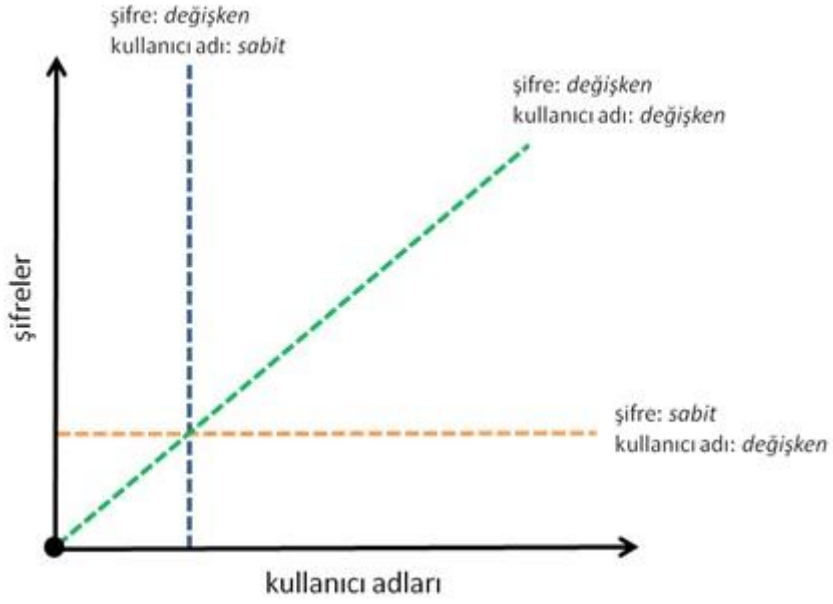
Burp Suite ile
Deneme - Yanılma Denetimi

Bedirhan Urgun, Şubat 2010, WGT E-Dergi 4. Sayı

Geçerli hesapların bulunması için kullanılan teknikler (Kaba kuvvet veya sözlük tabanlı saldırılar), tarama yöntemleri bakımından dörde ayrılırlar;

1. Yatay
2. Dikey
3. Diagonal
4. 3 boyutlu

Basitçe, dikey taramalarda kullanıcı adı sabit tutularak her denemede farklı şifre kullanılır. Yatay taramalarda ise tam tersi, şifre sabit tutularak her denemede farklı kullanıcı isimleri kullanılır. Diagonal taramalarda, her denemede farklı bir kullanıcı adı ve şifre ikilisi kullanılır. Böylece bazı sunucu taraflı hesap deneme/yanılma kontrolleri atlatılabilir. Son olarak, 3 boyutlu taramalarda diagonal tarama tipine ek olarak denemeler farklı IP adreslerinden (Bir IP havuzu olduğu düşünülürse) senkronize olarak yapılır. Bu şekilde sunucu tarafında yapılacak kontroller daha rahat atlatılabilir.



