Burpsuite ile Şifre Kırma Saldırısında Arayüzde Bildirim Metotları

Burp ile yapılan Brute Force ve Dictionary saldırılarında ekranda akan denemeler sırasında iki metot söz konusudur. Bunlardan birincisi yanlış denemelerde gelen bir cümleyi referans alma, ikincisi ise doğru denemede gelen (gelecek) bir cümleyi referans almadır.

Web uygulama login sayfalarında yanlış hesap bilgisi girildiğinde bir hata / uyarı cümlesi gelir. Doğru hesap bilgisi girildiğinde ise belki bir hoşgeldiniz cümlesi gelir. Dolayısıyla olası hesapları denerken denemelerimiz içerisinden hangisinin doğru hesap olduğu bilgisini tespit edebilmemiz adına kullanabileceğimiz iki adet referans noktası vardır. Bu iki referans noktasından birini seçerek yüzlerce deneme içerisinden hangisinin doğru deneme (yani gerçekten var olan bir hesap) olduğu bilgisine ulaşabiliriz. Örneğin;

Giriş yapılırken yanlış denemeler sonucu gelen hata cümlesi referans alındığında;

> yanlış giriş teşebbüslerinde hata kelimeleri sütunu tick alır,
> doğru giriş teşebbüsünde ise hata kelimeleri sütunu tick almaz.

Kullanıcı Adı	Şifre	yanlis sifre girdiniz	
admin	aaaa	(tick)	
admin	aaab	(tick)	
...	…	(tick)	
...	…	(tick)	
admin	toka	(**empty**)	// Şifre Tespit Edildi
…	…	(tick)	
admin	zzzz	(tick)	

Giriş yapılırken doğru deneme sonucu gelen hoşgeldiniz vari cümle referans alındığında;

> yanlış giriş teşebbüslerinde hoşgeldiniz benzeri kelime sütunu tick almaz,
> doğru giriş teşebbüsünde ise hoşgeldiniz benzeri kelime sütunu tick alır.

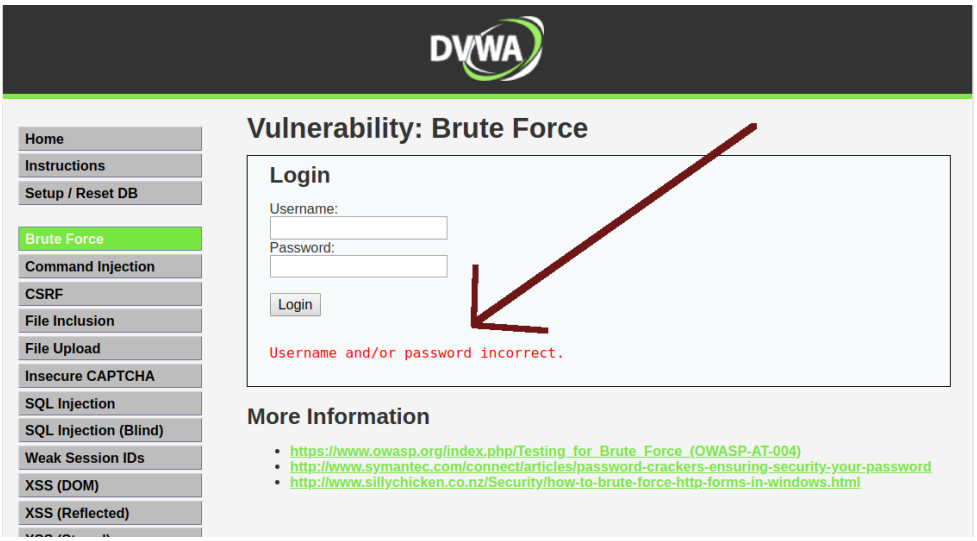
Kullanıcı Adı	Şifre	hosgeldiniz	
admin	aaaa	(empty)	
admin	aaab	(empty)	
...	…	(empty)	
...	…	(empty)	
admin	toka	(**tick**)	// Şifre Tespit Edildi
…	…	(empty)	
admin	zzzz	(empty)	

Uygulama

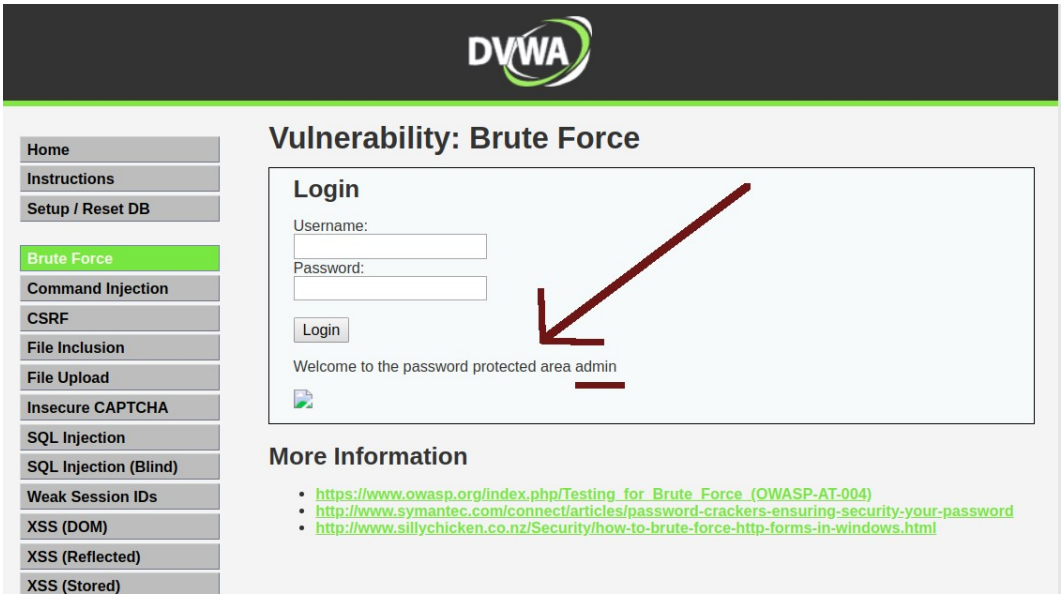
(+) Bu başlık birebir denenmiştir ve başarılı olunmuştur.

