TÜRK BİLİM ARAŞTIRMA VAKFI
TÜBAV
1995
TURKISH SCIENCE RESEARCH FOUNDATION

Yıl: 2023, Cilt:16, Sayı:1, Sayfa: 17-23

SQL ENJEKSİYONU SALDIRILARININ MAKİNE ÖĞRENMESİ İLE TESPİTİ

Emre POLAT*, Halil İbrahim BÜLBÜL**

* Gazi Üniversitesi, Bilgi Güvenliği Mühendisliği ABD Yüksek Lisans Öğrencisi, emre.polat@gazi.edu.tr
** Gazi Üniversitesi, Bilgi Güvenliği Mühendisliği ABD Öğretim Üyesi, bhalil@gazi.edu.tr

ÖZET

Veri tabanı sistemleri, birbirleriyle ilişkili bilgilerin ya da verilerin tablolar halinde yapılandırılmak suretiyle depolandığı elektronik sistemlerdir (Elmasri & Navathe, 2010). Günümüzde veri tabanı sistemlerinden, yemek siparişinden bankacılık işlemlerine, otel rezervasyon işlemlerinden e-devlet işlemlerine, sağlık işlemlerinden sigortacılığa kadar uzanan çok geniş bir yelpaze içerisinde istifade edilmektedir. Ayrıca bu sistemler üzerinde devletin gizli ve hizmete özel gizlilik dereceli bilgileri, kurum / kuruluşlara ait özel veriler ile birlikte kişilerin nüfus bilgileri, ikametgâh bilgileri, iletişim bilgileri, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi, vakıf ya da sendika üyeliği, sağlığı, fotoğrafı, parmak izi gibi özel nitelikli verileri muhafaza edilmektedir. Dolayısıyla veri tabanı sistemlerinin başta SQL enjeksiyonu saldırıları olmak üzere muhtemel tehditlere karşı korunması çok önemli bir konu halini almıştır.

Bu çalışmada, SQL enjeksiyonu saldırılarının tespit edilmesinde birbirinden farklı iki veri seti kullanılmak suretiyle makine öğrenmesi uygulaması önerilmiş ve literatürde yer alan tespit ve korunma yöntemleri incelenmiştir.

Anahtar Kelimeler: SQL Enjeksiyonu Saldırısı, Siber Saldırı, Makine Öğrenmesi

DETECTING SQL INJECTION ATTACKS WITH MACHINE LEARNING

ABSTRACT

Database systems are electronic systems in which information or data related to each other is stored by structuring in tables (Elmasri & Navathe, 2010). Today, database systems are used in a wide range from food ordering to banking transactions, from hotel reservations to e-government transactions, from health transactions to insurance. In addition to the confidential and service-specific confidential data of the state, private data belonging to institutions / organizations, as well as personal population information, residence information, contact information and ethnic origin, political thought, philosophical belief, religion, foundation or private data such as union membership, health, photographs, fingerprints are preserved on these systems. Therefore, the protection of database systems against possible threats, especially SQL injection attacks, has become a very important issue.

In this study, machine learning application has been proposed by using two different data sets to detect SQL injection attacks and detection and prevention methods in the literature have been examined.

Keywords: SQL Injection Attack, Cyber Attack, Machine Learning

1. GİRİŞ

Web uygulama güvenliği alanında faaliyet gösteren bir topluluk olan Açık Web Uygulama Güvenliği Projesinin 2021 yılında yayınladığı raporda, SQL enjeksiyonu saldırıları bilgisayar korsanları tarafından en çok tercih edilen saldırı yöntemlerinden birisi olarak gösterilmiştir (OWASP, 2022). Yine Açık Web Uygulama Güvenliği Projesi tarafından test edilen uygulamalarda 2021 yılı içerisinde yaklaşık 274.000 SQL enjeksiyonu saldırı girişimi tespit edilmiştir (Crowdstrike, 2022). Ayrıca yapılan bir başka araştırmada (Venturebeat, 2022), eğitim alanındaki web uygulamalarının %35'inin, devlet kurumlarına ait web uygulamalarının %32'sinin ve sanayi alanında hizmet sunan web uygulamalarının %22'sinin SQL enjeksiyonuna karşı zafiyet barındırdığından bahsedilmektedir.

