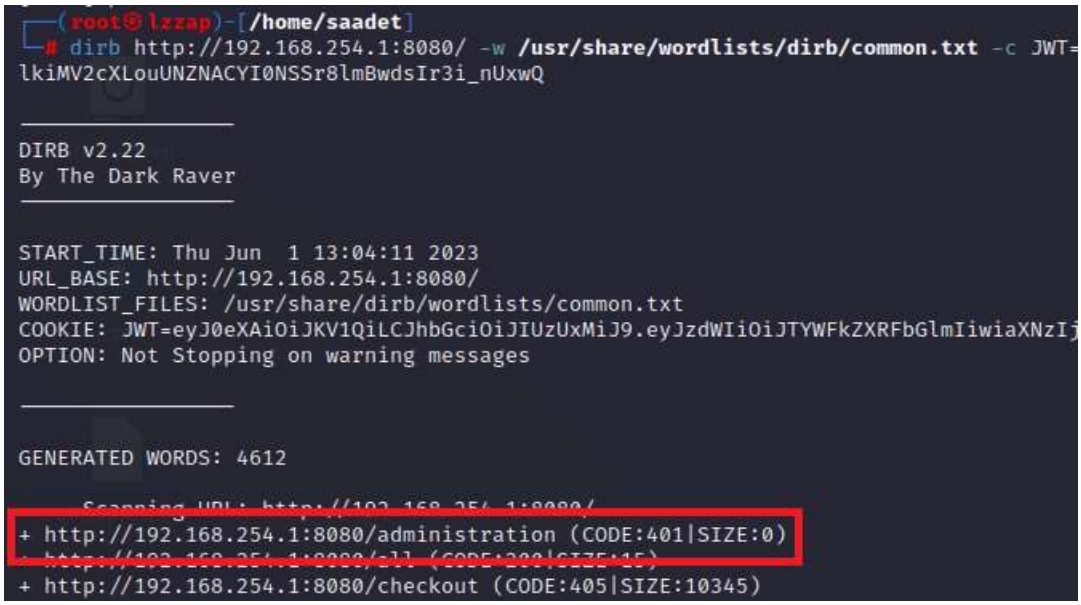
Security Misconfiguration

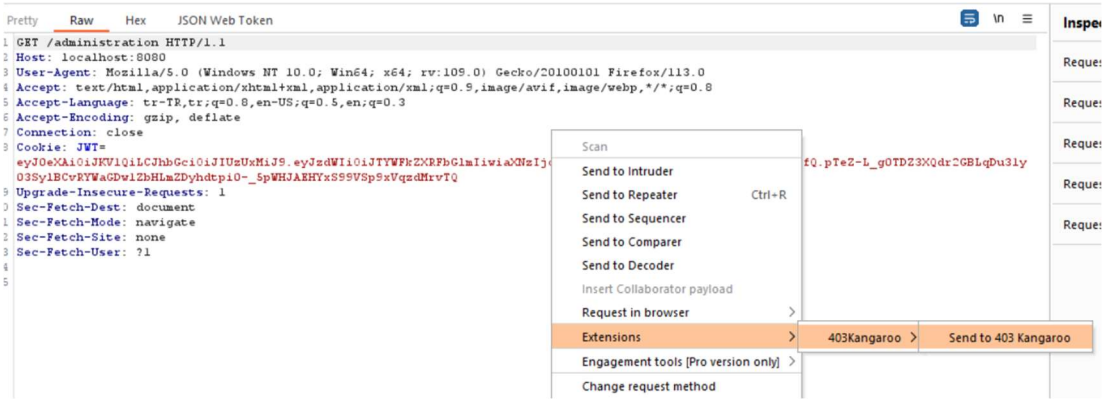
Güvenliğin yanlış konfigüre edilmesi çok geniş bir zafiyet alanıdır. Farklı uygulamalar ve farklı teknolojiler için farklı şekillerde ortaya çıkabilir. Güvenlik önlemi alınırken bu güvenlik önleminin yanlış konfigüre edilmesi, olası diğer senaryoların düşünülmemesinden ve saldırganın da siteyle normal bir kullanıcı gibi etkileşime geçeceğinin düşünülmesinden kaynaklanır. X-forwarded-for gibi başlıklar genelde kullanıcı başka bir proxy üzerinden siteye geliyorsa sitenin kullanıcının ana IP adresini öğrenmesi için kullanılır örneğin arada bir sunucu varsa ve bu kullanıcı önce o sunucuya gelip isteği o sunucu üzerinden ana sunucuya yönlendiriliyorsa aradaki sunucuya bir x-forwarded-for başlığı eklenir ve bu başlık değerine ana sunucuyu ziyaret etmek isteyen kullanıcının IP değeri eklenir. Eğer uygulama bu headerda bulunan değerleri kullanıcının gerçek IP adresi olarak set etmek isterse geliştirici bu değerin ve başlığın bir saldırgan tarafından set edilebileceğini göz ardı ederek güvenlik konfigürasyonunu hatalı yaptığı anlamına gelir.