DVWA web uygulamasını ele alacak olursak

bu login sayfasında yanlış şifre girildiğinde



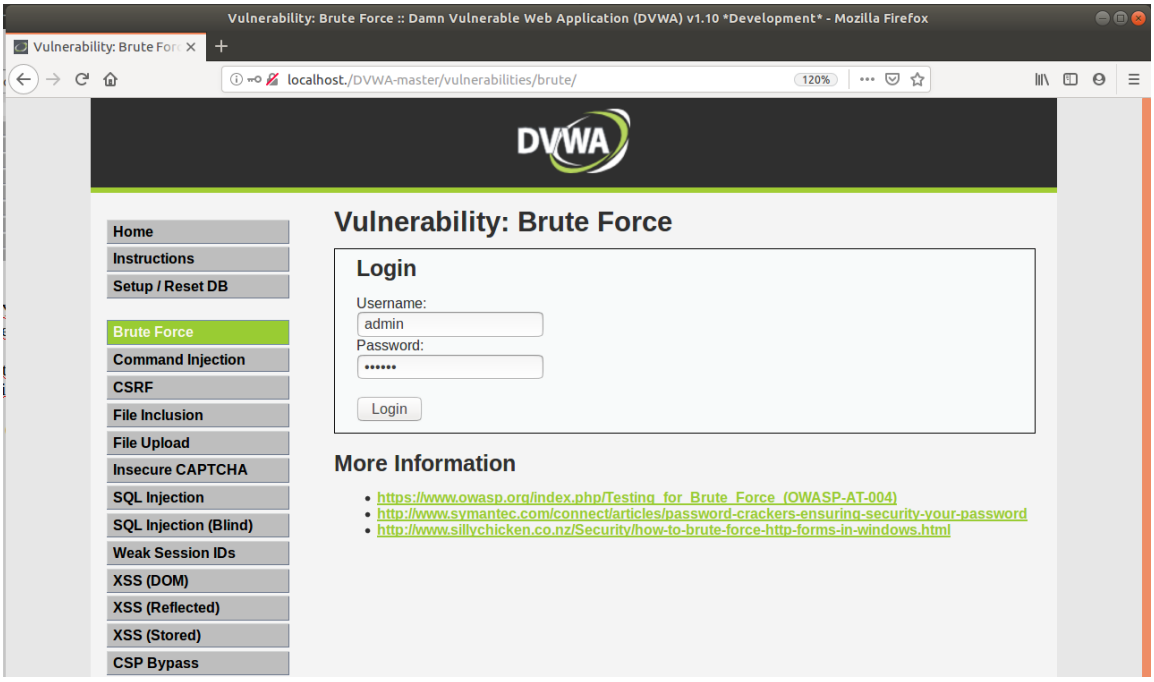
ve doğru şifre girildiğinde



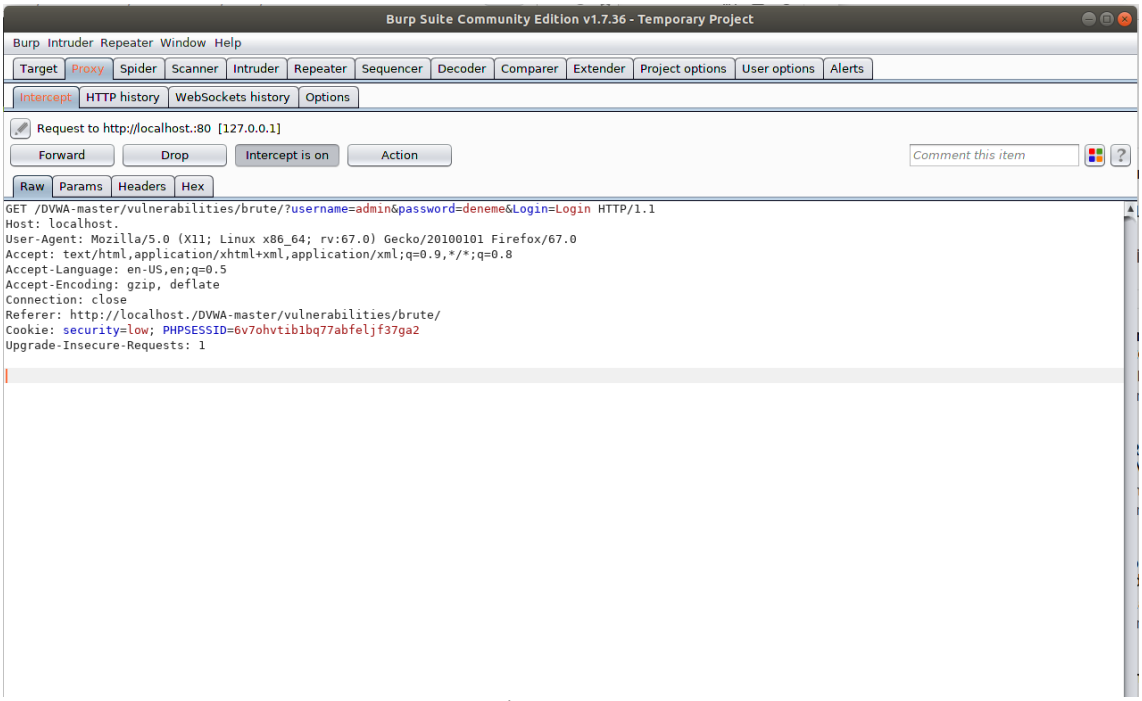
mesajları ekrana gelir. Yani yanlış şifre girildiğinde kapının dışarısındayız ve bize hata mesajı gelir. Doğru şifre girildiğinde ise içeri gireriz ve bize hoşgeldiniz mesajı gelir.