Bu çalışma kapsamında, SQL enjeksiyonu saldırılarını tespit ve önlemede kullanılan yöntemlerle ilgili literatürde yer alan çalışmalar, kodlama pratikleri ile tespit ve önleme sistemleri başlıkları altında ele alınmıştır. Yapılan değerlendirmeler neticesinde, SQL enjeksiyonu saldırılarının tespitinde makine öğrenmesi yardımı ile daha etkili bir tespit yönteminin elde edileceği önerilmektedir. Bu bilgilerden hareketle makine öğrenmesi kullanılarak SQL enjeksiyonu saldırı tespiti çalışması yapılmıştır. Bu çalışmanın bugüne kadar yapılan çalışmalardan farkı makine öğrenmesi uygulamasında iki farklı veri seti kullanılmış olmasıdır. Böylelikle sınıflandırma algoritmaları ile oluşturulan modellerin güvenilirliğinin arttırılması hedeflenmiştir. SQL enjeksiyonu saldırısının kullanıcı girdisi vasıtasıyla gerçekleştirildiği varsayılmıştır.

2. SQL ENJEKSİYONU SALDIRILARI

SQL enjeksiyonu saldırısı, veri tabanına dayalı çalışan web uygulamalarının zafiyetlerini SQL deyimlerinin içerisine yerleştirilen birtakım ifadelerle istismar etmek suretiyle gerçekleştirilen bir çeşit siber saldırı türüdür (Laval vd., 2016). Yapılan bir başka tanıma göre ise SQL enjeksiyonu saldırıları, zararlı ifadeler içermeyen SQL deyimlerinin içerisine bazı semboller, deyimler ve ifadeler yerleştirerek sistemin manipüle edilmesi olarak görülmektedir (Avcı vd., 2021).

SQL enjeksiyonu saldırıları ilk olarak 1998 yılında web güvenliği ile ilgili yayın yapan bir dergi sayesinde duyulmuştur (Forristal, 1998). Günümüzde ise SQL enjeksiyonu saldırıları web uygulamalarına yönelik en tehlikeli saldırılar arasında kendisine yer edinmiştir. Çünkü hassas ve kişisel verilerin tutulduğu veri tabanları, SQL enjeksiyonu saldırılarına karşı zafiyeti bulunan web uygulamaları vasıtasıyla bilgisayar korsanlarının tam yetki ile erişimine açılabilmektedir (Jemal vd., 2020).

SQL enjeksiyonu saldırılarının temel nedeni, kullanıcı tarafından yapılan girdinin tam olarak doğrulanmamasıdır (Alwan & Younis, 2017). Halbuki kod yazım sürecinde geliştiricilere veri doğrulamanın uygun bir şekilde ve tam olarak yapılması maksadıyla birçok kaynak sunulmuştur (Howard & David, 2003). Bu kaynaklarda yer alan tekniklerin titiz ve dikkatli bir şekilde uygulanması ile bir dereceye kadar SQL enjeksiyonu saldırılarının önleneceği düşünülebilir. Ancak uygulama geliştiricilerin bir insan olduğu ve her zaman hata yapma ihtimali olabileceği göz ardı edilmemelidir. Ayrıca çok farklı türde ve çok fazla sayıda SQL enjeksiyonu saldırısı tekniği olduğu düşünüldüğünde her bir saldırı tekniği için farklı bir tespit ve önleme metoduna ihtiyaç duyulmaktadır (Halfond vd., 2006). Müteakip bölümde SQL enjeksiyonu saldırılarını tespit ve önlemede kullanılan yöntemler incelenmiştir.

