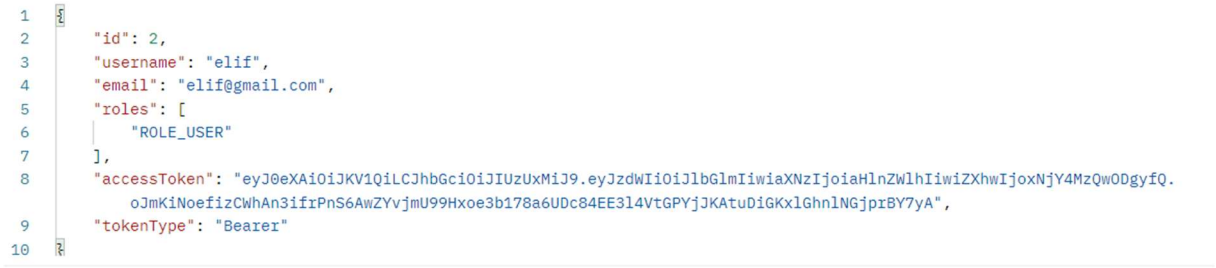
Improper Authentication via Weak Signing Key

Uygulamada planladığımız şekilde bu kısmı geliştirdiğimiz için bu bölümde uygulama da bulunan zafiyet nedeniyle birlikte anlatılmaktadır.
Improper Authentication zafiyeti saldırgan bir kullanıcıyı taklit etmeye çalıştığında uygulamanın bu iddianın sahte olduğunu anlamaması / kanıtlayamamasından kaynaklanır. Uygulama saldırganın hedef aldığı kullanıcıyı taklit ederek kullanıcının hesabına erişim sağlamasına izin verir.

Weak Signing Key zafiyeti ise JWT gibi teknolojilerde veya içinde şifreleme için anahtar kullanılan algoritmalarda anahtarın tahmin edilebilir ve brute-force uygulanarak elde edilebilir olması demektir. Saldırgan böylelikle elde ettiği anahtar değerini kullanarak eğer bir iletişim gerçekleşiyorsa iletişimin içeriğine erişim sağlayabilirken, eğer kimlik doğrulama gerçekleşiyorsa saldırgan bir kullanıcının hesabına erişim sağlayabilir.
Örneğin a.com sitesi kullanıcılar giriş yaptıktan sonra hepsine bir JWT token'ı atasın;
Elif kullanıcısının giriş isteği;

