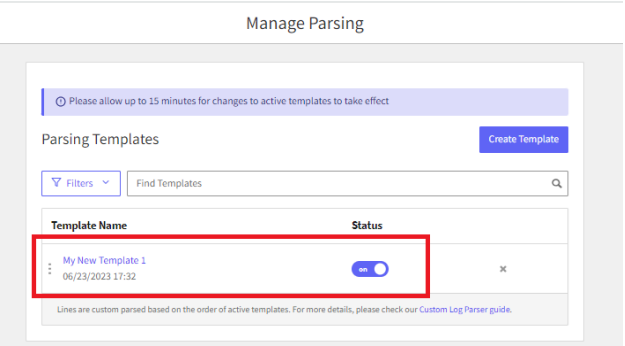
Görev 4: Şablonu Doğrula

Bir şablonu aktif hale getirmeden önce, test etmek istediğiniz günlük satırlarının çalıştığından emin olmalısınız.

1. **Günlük satırı** ekleyin ve test edin. Örnek satırı kullanabilirsiniz. Test sırasında, birden fazla satırı test etmek için satırlar eklemeyi unutmayın.
2. Günlük satırlarını geçerli veya geçersiz olarak işaretleyin.
   a. Bir satır geçersiz olarak işaretlenirse, sizi Ayrıştırma Şablonu adımına geri götürecektir.
3. Satırı geçerli olarak işaretleyin ve Bu ayrıştırma şablonunu bu sorguya uyan örnek satırlara uygulayın: giriş alanına sorgunuzu girin.



4. **Aktif Et** butonuna tıkladığınızda **açık** durumu göreceksiniz. Ve uygulama günlükleriniz için etkili olması 15 dakika sürecektir.



Not: Aktif ayrıştırma şablonları, şablon etkinleştirildikten sonra gelen satırlara yalnızca uygulanır. Şablon aktif hale gelmeden önce alınan tüm günlük satırları, ayrıştırma şablonu tarafından ayrıştırılmaz.

Uygulamanız yeni günlükler ürettiğinde, uygulama günlüklerinizi analiz etmenize yardımcı olan eşleşen verileri size sunar, böylece uygulamanızın doğru çalışıp çalışmadığını bilirsiniz.

Özet

Tebrikler! Mezmo kullanarak bir Ayrıştırma Şablonu oluşturdunuz.

Bu laboratuvar çalışmasında, mezmo platformuna erişim sağladınız ve keşfettiniz. Verilen örnek günlük satırı üzerinde özel ayrıştırma gerçekleştirdiniz ve ip_address, timestamp, response bilgilerini ayrıştırarak doğruladınız.

Yazar(lar)

Pallavi Rai

Katkıda Bulunan(lar)

Anamika Agarwal
Shivam kumar