HYGIEA projesinde bulunan misconfiguration örneği admin kullanıcısının sahip olduğu yönetim paneline(Kullanıcıları silme işleminin olduğu panel) sadece “Admin” yetkilerine sahip olan kullanıcıların veya local IP adresinden erişebilmesi üzerine tasarlanmıştı. Burada sistem arkada hatalı bir şekilde kullanıcının IP değerini X-Forwarded-For başlığı varsa oradan gerçek IP değeriymiş gibi set ediyordu. Ardından bu IP değerinin izin verilen IP listesinde olup olmadığını veya giriş yapmaya çalışan kullanıcının admin yetkisine sahip olup olmadığını kontrol ediyordu. İki durumdan biri doğru olduğu sürece saldırgan proxy ile araya girerek bir X-forwarded-for:127.0.0.1 değerini verdiğinde normalde 401 yetkisiz cevabı dönen uygulama 200 dönerek kullanıcıya yönetim panelini gösteriyodu. Adımları görselli olarak açıklamak gerekirse;
Öncelikle uygulamaya dizin taraması yapıyoruz.



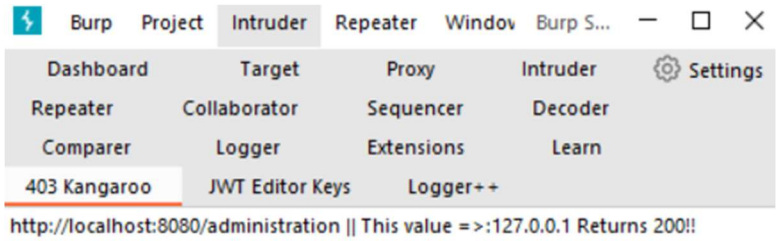
Şekil 1.1 /administration dizininin bulunması

Burada administration dizinine erişim yetkimiz olmadığını belirten 401 mesajını aldığımızı görebiliriz burada saldırgan tercih olarak manuel olarak kullanabileceği bypass headerlarını ve değerlerini de kullanabilir. Biz staj döneminde Elif arkadaşımızın yazdığı 403 Kangaroo burp suite eklentisini kullanacağız.



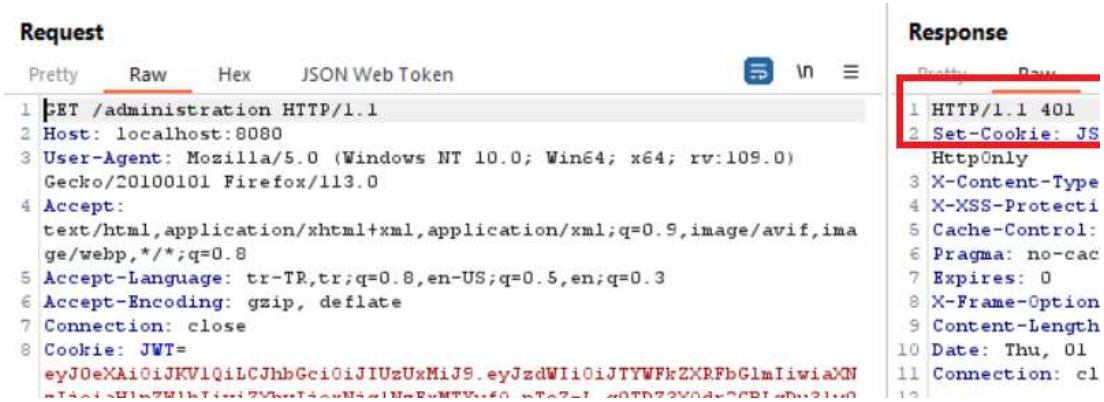
Şekil 1.2 isteğin burp uzantısına gönderilmesi

Bu araç içinde bulunan bypass headerlarına sırasıyla 127.0.0.1, 0.0.0.0 ve localhost değerlerini ekleyerek istek gönderiyor ve uygulama 401 yerine 200 dönerse hangi deüer kullanılarak uygulamanın 300 döndüğünü yazıyor. Ardından test yaparken bypass headeları ile birlikte değer girilerek hangi header'ın yanlış konfigüre edilerek bypass'a olanak sağladığını bulabiliriz.



Şekil 1.3 403Kangaroo dashboard

İsteği gönderdikten sonra yukarıdaki gibi burp suite üzerine eklenmiş 403 kangaroo sekmesinde 127.0.0.1 değerinin 200 OK cevabını döndüğünü görebiliriz. Burada headerları 127.0.0.1 başlığıyla gönderirsek erişim sağladığımızı görebiliriz . Öncelikle yetkisiz olduğumuzu gösteren isteğe bakalım ve ardından isteğe headerımızı ekleyerek bakalım:



Şekil 1.4 Yetkisiz istek cevabı

Yukarıda admin yetkisine sahip olmayan SaadetElif kullanıcısıyla istek gönderdiğimizde header olmadan erişim yetkimiz omayan admin
Strator dizinine erişemediğimizi görebiliriz. Ardından isteğe header değerimizi ekleyelim:

Şekil 1.5 Yetkisi bypass edilmiş istek cevabı

Header değerini eklediğimizde başarılı bir geri dönüş aldığımızı görebiliriz.