3. SQL ENJEKSİYONU SALDIRILARINA KARŞI GÜVENLİK ÖNLEMLERİ

Literatürde SQL enjeksiyonu saldırılarının tespiti ve önlenmesi maksadıyla birçok teknik ileri bulunmaktadır. Bu teknikler, yazılım geliştirme esnasında uygulanan kodlama pratikleri ile tamamen otomasyona dayanan tespit ve önleme sistemleri konu başlıkları altında toplanabilir. Bu tekniklerden önemli olan bazıları aşağıda sunulmuştur.

3.1. Kodlama Pratikleri

Yazılım geliştirme sürecinde girdi kontrolünün yapılması yönünde tedbirler alınması SQL enjeksiyonu saldırılarının önlenmesinde oldukça önemlidir. Girdi kontrolü aşağıda belirtilen metotlarla yapılabilmektedir.

Girdi Türünün Kontrolü: SQL enjeksiyonu saldırıları bir string ya da sayısal veri türünde parametrenin içerisine komut ya da bir takım ifadeler enjekte etmek suretiyle gerçekleştirilmektedir. Dolayısıyla bu parametrelerin basit bir kontrolü bile SQL enjeksiyonu saldırılarını birçok durumda engelleyebilmektedir (Halfond vd., 2006).

Girdilerin Kodlanması: String veri türü içerisine yerleştirilen enjeksiyon deyimleri genellikle özel karakterler barındırmaktadır. Dolayısıyla bu türden özel karakterlerin kullanımının engellenmesi yoluyla SQL enjeksiyonu saldırılarının önüne geçildiği görülmüştür (Halfond vd., 2006).

Girdi Kaynaklarının Kontrolü: SQL enjeksiyonu saldırılarından korunmak maksadıyla uygulamaya yapılan bütün girdiler kontrol edilmelidir. Dolayısıyla uygulamaya girdi yapan kaynakların her biri yazılım geliştiriciler tarafından kontrol edilmeli ve uygulama geliştirme sürecinde bu kaynaklara yönelik tedbirler alınmalıdır (Jemal vd., 2020).

Yukarıda bahsedilen hususlara ilave olarak;

- Veri tabanında kullanılan tablo ve sütun isimlerinin kolaylıkla tahmin edilemeyecek şekilde belirlenmesi (Demirol vd., 2013),
- Parametreli sorgu deyimlerinin kullanılması (Clarke, 2009),
- SQL deyimleri taranmak suretiyle istismara yol açabileceği değerlendirilen karakterlerin özel fonksiyonlarla zararsız karakterlere dönüştürülmesi (Demirol vd., 2013),
- Uygulama kodlarının yazılımı test eden kişiler tarafından çok dikkatli bir şekilde kontrol edilmesi (Vural & Sağıroğlu, 2010),
- Veri tabanı yöneticisi tarafından veri tabanına çeşitli araçlarla (MS Excel, MS SQL Server Management Studio vb.) erişim imkânı bulunan kişilere yetki dağılımı yapılırken "Bilmesi Gereken" ve "En Az Yetki" prensibine uyulması (Vural & Sağıroğlu, 2010),
- Uygulamanın bulunduğu sunucuda siber saldırılara karşı güvenlik önlemlerinin arttırılması ya da güvenlik duvarı kurulması (Daş vd., 2012) şeklindeki tedbirlerin SQL enjeksiyonu saldırılarının önlenmesinde etkili olabileceği değerlendirilmektedir.

3.2. Tespit ve Önleme Sistemleri

Farklı araştırmacılar tarafından yukarıda bahsedilen kodlama pratiklerinin yetersiz kaldığı alanlar görülmüş ve SQL enjeksiyonu saldırılarını daha etkili araçlarla engellemek maksadıyla literatüre birçok tespit ve önleme sistemi sunulmuştur. Bunlardan bazıları bu bölümde incelenecektir.

