Teknolojik gelişmelerin toplumun her kesimine hitap etmesi, çeşitli ihtiyaçlarıda beraberinde getirmektedir. Günlük hayatı zorlaştıran birçok hizmet artık web ve mobil uygulamalar ile yapılabilirken yazılımların son yıllarda çeşitlenmesiyle farklı sistemler arasında veri transferleri de ihtiyaç haline gelmiştir. Farklı sistemlerdeki veritabanlarının birbirleriyle platform bağımsız bir şekilde haberleşebilmeleri için web servisleri kullanılmaktadır. Web servislerindeki güvenlik ve gizlilik web uygulamalarında olduğu gibi oldukça önemlidir. Kullanıcılar, hayati önem taşıyan işlemleri online sistemler üzerinde, verilen hizmetlere güvenerek işlemlerini gerçekleştirmektedir. Geliştirilen web servis uygulamalarında, güvenlik önlemlerinin yazılımın ilk süreçlerinden itibaren dikkate alınması, güvenlik risklerini azaltmaktadır. Web servis uygulamalarının tek bir test modeline göre değerlendirilmesiyle, muhtemel açıklıklar yeterince tespit edilememektedir. Bu çalışmada, web servislerinin güvenliğini test etmek için geliştirilen hibrit model açıklanmaktadır. Hibrit modelde güvenlik testleri sırasında kullanılan statik ve dinamik analizin yanında gözden geçirme yöntemi dahil edilerek, otomatize araçların bulamadığı açıklıklartespit edilmektedir. Bu sayede web servislerinin geliştirilmesi sırasında dikkat edilmesi gereken bölümler tespit edilebilmektedir. Çalışma kapsamında web servislerinde olması gereken kimlik denetimi ve uygulama dillerine bağlı olarak oluşabilecek güvenlik açıkları örnek kodlarla birlikte anlatılmaktadır. Son olarak geliştirilen model ile test web servisleri, açık kaynak yazılımlar ve gözden geçirme yöntemiyle test edilerek, önerilen modelin geçerliliği test edilmektedir.