Yani Burp yazılımına eğer **grep-match** olarak **incorrect** kelimesini koyarsak tick işaretli olmayan deneme doğru şifre olacaktır, **welcome** kelimesini koyarsak ise tick işaretli olan deneme doğru şifre olacaktır. Şimdi bunu uygulayalım.

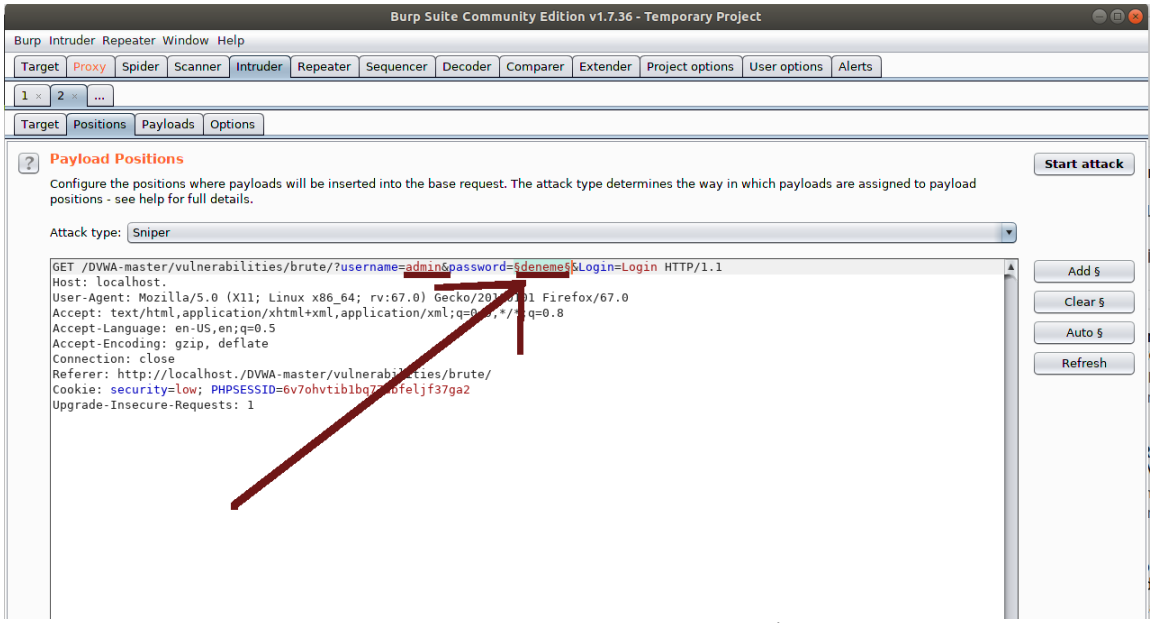
a) Burp'te Brute Force'u Hata Mesajını Referans Alarak Yapma



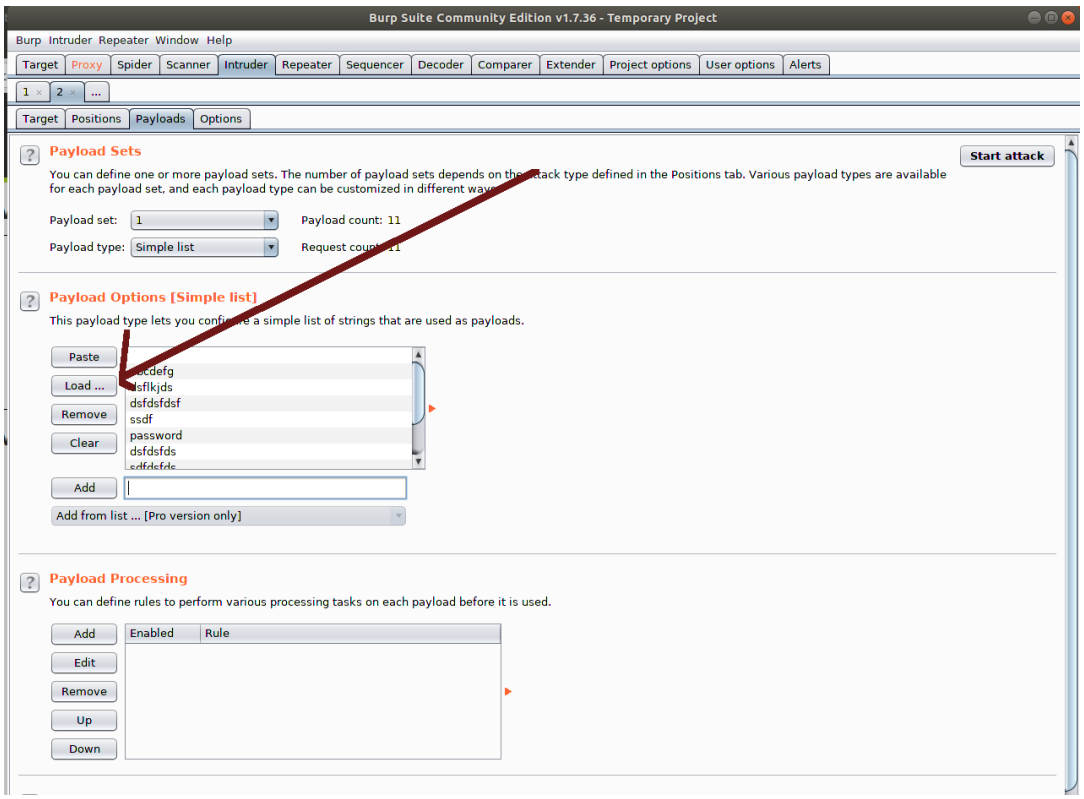
(Login Sayfası)