Huang ve arkadaşları (Huang vd., 2003) tarafından WAVES isimli, kara kutu tekniği ile web uygulamalarının SQL enjeksiyonu saldırılarına karşı açıklıklarını tespit eden bir sistem geliştirilmiştir. Bu teknikte web uygulamasının SQL enjeksiyonu saldırısı maksadıyla kullanılabilecek bütün noktalarını tarayan bir çeşit arama robotu kullanılmıştır. Daha sonra belirli bir listeye göre bu noktaları hedef alan saldırılar oluşturulmuştur. Bu esnada WAVES tarafından makine öğrenmesi teknikleri uygulanarak web uygulaması tarafından saldırılara verilen tepkiler izlenmiş ve başarılı sonuçlar elde edilmiştir.

Gould ve diğerleri (Gould vd., 2004) tarafından dinamik olarak oluşturulan SQL sorgularının tür doğruluğu bakımından kontrolünü yapmak maksadıyla JDBC-Checker statik analiz aracı geliştirilmiştir. JDBC-Checker vasıtasıyla dinamik olarak geliştirilen SQL sorgularındaki tür uyuşmazlıklarından faydalanarak SQL enjeksiyonu saldırıları tespit edilmektedir.

Fu ve diğerleri (Fu vd., 2007) yaptıkları çalışma ile SAFELI adlı tespit ve önleme sistemini literatüre sunmuşlardır. SAFELI vasıtasıyla SQL enjeksiyonu saldırısına yönelik çok hassas güvenlik açıklıkları yazılımın kaynak kodu bilgisinden faydalanarak tespit edilmektedir.

Halfond ve arkadaşı (Halfond & Orso, 2005) tarafından statik analiz ile yürütme zamanını gözlemlemeye dayalı ve model tabanlı AMNESIA tespit ve önleme sistemi geliştirilmiştir. AMNESIA tespit ve önleme sisteminin başarısı ilk aşamada oluşturulan statik modellerin doğruluğu ile orantılıdır.

Alazab ve arkadaşı (Alazab & Khresiat, 2016) yaptıkları çalışmada, SQL enjeksiyonu saldırılarını yürütme zamanında ve uygulama katmanında tespit eden bir sistem önermişlerdir. Önerdikleri sistemin, SQL enjeksiyonu içeren deyimleri henüz uygulama katmanında veri tabanına erişmeden tespit etmesi dolayısıyla oldukça avantajlı olduğu görülmüştür.

Alattar ve arkadaşı (Alattar & Medhane, 2013) tarafından SQL enjeksiyonu saldırılarını etkin bir şekilde gerçek zamanlı ortamda tespit eden ve önleyen R-WASP isimli bir araç önerilmiştir.

Manmadhan ve arkadaşı (Manmadhan & Thankappan, 2012) tarafından yapılan çalışmada, sorgu semantiği kontrol edilmek suretiyle dinamik sorgu yapısı doğrulaması temeli üzerine dayalı bir sistem önerilmiştir.

Çağlayan ve arkadaşları (Çağlayan vd., 2009) tarafından yapılan çalışmada aktif ve pasif DNS izlemeyi esas alan gerçek zamanlı bir tespit sistemi önerilmiştir.

4. YÖNTEM

SQL enjeksiyonu saldırıları üzerine yapılan çalışmalarda kullanılan veriler, genel olarak, balküpü (honeypot) veya bir web sitesi üzerindeki gerçek zamanlı web trafiğinin izlenmesi yoluyla elde edilen veriler ve bir web trafiğinin simüle edilmesi yoluyla elde edilen veriler olmak üzere iki şekilde elde edilmektedir (Ross, 2018). Bu çalışmada, açık kaynak web sitesinde (Kaggle, 2022) yer alan ve gerçek web trafiğin izlenmesi ile hazırlanmış veri setleri kullanılmıştır.

