Web Uygulamalarında Kural Tabanlı Saldırı Tespit ve Önleme Sistemleri

Sadık Tuna YAĞCI, Bilgisayar Mühendisliği, Gazi Üniversitesi, 14110068

***Özet*— Bir saldırı tespit ve önleme sistemi saldırılara efektif bir şekilde yanıt verebilmek için çok miktarda kategorize edilmiş verisetine ihtiyaç duyar. Bu verisetleri geçmişte yapılmış saldırıların ML (Machine Learning) algoritmalarından geçirilip sınıflandırılarak yeni saldırıların bulunması konusunda bir methoddur. Bu verisetlerinin nasıl uygulanacağı konusunda ortak bir method bulunmamaktadır. Bu güvenlik sorununun uygulama tarafı dünya çapında çok önemli bir sorundur ve bu saldırı tespit ve önleme uygulamalarının günümüz dünyasında bir web uygulamasında kullanılması konusunda henüz ortak bir methoda geçilememiştir. Bu makale, bu sistemlere ortak kullanılacak bir method yazma amacıyla bir kural tabanlı saldırı tespit ve önleme sistemi önermektedir. Bu sistemde verisetlerinden elde edilen karar şemaları bir kural listesine dönüştülerek web uygulamasında çalıştırılabilir hale getirilmektedir. Bu kurallar web uygulamasında her HTTP isteği geldiğinde çalıştırılarak saldırı tespit verisetleri gerçek bir uygulamada çalışabilir hale getirilmiştir. Saldırı önleme sistemleri günümüzde oldukça yaygın kullanılan, sistem-spesifik yöntemlerdir. Saldırı önleme, diğer adıyla savunma, sistemleri saldırganın sisteme girişinin engellenmesine yönelik çalışır. Bu makalede bir IP bazlı sisteme giriş engelleme tipi saldırı önleme sistemi önerilmiştir. Bu sistemin çalışması, kural bazlı saldırı tespit sistemine bağlıdır.**

I. GİRİŞ

Bu makale siber güvenlik alanında yapılmış saldırı tespit verisetlerinin günümüz web uygulamalarında kullanımına yönelik bir uygulama önermektedir. Bu uygulama aynı zamanda bir saldırı önleme sistemi önermektedir.

Saldırı tespit sistemleri (IDS), bir ağın saldırganlar tarafından başlatılmış illegal operasyonlara yönelik güvenliğini sağlamada önemli bir anlam taşımaktadır [1]. Şu anki saldırı tespit ve önleme sistemleri imza tabanlı izleme yaparak herhangi kötücül davranışları tespit ederek bir alarm paylaşmaktadır. Tanım olarak saldırı önleme sistemleri bir sınıflandırma problemidir. Saldırı tiplerine göre sınıflandırma yapılır ve yeni gelen paketin hangi saldırı kategorisine girdiğine bakılır. Temel motivasyon bu sınıflandırmadaki accuracy'nin arttırılmasıdır [2].

Saldırı önleme sistemleri (IPS), bir ağın saldırı altında olduğunun tespiti sonrası saldırganın imzasının tespit edilip sistem tarafından sisteme girişinin engellenmesi üzerine çalışmaktadır. Bu tür sistemlerde saldırganının sisteme girişinin engellenmesinde birden çok yöntem kullanılmaktadır. Bu makalede IP bazlı sisteme giriş engellenmesi yöntemi kullanılmaktadır. Bu method 2. Bölümde detaylıca anlatılmıştır.

Bu makaledeki proje, IDS ve elde edilen verisetlerini kullanarak bir IPS sistemi geliştirmeyi amaçlamaktadır. Günümüzde böyle sistemler kullanılmakta olup başlarında insan işçi bulunması şarttır. Bu proje, bu tür IPS sistemlerindeki insan işçisi sayısını azaltarak sistemi otomatize etmeyi amaçlamaktadır.