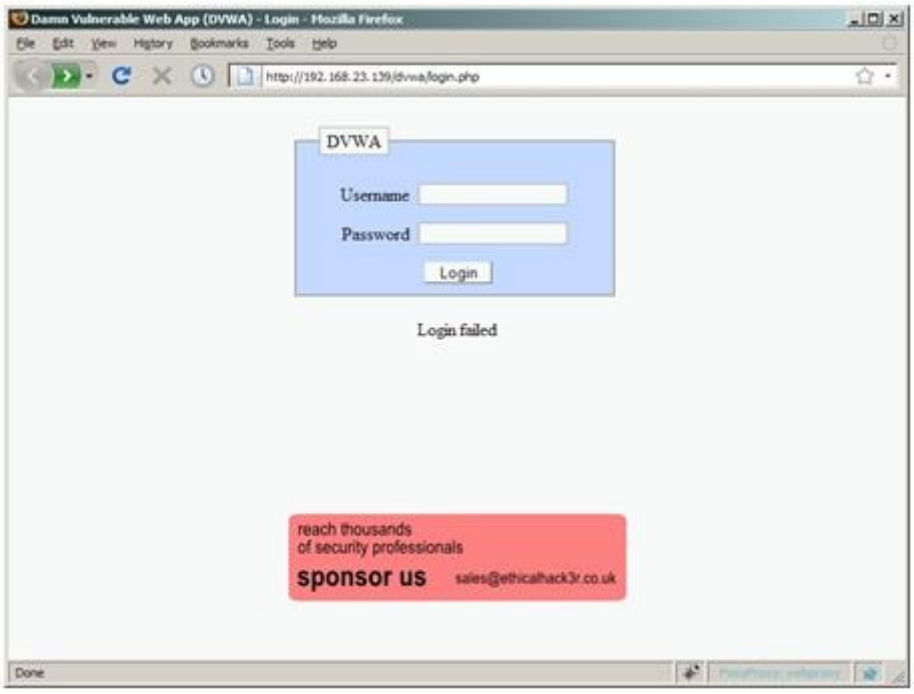
Burp Suite popüler olarak kullanılan kişisel HTTP vekillerindendir (HTTP Personal Proxy). Bu yazımızda ticari olan versiyonu, açık olan versiyonuna göre daha çok özellik barındıran bu aracın Intruder bileşenin bir bölümü anlatılacaktır. Bu bileşenin açık ve ticari olan versiyonlarındaki en önemli fark, açık olan versiyonunun hız performansının bilinçli olarak düşürülmüş olmasıdır. Yazı Burp Suite'in genel özelliklerini anlatmayacaktır.

Burp Intruder – Hibrid Dikey Tarama

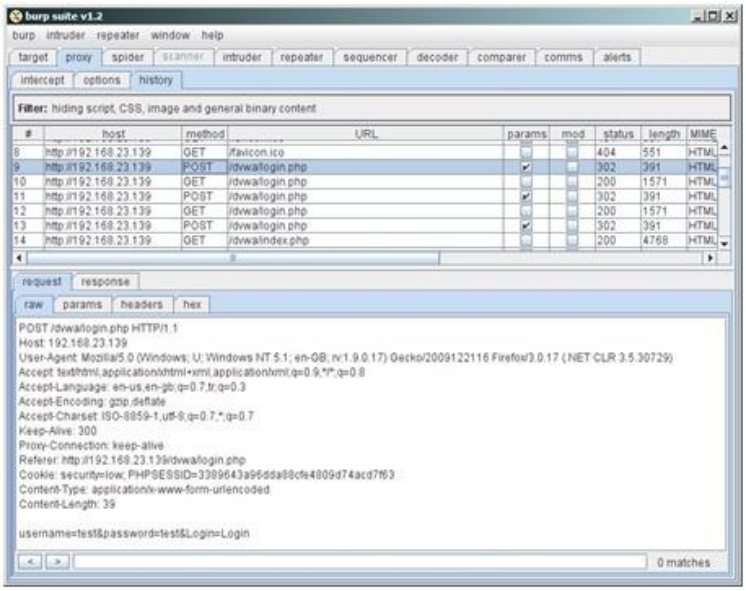
Temel olarak deneme/yanılma ile denetlenmek istenen kullanıcı adı ve şifre ikililerine, iki dosyadan gelen veriler ile toplamda girdilerin sayısının kartezyen çarpımı kadar istek gönderilir. Her iterasyonda kullanıcı adı sabit tutularak, şifre değiştirilir ve hibrid dikey bir tarama elde edilebilir.

```
foreach username in usernames.txt:
        foreach password in passwords.txt:
                brute(username, password)
```