Çalışma kapsamında, makine öğrenmesi uygulamasında kullanılmak üzere eğitim maksadıyla 22.000 satırlık bir veri seti ve test maksadıyla yaklaşık 2.200 satırlık iki adet veri seti oluşturulmuştur. Her bir veri seti içerisinde birinci sütunda SQL enjeksiyonu saldırısında kullanılan çeşitli semboller ve ifadeler içeren deyimlerle birlikte SQL enjeksiyonuna yönelik sembol ve ifade içermeyen temiz diye ifade edilebilecek deyimler yer almıştır. Bu veriler string veri türünde teşkil edilmiştir. İkinci sütunda ise makine öğrenmesi uygulamasında sınıflandırma verisi olarak kullanılacak veriler yer almıştır. Bahse konu veriler, her bir ifadenin SQL enjeksiyonuna yönelik bir ifade içerip içermediğinin incelenmesi neticesinde SQL enjeksiyonuna yönelik ifade içeren deyimler "1" ve SQL enjeksiyonuna yönelik ifade içermeyen deyimler "0" şeklinde integer değerlerle ifade edilmiştir. Veri Seti-1 olarak adlandırılan veri seti içerinde SQL enjeksiyonu içeren ifadelerin yanında SQL enjeksiyonuna yönelik olarak herhangi bir ifade içermeyen metin şeklinde ifadeler yer almıştır. Veri Seti-2 olarak adlandırılan veri seti içerisinde ise SQL enjeksiyonu içeren ifadelerin yanında genellikle kullanıcılar tarafından herhangi bir uygulamaya giriş esnasında kullanılan ve bu çalışma özelinde rastgele üretilmiş olan kullanıcı adı ve parolalara yer verilmiştir.

Makine öğrenmesi uygulaması k-en yakın komşu (k-nearest neighbour-KNN), destek vektör makinesi (support vector machine-SVM), karar ağacı (decision tree-DT) ve naive bayes (NB) sınıflandırma algoritmaları vasıtasıyla oluşturulan modeller ile yapılmış ve oluşturulan modeller ile elde edilen sonuçlar doğruluk (accuracy), kesinlik (precision), duyarlılık (recall) ve F_1 puanı (F_1 score) değerleri açısından değerlendirilmiştir.

Makine öğrenmesi uygulaması MATLAB ile gerçekleştirilmiştir. MATLAB uygulaması, kodlama dilinin sade ve anlaşılır olması, hata geri bildirimi yapması ve metin madenciliği anlamında gelişmiş bir alt yapıya sahip olması (Kolukısa, 2021) dolayısıyla tercih edilmiştir.

5. SQL ENJEKSİYONU SALDIRILARININ MAKİNE ÖĞRENMESİ İLE TESPİTİ

MATLAB uygulaması üzerinde gerçekleştirilen makine öğrenmesi uygulaması ile elde edilen sonuçlar Çizelge 5.1.'de sunulmuştur.

Veri Seti	Değer	Sınıflandırma Algoritmaları			
		KNN	SVM	DT	NB
Veri Seti-1	Doğruluk	0,99	0,79	0,80	0,53
	Kesinlik	0,99	0,85	0,86	0,75
	Duyarlılık	0,99	0,79	0,80	0,83
	F_1 Puanı	0,99	0,82	0,83	0,62
Veri Seti-2	Doğruluk	0,88	0,78	0,77	0,50
	Kesinlik	0,90	0,84	0,83	0,74
	Duyarlılık	0,87	0,79	0,78	0,52
	F_1 Puanı	0,89	0,82	0,81	0,61

Çizelge 5.1. Uygulama Sonuçları

Yukarıdaki çizelgede görüldüğü üzere hem veri seti-1 hem de veri seti-2 için en yüksek değerler k-en yakın komşu sınıflandırma algoritması ile elde edilmiştir. Destek vektör makineleri ve karar ağacı sınıflandırma algoritmaları ile birbirine yakın değerler elde edilmesine rağmen, naive bayes sınıflandırma algoritması ile nispeten düşük sonuçlar elde edilmiştir.