Bu otomatizasyon, kural bazlı bir IDS sistemi olarak düşünülmüş olup IDS sonucu elde edilen verisetlerinin bir Decision Tree (DT) algoritması sonucu kural setinden oluşturulabilir. Hazırlanan uygulamada kuralların nasıl hazırlandığı önemsizdir.

Bu proje web uygulaması olarak Tomcat[3] web sunucusu altındaki Spring Framework[4] uygulamalarında çalışmaktadır. Bu uygulamalar Java EE[5] platformu üzerinde geliştirilmiş olup Tomcat platformunun çalışabildiği herhangi bir işletim sistemi üzerinde çalıştırılabilir.

Elde edilen sonuçlarda hazırlanan IDPS (Intrusion detection and prevention system) sisteminin hazırlanan kuralları %100 olarak gerçekleştirilebildiği görülmüştür. Bu uygulamada kuralların sistemi ne kadar koruyabildiği test edilmemiş olup bu konu proje kapsamına alınmamıştır.

II. ARAÇ VE YÖNTEMLER

Günümüzde IDS/IPS sistemlerinin bir çoğu güncel olarak son saldırı türlerine entegre olmaktadır. Yeni bir saldırı türü bulunduğu zaman hem bu saldırının tespit yöntemi hem de savunma yöntemi güncellenmektedir. Bu sistemlerdeki saldırı türleri incelenmiş olup hazırlanacak otomatizasyonda kullanılacak parametreler bu saldırı tespit sistemlerine göre hazırlanmıştır.

A. Veri Bilgisi

Bu projede siber saldırılar 6 kategoride ele alınmıştır:

Saldırı Türleri
DDOS
SQL Injection
XSS
Path Scanning
APT
Brute-force

Tablo 1- Saldırı Türleri

Günümüzde çok daha fazla saldırı kategorisi olmasına

rağmen projede yalnızca 6 kategori ele alınmıştır. Bu saldırı türleri incelenmiş olup bunlara ait özellikler kaydedilmiştir. Bu özellikler kullanılarak bu saldırıların tespit edilebileceği görülmüştür (bu kısım detaylı olarak 3. Bölüm A altbölümünde anlatılmıştır). Lakin bu özelliklerin kapsamı kesin bir sayıyla ifade edilememektedir. IDS sistemlerde bu kapsam Machine Learning tabanlı algoritmalarla belirlenmektedir [6]. Geliştirilen sistem, Web uygulamalarında kural bazlı saldırı tespit ve önleme sistemi (WUKAS), bu özellikleri konfigüre edilebilir parametreler olarak almıştır. Bu parametreler 6 parçadan oluşmaktadır.

Parametre	Açıklama	Örnek
Zaman aralığı	Süre sayısı.	(Integer) 5, 10, 15
Zaman aralığı türü	Sürenin türü. Saniye, dakika veya saat.	(Enum) Saniye, Dakika veya Saat.
İstek path'i	İsteğin web uygulamasının hangi path'ine geldiği.	(String) Api/v2/projeler, Api/v2/users/{name}
Dönüş HTTP kodu	HTTP status kodu.	(Integer) 200, 500, 404
İstek sayısı	Web uygulamasına belirtilen zaman aralığında kaç tane istek geldiği.	(Integer) 10, 20, 30, 500, 1000
İstek HTTP methodu	HTTP method'ları: GET, POST, DELETE vs.	(Enum) GET, POST, DELETE
İstek HTTP methodunda SQL syntax'ı sayısı	SQL Injection saldırısını önlemeye dair konulmuş parametre. GET isteği atıldığında belirli sürede parametrelerde kaç tane Sql SYNTAX'ı geçtiği.	(Integer) 5, 10,15
İstek HTTP methodunda HTML syntax'ı sayısı	XSS saldırısını önlemeye dair konulmuş parametre. GET isteği atıldığında belirli sürede parametrelerde kaç tane HTML syntax'ı geçtiği.	(Integer) 5, 10, 15
IP gruplama	İsteklerin aynı IP'ye göre gruplandırılması	(Boolean) True, False