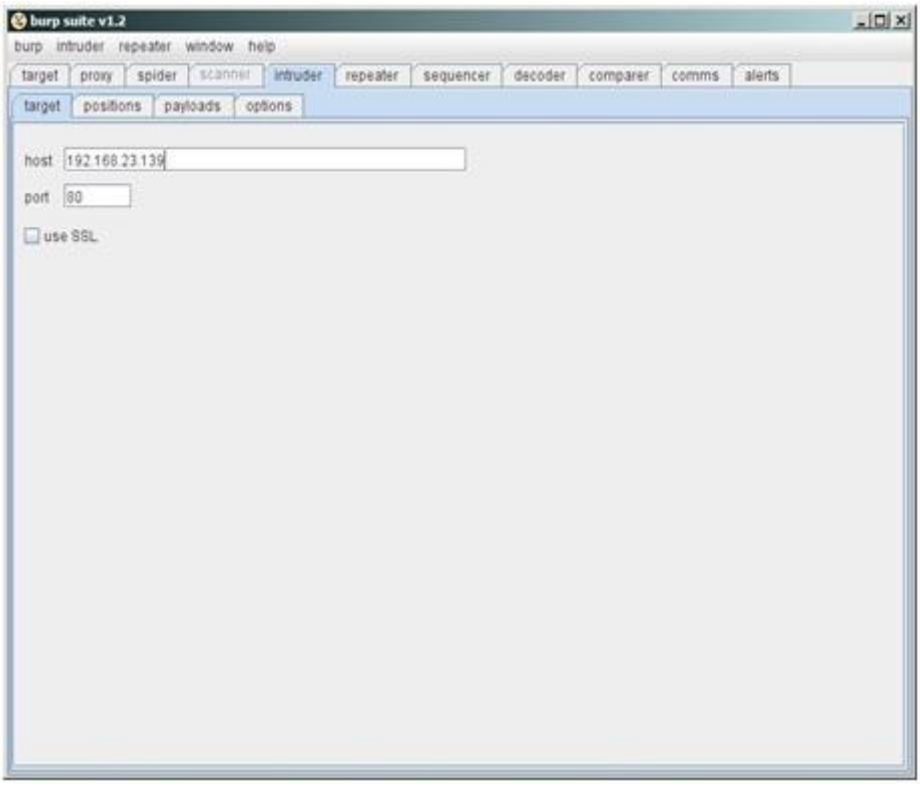
Örnek uygulamada hatalı kullanıcı adı ve şifre ikilisi "Login failed" hata mesajı ile cevaplanmaktadır.



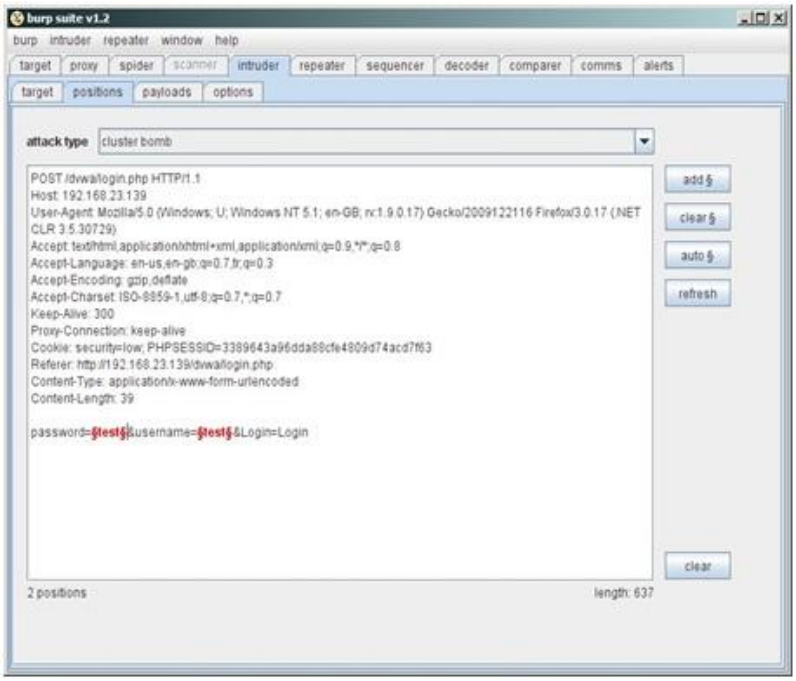
Hatalı giriş isteği Burp ile yakalandıktan sonra, POST isteği sağ tıklanarak Intruder'a gönderilir.