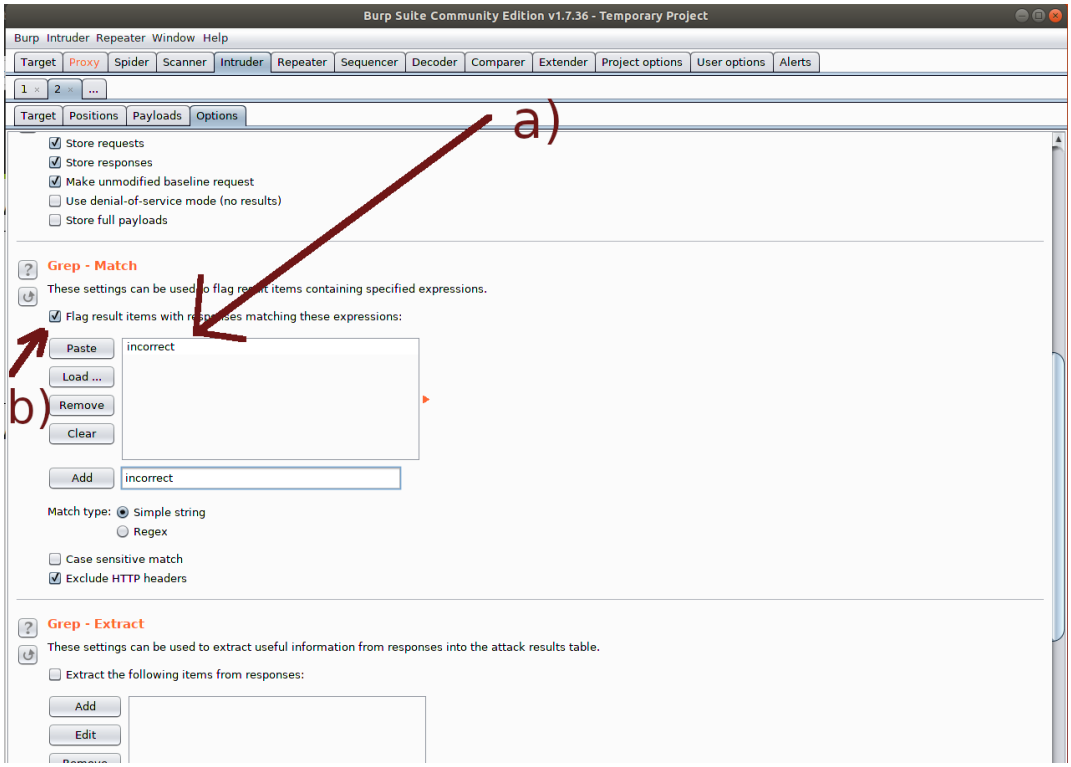
(Burp İle Araya Girilir)



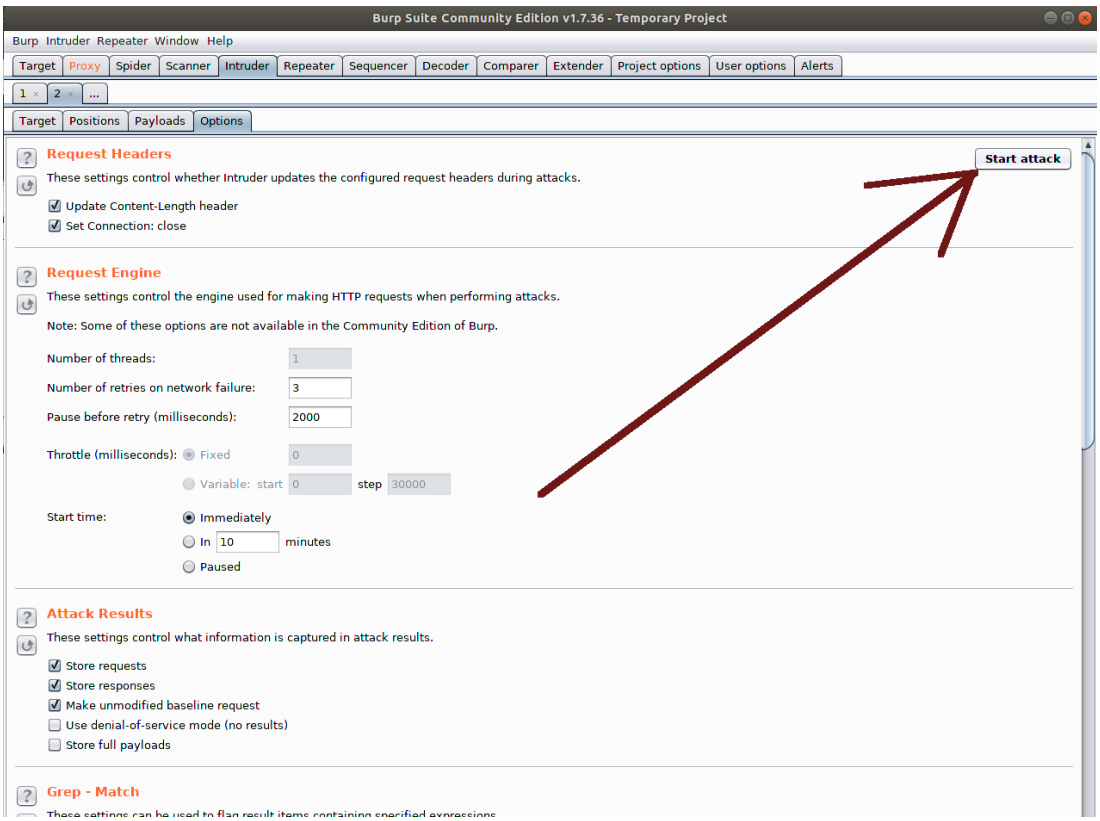
(Dictionary Attack için Şifre Parametresi İşaretlenir)