Tablo 2- Konfigüre edilebilecek parametreler

B. *Geliştirme ortamı*

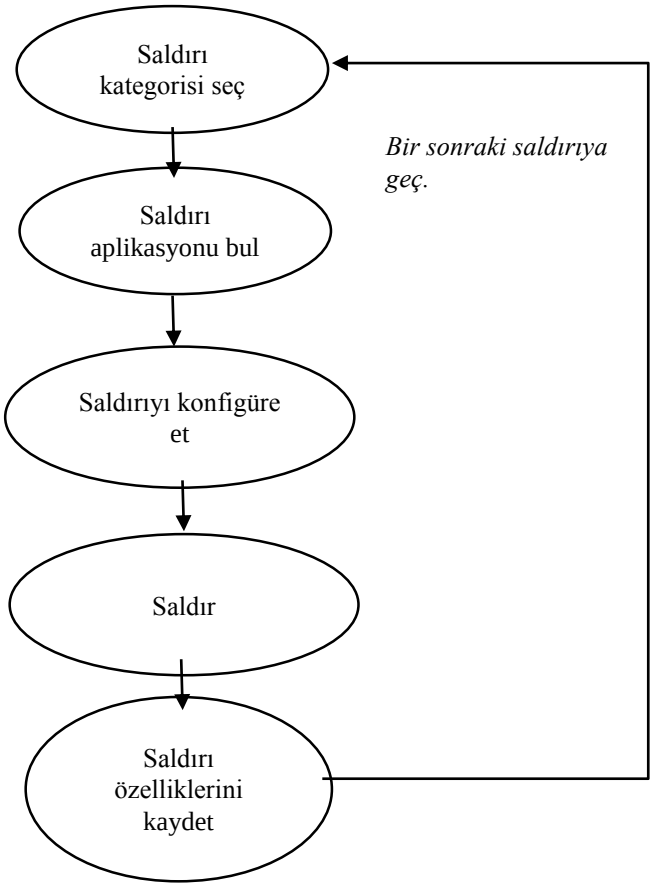
WUKAS, Tomcat platformu altında Spring Framework için geliştirilmiş bir uygulamadır. WUKAS yalnızca Spring Framework altında çalışabilirken herhangi bir Java EE sunucusu altında çalışabilir. Test edilmiş sistemler olarak: Tomcat, Glassfish[7], TomEE[8].

WUKAS, veritabanı olarak PostgreSQL[9] veritabanı kullanır.

III. GERÇEKLEŞTİRİLEN UYGULAMA

A. *Parametre Oluşturma*

WUKAS için seçilen parametreler günümüz saldırı türlerinin özellikleri incelenerek seçilmiştir. Bu saldırı türleri Tablo 2'de gösterilmiş olup bu saldırı türleri detaylıca incelendikten sonra spesifik özellikleri ortaya çıkarılmıştır. Bu özelliklerin ortaya çıkarılması aşağıdaki akış diyagramında gösterilmiştir.



Şekil 1- Parametre Oluşturulması

Oluşturulan saldırı özellikleri kategorilere göre aşağıda ifade edilmiştir.

Saldırı Türleri	Özellikler
DDOS	3 saniyede gelen istek sayısı belli bir miktarın üstünde
SQL Injection	5 saniye boyunca gelen istekler içerisinde SQL syntax'ı 10'un üstünde
XSS	5 saniye boyunca gelen istekler içerisinde HTML syntax'ı 10'un üstünde
Path Scanning	3 saniye içerisinde aynı IP'den 20 defa HTTP 404

	alınması
APT	Aynı path'in 100 defa HTTP 500 alınması
Brute-force	Aynı path üzerinden 2 saniyede 100 defa HTTP 500 alınması

Tablo 3- Saldırı özellikleri

B. Kural Oluşturulması

WUKAS, oluşturulan bir parametre grubuna kural adı vermektedir. Kurallar veritabanında "rule" adında bir table'da tutulmaktadır.

WUKAS kurallarının silme, değiştirme, ekleme işlemleri veritabanı üzerinden yapılmaktadır.