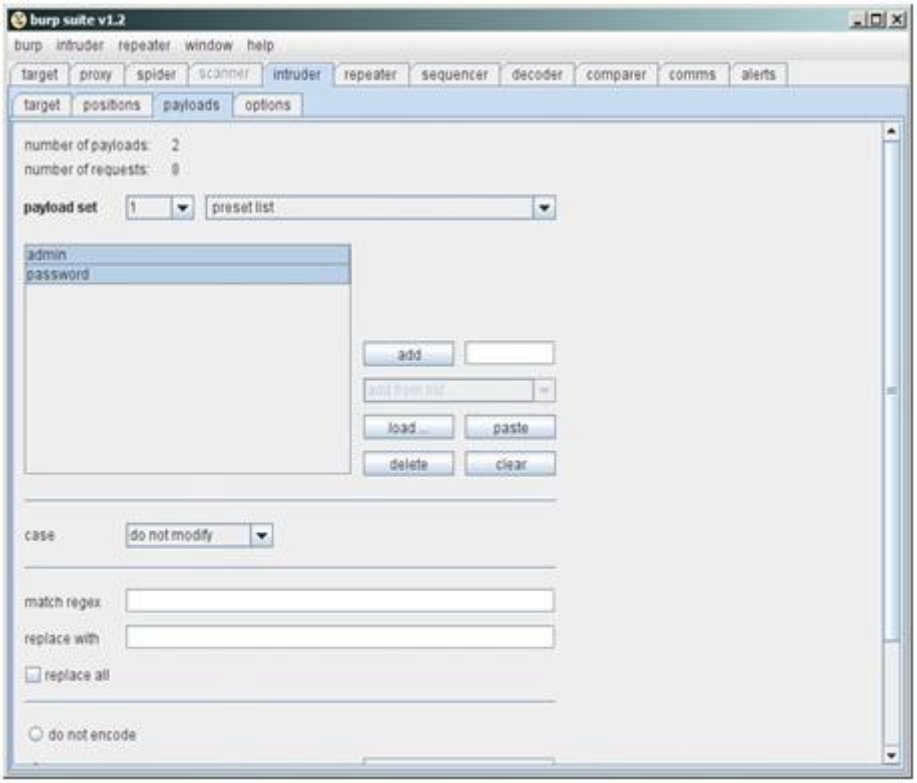
Intruder bölümünün ilk sekmesi hedefin ayarlandığı bölümdür. Bu bölümdeki bilgiler otomatik olarak doldurulur ve genellikle müdaheleye gerek kalmaz.



Intruder bölümünün ikinci sekmesi gönderilecek isteklerin şablonunun oluşturulduğu bölümdür. Bu bölümde kaba kuvvet ile denenecek değerler seçilir. Önce clear$ butonuna tıklanır, daha sonra yapılacak istekte değişmesi beklenen değerin başına gelinip, add$ butonuna tıklanır, son olarak yapılacak istekte değişmesi beklenen değerin sonuna gelinip, add$ butonuna tıklanır. Bu işlem bütün değişmesi beklenen değerler için tekrarlanır. “attack type” bölümünde “cluster bomb” seçilir.