Doğruluk değeri açısından değerlendirildiğinde k-en yakın komşu sınıflandırma algoritması ile veri seti-1 için 0,99 ve

veri seti-2 için 0,88 değerleri elde edilmiş ve bu değerin her iki veri seti içinde en yüksek değerler olduğu görülmüştür. Destek vektör makineleri ve karar ağacı sınıflandırma algoritmaları ile veri seti-1 için sırasıyla 0,79 ve 0,80 doğruluk değerleri, veri seti-2 için 0,78 ve 0,80 doğruluk değerleri elde edilmiştir.

Kesinlik değeri açısından değerlendirildiğinde k-en yakın komşu sınıflandırma algoritması ile veri seti-1 için 0,99 ve veri seti-2 için 0,90 değerleri elde edilmiş ve bu değerlerin her iki veri seti içinde, doğruluk değerinde olduğu gibi, en yüksek değerler olduğu görülmüştür. Destek vektör makineleri ve karar ağacı sınıflandırma algoritmaları ile veri seti-1 için sırasıyla 0,85 ve 0,86 kesinlik değerleri, veri seti-2 için 0,84 ve 0,83 kesinlik değerleri elde edilmiştir. Naive bayes algoritması ile kesinlik değeri olarak veri seti-1 ve veri seti-2 için sırasıyla 0,75 ve 0,74 değerleri elde edilmiştir.

Duyarlılık değeri açısından değerlendirildiğinde k-en yakın komşu sınıflandırma algoritması ile veri seti-1 ve veri seti-2 için sırasıyla 0,99 ve 0,88 değerleri elde edilmiştir. Bu algoritmanın ardından en yüksek değerler destek vektör makineleri ve karar ağacı sınıflandırma algoritmaları ile elde edilmiştir. Destek vektör makineleri algoritmasıyla elde edilen değerler her iki veri seti içinde 0,79 şeklinde olmuştur. Karar ağacı algoritması ile veri seti-1 ve veri seti-2 için sırasıyla 0,80 ve 0,78 değerleri ve naive bayes algoritması ile 0,83 ve 0,52 değerleri elde edilmiştir.

F_1 puanı açısından değerlendirildiğinde k-en yakın komşu sınıflandırma algoritması ile veri seti-1 için 0,99 ve veri seti-2 için 0,89 değerleri elde edilmiş ve bu değerlerin her iki veri seti içinde en yüksek değerler olduğu görülmüştür. Destek vektör makineleri algoritmasıyla elde edilen değerler her iki veri seti içinde 0,82 şeklinde olmuştur. Karar ağacı sınıflandırma algoritmaları ile elde edilen F_1 puanı veri seti-1 veri seti-2 için sırasıyla 0,83 ve 0,81 şeklinde elde edilmiştir. Naive bayes algoritması ile yine sırasıyla 0,62 ve 0,61 değerleri elde edilmiştir.

6. SONUÇ

Uygulamadan elde edilen bulgular incelendiğinde, naive bayes algoritması haricinde kullanılan diğer makine öğrenmesi algoritmalarının hem veri seti-1 hem de veri seti-2 için SQL enjeksiyonu saldırılarını sınıflandırmada başarılı olduğu görülmüştür. Uygulamada kullanılan sınıflandırma algoritmaları içerisinde en yüksek değerler k-en yakın komşu algoritması ile elde edilmiştir. Bu açıdan en başarılı algoritmanın k-en yakın komşu algoritması olduğu yapılan uygulama özelinde söylenebilir.