Saldırı türlerine özel IPS hazırlamak amacıyla kurallar hazırlanmalıdır. Aşağıdaki saldırı türlerine özel hazırlanmış kurallar bulunmaktadır.

DDOS: 5 saniye içerisinde 10.000 istek sayısı.

Parametreler:

Parametre	**Örnek**
Zaman aralığı	5
Zaman aralığı türü	Saniye
İstek path'i	(Null)
Dönüş HTTP kodu	(Null)
İstek sayısı	10000
İstek HTTP methodu	(Null)
İstek HTTP methodunda SQL syntax'ı sayısı	(Null)
İstek HTTP methodunda HTML syntax'ı sayısı	(Null)
IP gruplama	True

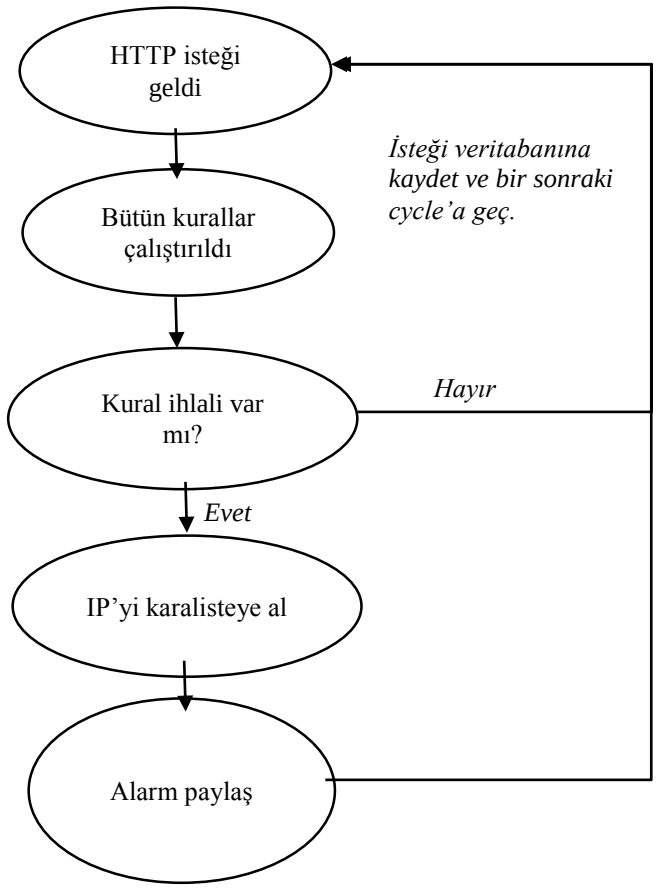
Tablo 4- DDoS saldırısı için örnek bir kural tablosu

Tablo 4 incelediğinde tahmin edildiği gibi null değerler için bir gruplama yapılmayacaktır.

Farklı bir senaryoda yalnızca HTTP POST metodu kullanıldığı farz edilirse, buna dair parametre POST olarak set edilerek bu kural gerçekleştirilir. Örnek bir brute-force IDP'si için bu kural uygulanmalıdır.

C. Kuralların Uygulanması

Oluşturulan kurallar WUKAS'a her HTTP isteği geldiğinde denetlenmektedir. Bu denetleme işlemi aşağıdaki şemada anlatılmıştır.



Şekil 3- Kuralların Uygulanması

Şekil 3'deki şemada görüldüğü üzere gelen her HTTP isteği bir Java Thread'i[10] altına alınmaktadır. Her isteğin incelenip bir sonuca bağlanana kadar geçen süre sunucu için bir döngü olarak tanımlanmıştır.

Uygulama her döngü için gelen istekleri kurallar bütünlüğünden geçirerek bir sonuca varmaktadır. Eğer gelen istek bir kuralı tetiklediyse bu IP, IPS aşaması için karalisteye alınır ve bir alarm olarak WUKAS'ı kullanan ilgili yerlere paylaşılır. Eğer kural ihlali yoksa bu IP bir girdi olarak bütün özellikleriyle veritabanına kaydedilir.