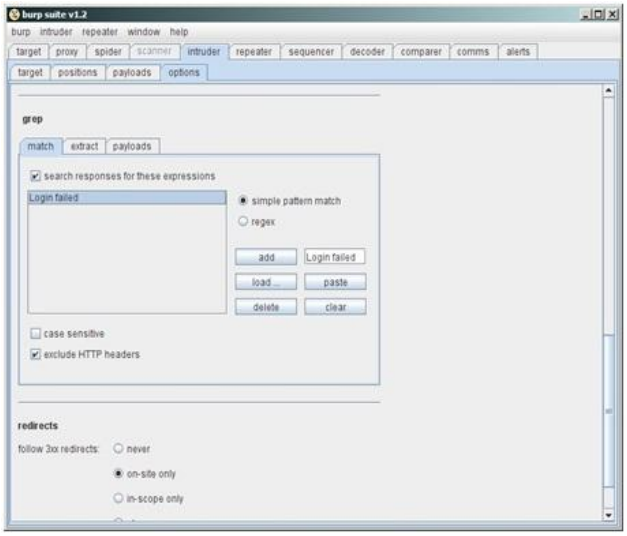


Intruder bölümünün üçüncü sekmesi denenmek istenen değerlerin sisteme tanıtıldığı bölümdür. Bu bölümde iki adet “payload set” seçilmelidir. Birinci “payload set” kullanıcı adı, ikinci “payload set” şifre için kullanılacaktır. “Payload set” tipi “preset list” olarak seçilir ve ilk payload için passwords.txt ikinci payload için usernames.txt dosyaları “Load” tuşuna basarak yüklenilir.

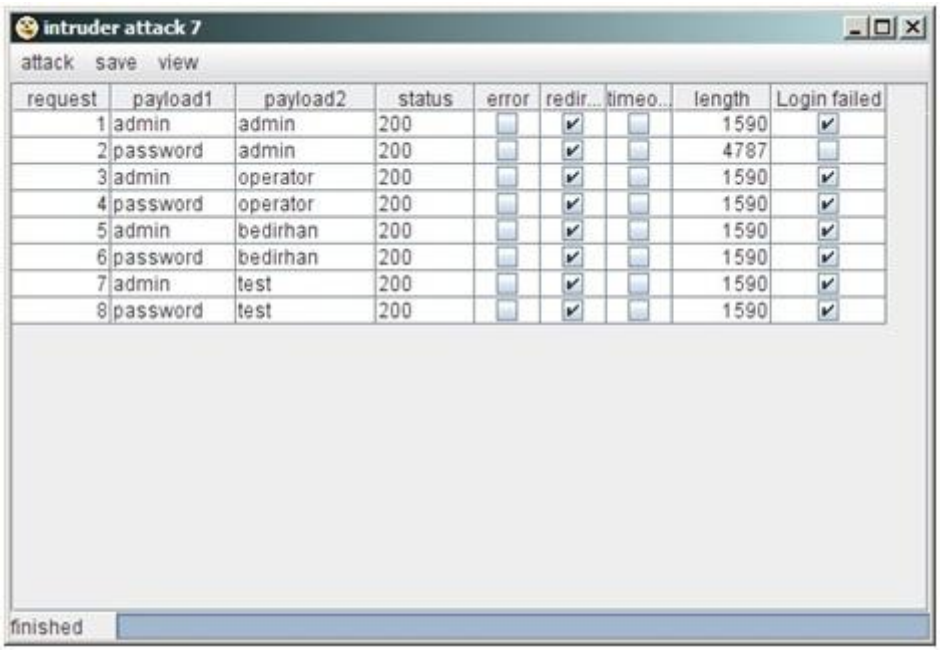


Intruder bölümünün dördüncü ve son sekmesi denemelerde oluşturulacak isteklerin ve cevapların analiz edilme ayarlarının yapıldığı bölümdür. Özellikle bu bölümde denemelerin

başarılı olup olmadığının anlaşılması için alınan cevaplarda anahtar kelimeler aranabilir. Örnekte başarısız giriş denemelerinin ürettiği “Login failed” kelimeleri kullanılmıştır.



Ayarlamalar yapıldıktan sonra Intruder başlatılır. Burp aracının profesyonel versiyonu paralıdır. Herkese açık versiyonunda bu nedenle Intruder özellikle yavaş çalıştırılmaktadır. Bu nedenle denemelerin gerçeklenmesi zaman almaktadır.



Sonuç

Kullanıcı hesabı deneme/yanılma denetimlerinde en önemli adım bu işlemin otomatize edilmesidir. Kırılması zor (OCR veya replay saldırılarına bağışık) bir CAPTCHA veya (IP-İstek kısıtlaması gibi) anti-brute force tekniği ile bu saldırılardan belli bir dereceye kadar korunmak mümkündür.