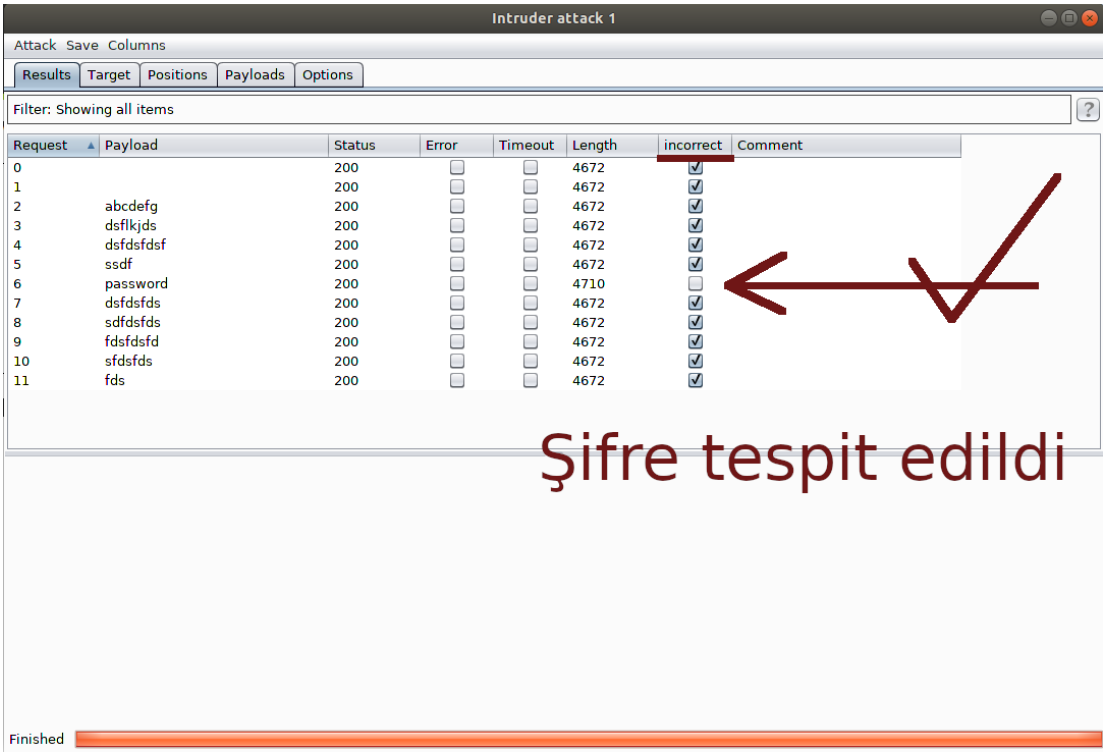
(Burp'e Sözlük Dosyası Verilir)



(Burp'e, Yanlış Denemelerde Ekrana Gelen Hata Cümlesi / Kelimesi Verilir)

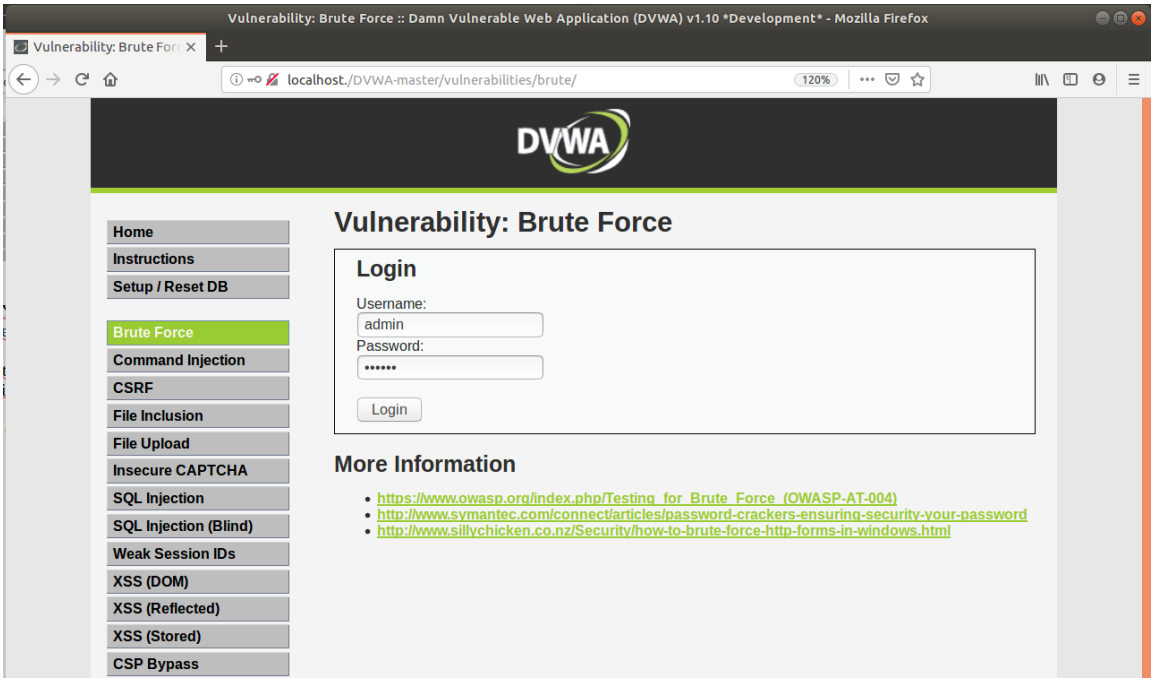


(Saldırı Başlatılır)