Kural ihlalinin olup olmadığı aşamasında WUKAS, bütün kuralları önceden gelen HTTP isteklerinin tutulduğu tabloda SQL sorgusu gerçekleştirerek bir ihlal olup olmadığı sonucuyla denetler. Bu aşamada gelen isteğin IP'sinin karalistede tutulup tutulmadığı varsayılan bir kuraldır ve bütün isteklere tabi tutulmaktadır. Eğer bir kural ihlali varsa diğer kurallara bakılmaksızın IP karalisteye alınmaktadır.

Kuralların uygulanması için herhangi bir kural sayısı limiti belirtilmemekle beraber kural sayısı ile her döngü için geçen süre Testler bölümünde incelenmiştir.

D. Saldırı Önleme Methodu

Saldırı önleme, IPS metodu WUKAS uygulamasında yalnızca IP block yöntemini kapsamaktadır. Bu kapsamda herhangi bir kural ihlali bulunduğunda bu IP'nin sisteme girişi engellenmekte, yani aynı IP'den gelen her istek HTTP 500 kodu ile karşılaşmaktadır.

Saldırı önleme aşaması Şekil-2'de görüldüğü üzere bir kural ihlali olduğunda veya IP daha önceden karaliste adı verilen kötücül IP'lerin tutulduğu bir table'da ise çalışmaktadır.

IV. TESTLER

WUKAS uygulamasının testleri iki aşamada gerçekleştirilmiştir. Bu aşamalardan ilkinde kuralların çalışabilirliği, ikincisinde ise kural sayısının döngü zamanına etkisi test edilmiştir.

Bu aşamalarda WUKAS uygulaması bir adet Intel Core i5-5200 işlemcisi içeren, 8 GB ram bulunduran Windows işletim sistemli Victor marka dizüstü bilgisayar üzerinde Tomcat platformu altında çalıştırılmıştır.

Saldırgan aynı makine üzerinde bir adet sanal makine içerisinde Kali Linux [11] işletim sisteminde çalışmaktadır. Saldırganın kullandığı uygulamalar aşağıdaki tabloda listelenmiştir.

Saldırı Türü	**Uygulama**	**Saldırı Parametreleri**
DDOS	GoldenEye[12]	1 saniye içerisinde 1500 istek atılmıştır.
SQL Injection	Sqlmap[13]	5 saniye içerisinde 50 istek atılmıştır.
XSS	Xsser[14]	5 saniye içerisinde 50 istek atılmıştır.
Path Scanning	Manual	20 saniye içerisinde 6 adet HTTP 404 alınacak path'lere istek atılmıştır.
APT	Manual	48 saat içerisinde 1000 adet 404 alınacak path'lere istek atılmıştır.
Brute-force	Burp Suite[15], Hydra[16]	10 saniye içerisinde 30 adet HTTP 500 alınacak HTTP POST atılmıştır.

Tablo 5- Kali Linux işletim sistemi altında saldırıları gerçekleştirmek için seçilmiş uygulamalar