SQL enjeksiyonu saldırılarının makine öğrenmesi ile tespit edilmesi konusunda yapılan diğer çalışmalar incelendiğinde; Muhammad ve arkadaşlarının yaptığı çalışmada (Azman vd., 2021) ilk uygulama için %93 ve sonraki 4 uygulamada %100 doğruluk oranı elde edildiği, Krishnan ve arkadaşları tarafından yapılan çalışmada (Krishnan vd., 2021) evrimli sinir ağı algoritması kullanılarak %97 doğruluk oranı elde edildiği ve Hasan ile arkadaşları (Hasan vd., 2019) tarafından yapılan çalışmada ise %93,8 doğruluk oranı elde edildiği görülmüştür.

Yapılan makine öğrenmesi uygulamasında metin şeklinde deyimler içeren veri setinin yanında kullanıcı adı ve parola verilerini içeren farklı bir veri seti daha kullanılmıştır. Oluşturulan makine öğrenmesi modelleri ile birbirinden farklı veriler içeren veri setleri için, doğruluk değerleri haricinde, hemen hemen birbirine yakın değerler elde edilmiştir. Veri seti-1 ve veri seti-2 için doğruluk değerleri arasındaki bu farkın ortalama 0,1 puan civarında olduğu görülmüştür. Yapılan uygulama bu açıdan incelendiğinde, birbirinden farklı veri setlerinin kullanılması ile oluşturulan makine öğrenmesi modellerinin bir bakıma güvenilirliği test edilmiş ve değerler arasında çok fazla göze çarpan bir farklılık olmaması açısından olumlu sonuçlar elde edilmiştir. Veri setlerinin sayısının arttırılması ve bu veri setleri içerisinde yer alan verilerin çeşitlendirilmesi ile modellerin güvenilirliğinin sorgulanabileceği görülmüştür.

Sonuç olarak bu çalışmada, her geçen gün önemi daha da artan makine öğrenmesi modelleri ile farklı veri setleri kullanılarak SQL enjeksiyonu saldırılarının tespit edilmesine yönelik bir yöntem ortaya konmuştur. Gelişen teknoloji dünyasında siber güvenlik alanında makine öğrenmesi ve yapay zeka uygulamalarının her geçen gün daha da önem kazanacağı ve bu uygulamaların siber güvenlik alanında birçok soruna kolay ve hızlı bir çözüm bulabileceği değerlendirilmektedir.

SQL enjeksiyonu saldırılarının çerezler veya sunucu değişkenleri vasıtasıyla gerçekleştirildiği varsayılarak yapılacak ve veri setlerinin bu kapsamda düzenleneceği çalışmalar ile modellerin güvenilirliği açısından veri setleri arasındaki korelasyonun değerlendirileceği çalışmalar gelecek çalışmalar kapsamında değerlendirilmelidir.

KAYNAKLAR

Alattar, M., & Medhane, S. P. (2013). R-WASP: Real Time-Web Application SQL Injection Detector and Preventer. International Journal of Innovative Technology and Exploring Engineering, Volume-2, Issue-5,, 327-330.

Alazab, A., & Khresiat, A. (2016). New Strategy for Mitigating of SQL Injection Attack. International Journal of Computer Applications, 1-10.

Alwan, Z., & Younis, M. (2017). Detection and Prevention of SQL Injection Attack:A Survey. International Journal of Computer Science and Mobile Computing Vol.6 Issue 8, 5-17.

Avcı, İ., Koca, M., & Atasoy, M. (2021). Windows Tabanlı Uygulamalarda SQL Enjeksiyon Siber Saldırı Senaryosu ve Güvenlik Önlemleri. Avrupa Bilim ve Teknoloji Dergisi Özel Sayı 28, 213-219.

Azman, M. A., Marhusin, M. F., & Sulaiman, R. (2021). Machine Learning-Based Technique to Detect SQL Injection Attack. Journal of Computer Science Volume 17, Number 3, 296-303.

Clarke, J. (2009). SQL Injection Attacks and Defence. Syngress.

Crowdstrike. (2022, 11 07). Crowdstrike web sitesi: https://www.crowdstrike.com/cybersecurity-101/sql-injection/ adresinden alındı

Çağlayan, A., Toothaker, M., Drapeau, D., & Burke, D. (2009). Real-Time Detection of Fast Flux Service Networks. Conference For Homeland Security.