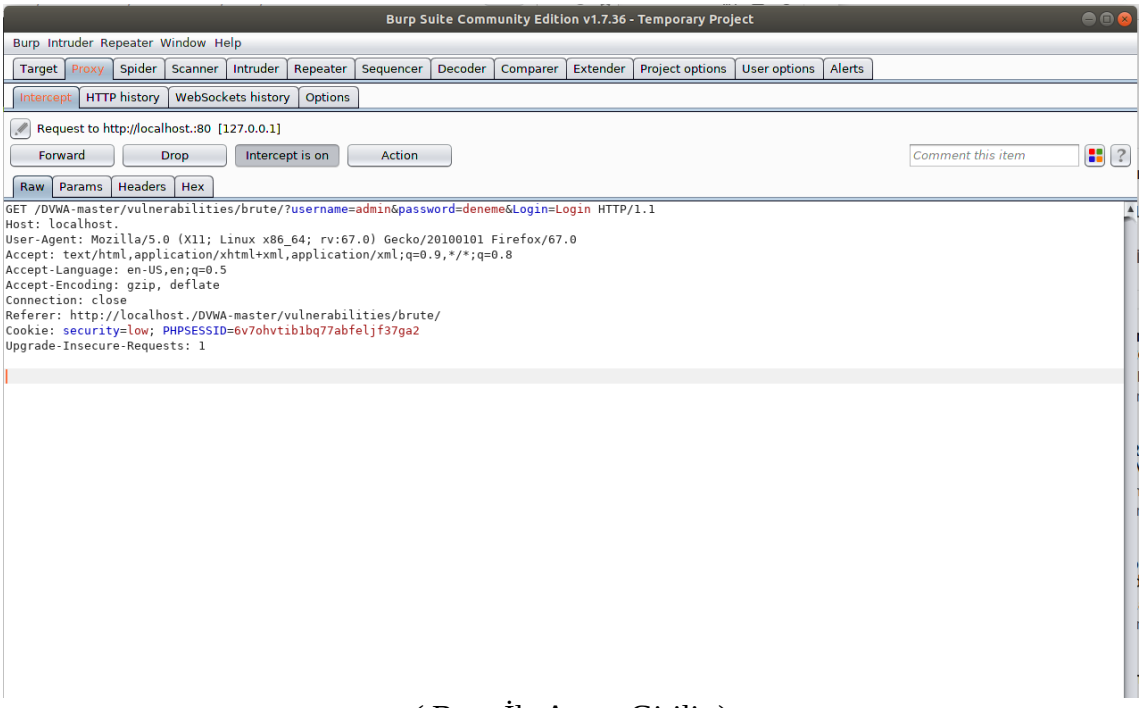


(Doğru Şifre Denemesinde Yanlış Şifre Girdiniz Tarzı Hata Kelimesi Gelmediğinden Tick İşaretsiz Olur ve Doğru Şifrenin O Olduğunu Anlarız)

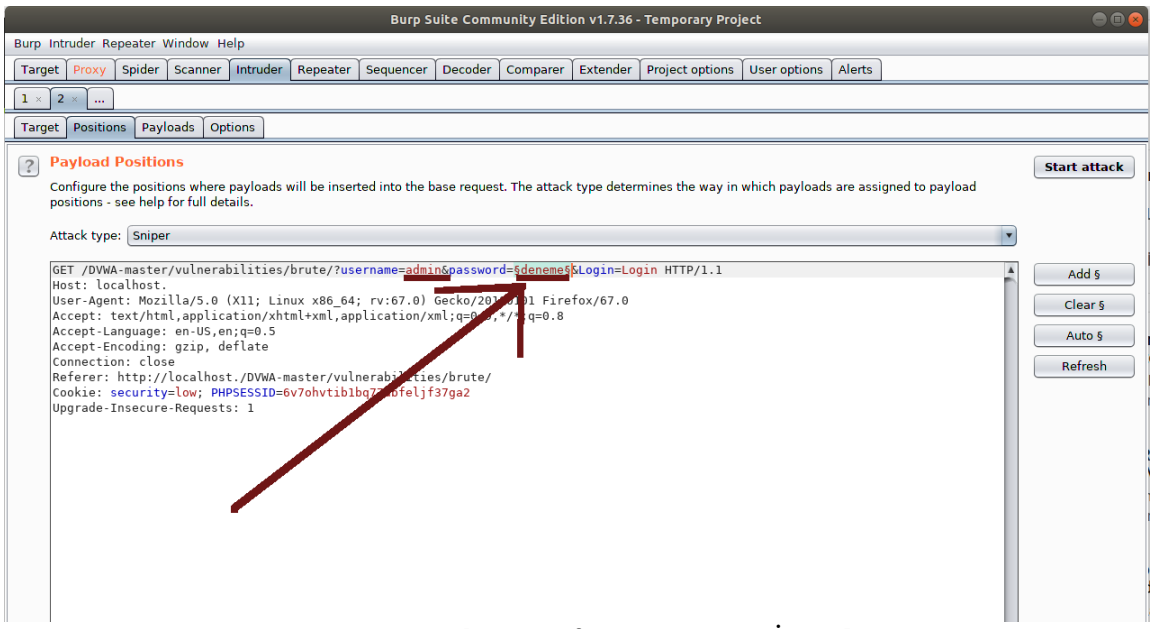
b) Burp’te Brute Force’u Oturum Açıldı Mesajını Referans Alarak Yapma