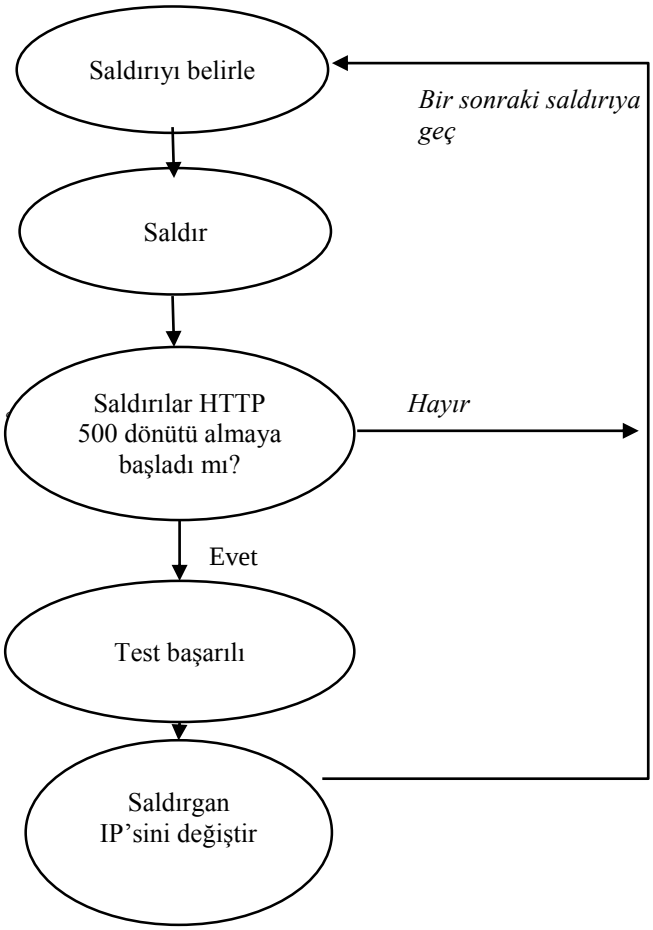
Tablo 5'deki manual hücresi hiçbir uygulama kullanılmadan varsayılan tarayıcı üzerinden istekler gerçekleştirilerek tamamlandığı anlamına gelmektedir. Tablodaki saldırıların her biri aynı IP ile gerçekleştirilmiş olup her saldırı sonrası WUKAS karalistesi temizlenmiştir.

Her saldırı için hazırlanmış test kural listesi aşağıda belirtilmiştir.

Saldırı Türü	**Kurallar**
DDOS	1 saniye içerisinde aynı IP'den 1000'den fazla istek
SQL Injection	5 saniye içerisinde aynı IP'den
XSS	5 saniye içerisinde 50 istek atılmıştır.
Path Scanning	20 saniye içerisinde 6 adet HTTP 404 alınacak path'lere istek atılmıştır.
APT	48 saat içerisinde 1000 adet 404 alınacak path'lere istek atılmıştır.
Brute-force	10 saniye içerisinde 30 adet HTTP 500 alınacak HTTP POST atılmıştır.

A. *Uygulama çalışabilirliği*

Uygulama Tablo 5'deki saldırı türlerinin WUKAS üzerinde ayrı zaman dilimlerinde gerçekleştirilmesi kapsamında yapılmıştır. Bu kapsamdaki akış şeması aşağıda belirtilmiştir.



Şekil 4- Test akış şeması

Şekil 4'de belirtilen test akış şeması WUKAS uygulaması için denenmiş olup bütün saldırı türleri bu testi %100 başarıyla tamamlamıştır.

B. *Performans*

WUKAS uygulaması kural tanımlama konusunda bir limit belirtmemekle birlikte kullanıcının tanımladığı kural sayısı arttıkça bir döngü için geçen sürenin artacağı tahmin edilmektedir.

Bu test aşamasında WUKAS uygulamasının tek bir istek tipi karşısında kural sayısının döngü için gereken süreye etkisine bakılacaktır. Önceki aşamalarda anlatıldığı üzere bir isteğin bütün kurallardan geçip bir karara bağlanmasına kadar olan süreye döngü denilmektedir.

Bu performans testinde her kural sayısı n için saldırgan yalnızca bir tane güvenilir paket yollayacaktır. Döngü için geçen süre t(ms) olarak hesaplanacaktır. Kural tipi olarak "3 saniye içerisinde, aynı IP'ye, 1500'den fazla HTTP 400 response'ı gönderilmiş mi?" şeklinde ifade edilecek bir kural tanımlanmıştır. Test boyunca n arttırılıp t gözlenmiştir. Her n arttırıldığı zaman WUKAS karalistesi temizlenmiştir.

Döngünün hesaplanması WUKAS log sistemi takip edilerek izlenmiştir. Sonuçlar aşağıdaki tabloda gösterilmiş olup kural miktarı n aralık olarak verilmiştir.

n	**t**
1-5	180-280ms
5-15	280-560ms
15-100	560ms-10s

Tablo 6- Performans testi sonuçları

Performans testi sonunda kural sayısı arttıkça döngü süresinin katlanarak arttığı tespit edilmiştir.