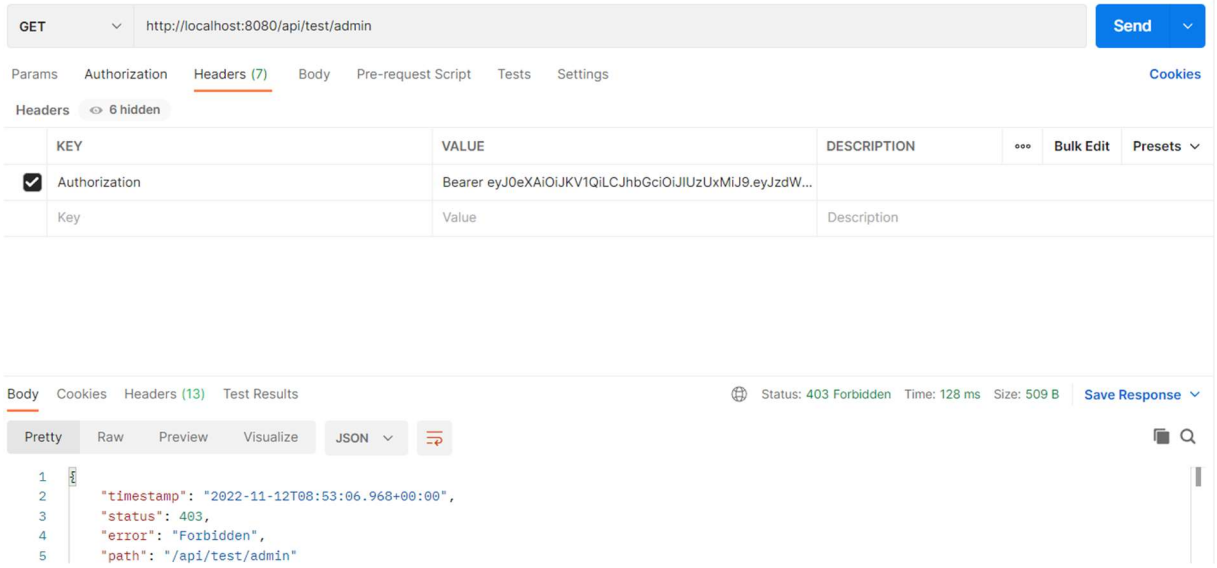
Şekil 1.1 login isteği

Sunucudan elif kullanıcısına dönen cevap;



Şekil 1.2 sunucunun başarılı giriş isteğine cevabı

Yukarıdaki görselde accessToken parametresini ve kullanıcıya verilen JWT değerini görebiliriz. Bu değer ile sadece “admin” kullanıcısının erişimi olan “Admin Board” kısmına erişim denendiğinde sunucudan erişim izni olmadığı ile ilgili bir cevap döndüğünü görebiliriz;



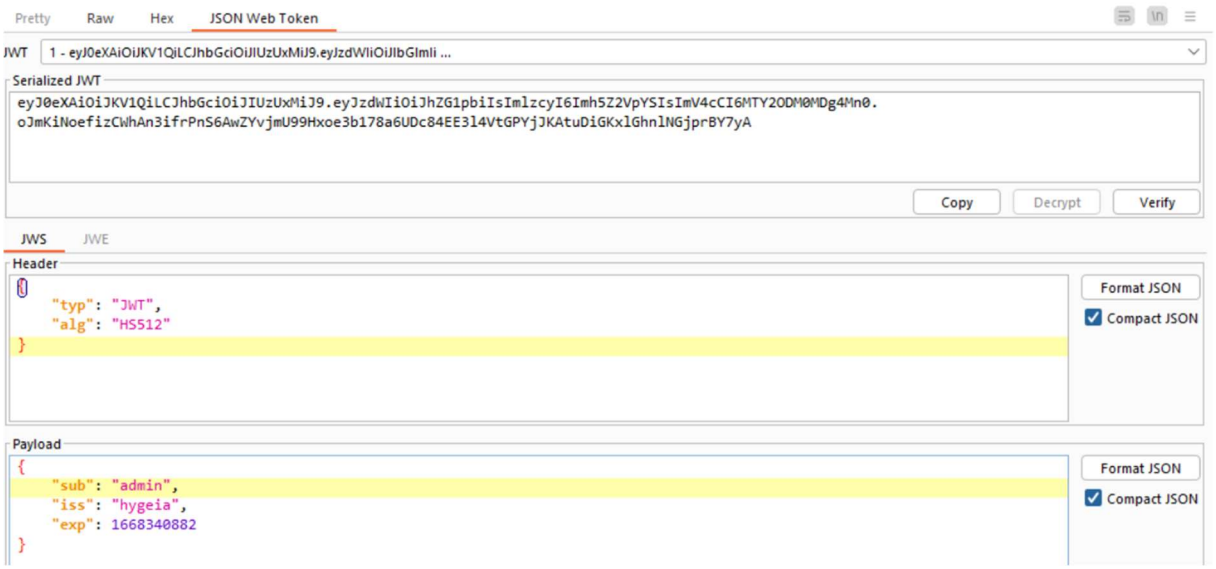
Şekil 1.3 admin portalına yetkisiz erişim isteğine dönen cevap

Elif kullanıcısına ait token değerine “Hashcat” aracı ve “wfuzz/common_pass.txt” kelime listesi ile sözlük saldırısı yapılırsa;