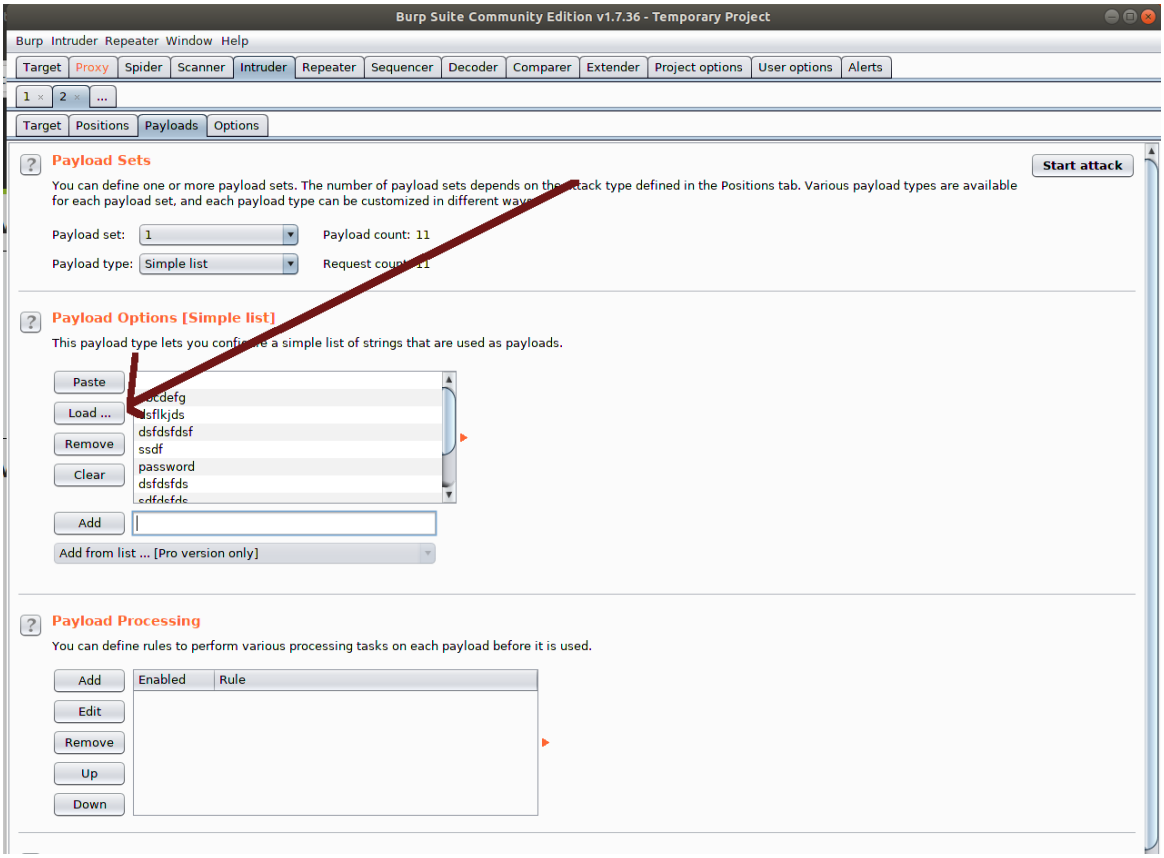
(Login Sayfası)



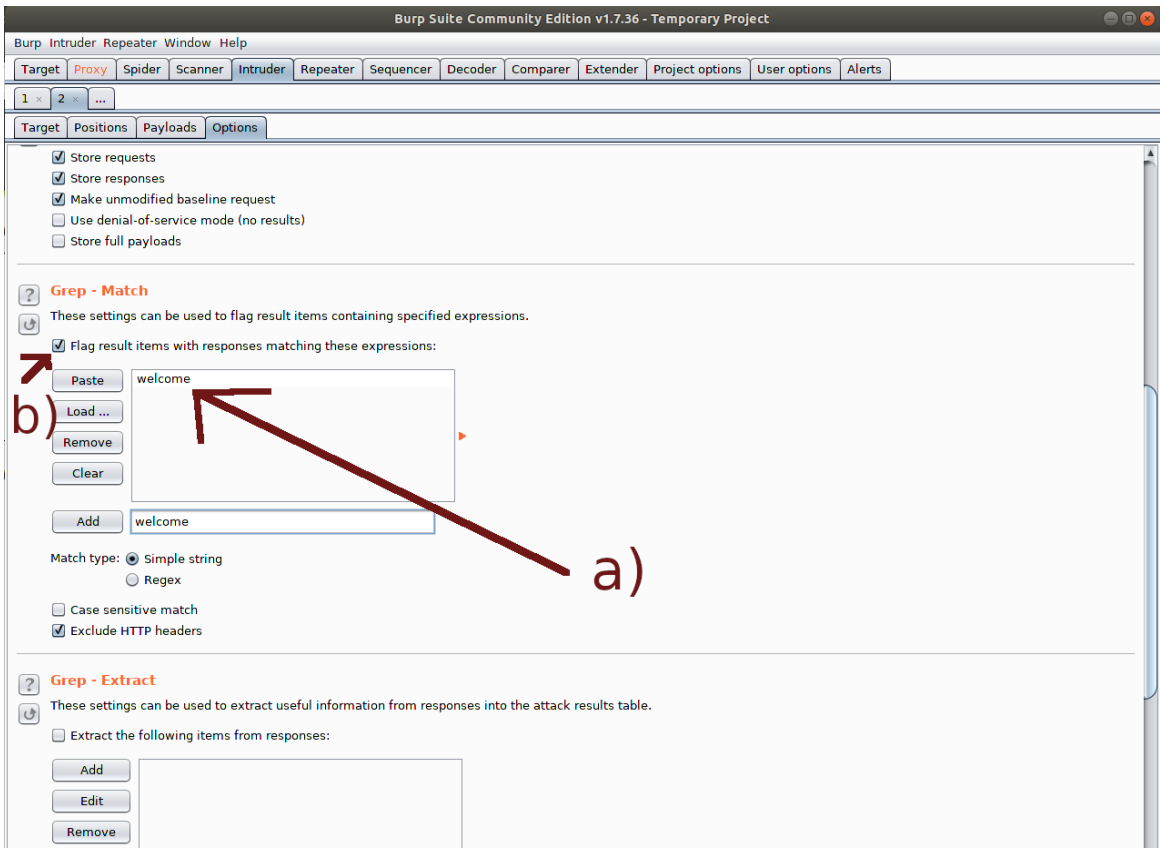
(Burp İle Araya Girilir)