V. SONUÇ

Bu kağıtta IDS ve IPS'in gerçek hayat üzerinde kullanımına yönelik bir uygulama sunulmuştur. Bu uygulama kural tabanlı koruma ile IDS ve IP bazında savunma ile IPS yöntemlerini sağlamıştır. Bu uygulamayla birlikte siber güvenlik sektöründeki iş yükünün azaltılarak siber güvenlik önlemlerinin otomatize edilmesi ve otomatize sistemler ile IDS/IPS sistemlerinin insan çalışana göre hızlandırılması amaçlanmıştır. Bu çalışamalar sonucunda bir IDPS uygulaması olan WUKAS önerilmiştir.

REFERANSLAR

[1] Shaohua Teng, Naiqi Wu, *Senior Member*, Haibin Zhu, Luyao Teng, and Wei Zhang, "SVM-DT-Based Adaptive and Collaborative Intrusion Detection," IEEE/CAA JOURNAL OF AUTOMATICA SINICA, VOL. 5, NO. 1, JANUARY 2018

[2] CHUANLONG YIN , YUEFEI ZHU, JINLONG FEI, AND XINZHENG HE, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," IEEE Access, 2017

[3] Tomcat 7–Open source implementation of the Java Servlet, JavaServer Pages, Java Expression Language and Java WebSocket technologies. Erişim Zamanı: Aralık. 2017. [İnternet]. Kaynak: http://tomcat.apache.org/

[4] Spring Framework 5–End-to-end support for reactive & servlet based apps on the JVM. Erişim Zamanı: Aralık. 2017. [İnternet]. Kaynak: http://spring.io/

[5] Java EE–Java Platform, Enterprise Edition (Java EE) is the standard in community-driven enterprise software. Erişim Zamanı: Aralık. 2017. [İnternet]. Kaynak: http://www.oracle.com/technetwork/java/javaee/overview/index.html

[6] Anna L. Buczak, Erhan Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 18, NO. 2, SECOND QUARTER 2016

[7] Glassfish– Open Source Java EE Reference Implementation. Erişim Zamanı: Aralık. 2017. [İnternet]. Kaynak: https://javaee.github.io/glassfish/

[8] TomEE–The Embedded or Remote EE Application Server. Erişim Zamanı: Aralık. 2017. [İnternet]. Kaynak: http://tomee.apache.org/

[9] PostgreSQL–Powerful, open source object-relational database system. Erişim Zamanı: Aralık. 2017. [İnternet]. Kaynak: https://www.postgresql.org

[10] Thread–Thread of execution in a program. Erişim Zamanı: Aralık. 2017. [İnternet]. Kaynak: https://docs.oracle.com/javase/7/docs/api/java/lang/Thread.html

[11] Kali Linux–Advanced Penetration Testing Distribution. Erişim Zamanı: Aralık. 2017. [İnternet]. Kaynak: https://www.kali.org/

[12] GoldenEye–HTTP DoS Test Tool. Erişim Zamanı: Aralık. 2017. [İnternet]. Kaynak: https://github.com/jseidl/GoldenEye

[13] Sqlmap–Open source penetration testing tool. Erişim Zamanı: Aralık. 2017. [İnternet]. Kaynak: http://sqlmap.org/

[14] XSSer–Cross Site "Scripter" (aka XSSer) is an automatic -framework- to detect, exploit and report XSS vulnerabilities in web-based applications. Erişim Zamanı: Aralık. 2017. [İnternet]. Kaynak: https://xsser.03c8.net/

[15] Burp Suite–Graphical tool for testing Web application security. Erişim Zamanı: Aralık. 2017. [İnternet]. Kaynak: https://portswigger.net/burp

[16] Hydra–Brute force crack a remote authentication service. Erişim Zamanı: Aralık. 2017. [İnternet]. Kaynak: http://sectools.org/tool/hydra/