Daş, R., Kara, Ş., & Gündüz, M. Z. (2012). Casus Yazılımların Bilgisayar Sistemlerine Bulaşma Belirtileri ve Çözüm Önerileri. 5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı. ANKARA.

Demirol, D., Daş, R., & Baykara, M. (2013). SQL Enjeksiyon Saldırılarına Karşı Güvenlik Önlemleri. 1st International Symposium on Dijital Forensics and Security (ISDFS'13). Elazığ.

Elmasri, R., & Navathe, S. B. (2010). Fundamentals of Database Systems, 6th Edition. Pearson.

Forristal, J. (1998, Aralık 25). NT Web Teknolojisi Güvenlik Açıkları. Phrack, s. 54.

Fu, X., Lu, X., Peltsverger, B., & Chen, S. (2007). A Static Analysis Framework For Detecting SQL Injection Vulnerabilities. 1st Annual International Computer Software and Applications Conference, (s. 1-8).

Gould, C., Su, Z., & Devanbu, P. T. (2004). JDBC Checker: A Static Analysis Tool For SQL/JDBC Applications. 26th International Conference on Software Engineering, (s. 697-698).

Halfond, W. G., & Orso, A. (2005). AMNESIA: Analysis and Monitoring for Neutralizing SQL-Injection Attacks. IEEE and ACM International Conference on Automated Software Engineering.

Halfond, W. G., Viegas, J., & Orso, A. (2006). A Classification of SQL Injection Attacks and Countermeasures. Computer Science, Mathematics.

Hasan, M., Balbahaith, Z., & Tarique, M. (2019). Detection of SQL Injection Attacks: A Machine Learning Approach. 2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA).

Howard, M., & David, L. (2003). Writing Secure Code. Washington: Microsoft Press.

Huang, Y.-W., Huang, S.-K., Lin, T.-P., & Tsai, C.-H. (2003). Web application security assessment by fault injection and behavior monitoring. Conference: Proceedings of the 12th international conference on World Wide Web.

Jemal, I., Omar, C., Habib, H., & Mahfoudhi, A. (2020). SQL Injection Attack Detection and Prevention Techniques Using Machine Learning. International Journal of Applied Engineering Research Volume 15, Number 6, 569-580.

Kaggle. (2022, 07 11). Kaggle Web Sitesi: https://www.kaggle.com/ adresinden alındı

Kolukısa, A. A. (2021). WEKA ile Bulanık Mantık Uygulaması.

Krishnan, A., Sabu, A., Sajan, P., & Sreedeep, A. (2021). SQL Injection Detection Using Machine Learning. Gestao Inovaçao e Technologias, Volume 11, Number 3.

Laval, M., Sultan, A. B., & Shakiru, A. O. (2016). Systematic Literature Review on SQL Injection Attack. International Journal of Soft Computing, , 26-35.

Manmadhan, S., & Thankappan, M. (2012). A Method of Detecting Sql Injection Attack to Secure Web Applications. International Journal of Distributed and Parallel Systems 3(6), 1-8.

OWASP. (2022, 08 15). OWASP: https://owasp.org/www-project-top-ten/ adresinden alındı

Ross, K. (2018). Master's Theses and Graduate Research. SQL Injection Detection Using Machine Learning Techniques and Multiple Data Sources. San Jose State University Scholar Works.

Venturebeat. (2022, 11 07). Venturebeat web sitesi: https://venturebeat.com/security/report-35-of-educational-institutions-have-a-sqli-vulnerability/ adresinden alındı

Vural, Y., & Sağıroğlu, Ş. (2010). Veritabanı Yönetim Sistemleri Güvenliği: Tehditler ve Korunma Yöntemleri. Politeknik Dergisi Cilt:13 Sayı:2, 71-81.