Şekil 1.4 token’a yapılan sözlük saldırısının sonucu

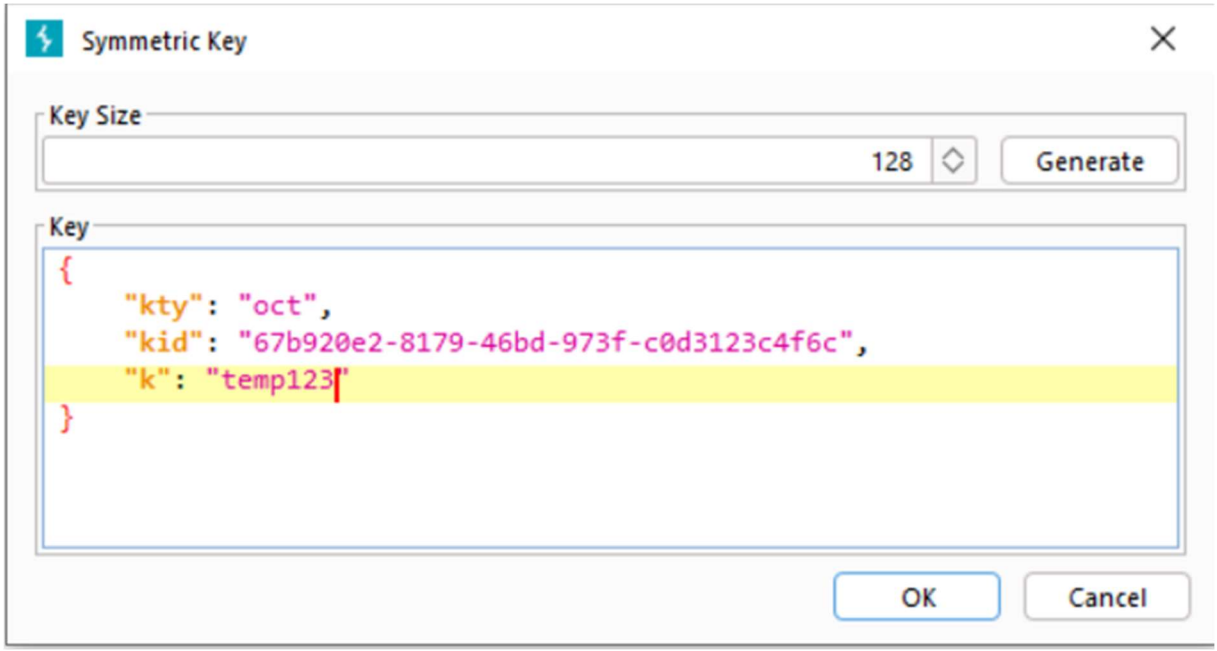
JWT şifrelenmesi için kullanılan anahtarın “temp123” değeri olduğu görülür.

Öncelikle JWT değerinin içindeki kullanıcı adı elif kullanıcısından admin kullanıcısına çekilmelidir.