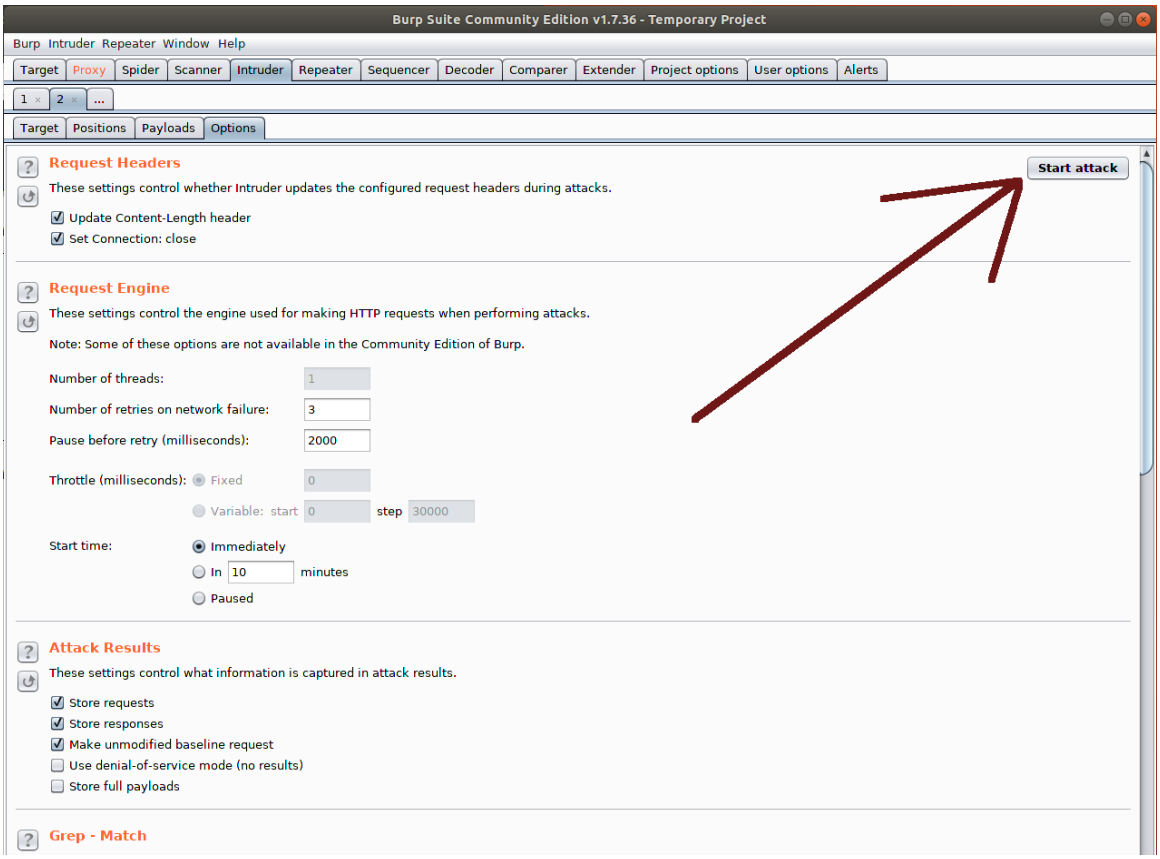
(Dictionary Attack için Şifre Parametresi İşaretlenir)



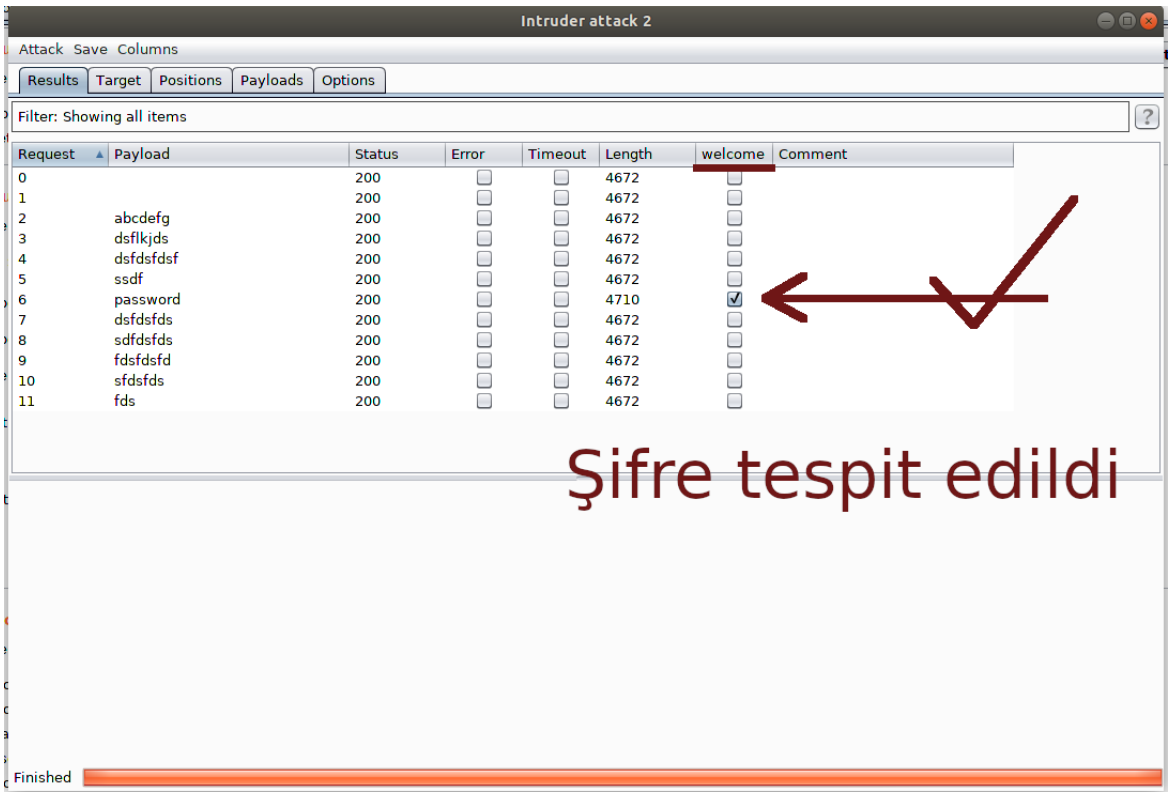
(Burp’e Sözlük Dosyası Verilir)



(Burp'e, Doğru Denemede Ekrana Gelecek Hoşgeldiniz Türünden Cümle / Kelime Verilir)



(Saldırı Başlatılır)



(Doğru Şifre Denemesinde Oturum Açıldı / Hoşgeldiniz Tarzı Olumlu Bir Kelime Geldiğinden Tick İşaretli Olur ve Doğru Şifrenin O Olduğunu Anlarız)

Kaynaklar

https://www.youtube.com/watch?v=U43o5cCVfXo