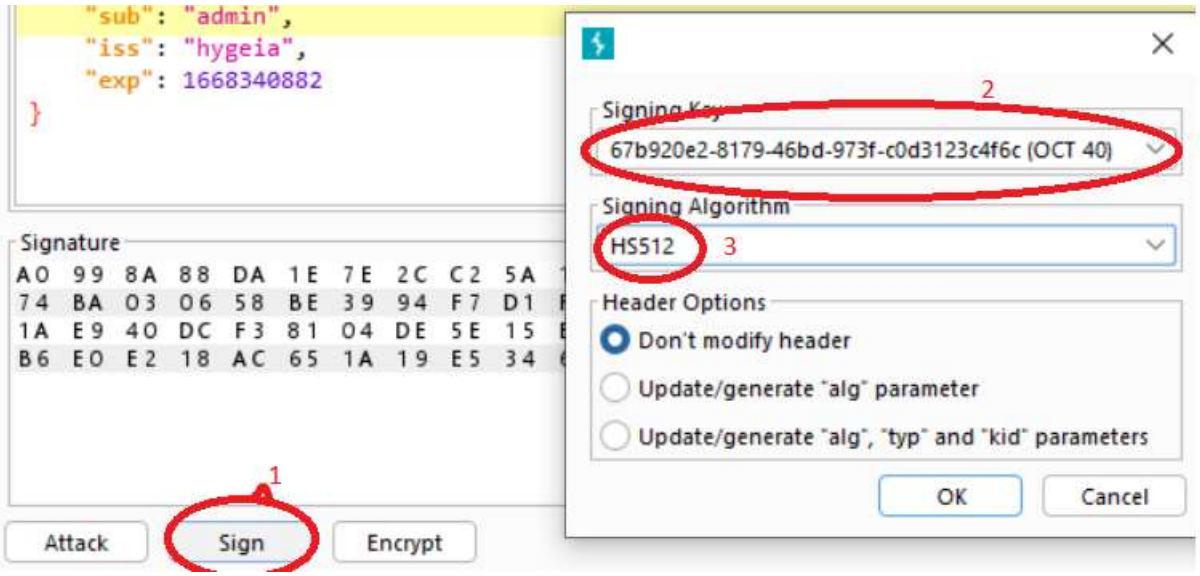
Şekil 1.5 JWT değerlerinin değiştirilmesi

Ardından simetrik bir anahtar oluşturularak içine “temp123” değeri atanmalıdır;



Şekil 1.6 sözlük saldırısında elde edilen anahtar değerinin girilmesi

Kullanıcı adının “admin” olarak değiştirildiği istek oluşturulan bu anahtar ile imzalanır;

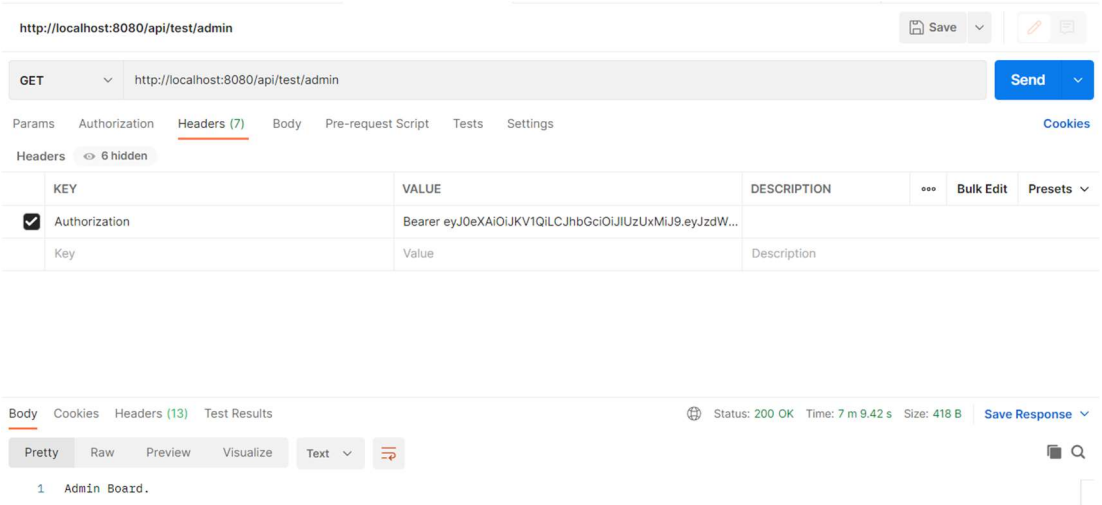


Şekil 1.7 Saldırgan tarafından token'ın imzalanma aşamaları

(2) temp123 değerini verdiğimiz anahtar.

(3) Elif kullanıcısından aldığımız JWT üzerinde görülen şifreleme algoritması.

JWT değerini imzalama işlemini gerçekleştirdikten sonra ise "admin" kullanıcısının hesabına giriş yapabildiğimiz için "Admin Board" sayfasını görebiliriz.



Şekil 1.8 admin kullanıcısının erişimi olan sayfaya başarılı giriş isteği