ISSN 1300-4646 | e-ISSN 2147-7582 **Research Article/ Araştırma Makalesi**

ATATÜRK ÜNİVERSİTESİ / ATATÜRK UNIVERSITY

İKTİSADİ VE İDARİ BİLİMLER DERGİSİ / JOURNAL OF ECONOMICS AND ADMINISTRATIVE SCIENCES

Web Uygulamalarında Güvenlik ve Süreç Etkinliği Kapsamında Bir Araç: DEBSA[1]

Hakan AŞAN[2]
Yılmaz GÖKŞEN[3]

Geliş Tarihi/ Received	Kabul Tarihi/ Accepted	Yayın Tarihi/ Published
23/06/2020	*29/09/2020*	*23/10/2020*

Citation/Atıf: *Aşan, H. ve Gökşen, Y., (2020), Web Uygulamalarında Güvenlik ve Süreç Etkinliği Kapsamında Bir Araç: DEBSA, Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi, 34(4): Sayfa: 1407-1430, DOI: https://doi.org/10.16951/atauniiibd.756761*

Öz: İnternet kullanımının yaygınlaşması hem bireysel anlamda hem de organizasyonlar açısından web uygulamalarının kullanımını arttırmıştır. Buna bağlı olarak gönderilen, alınan, saklanan ve analiz edilen veri hacminde önemli bir artış olmuştur. Web uygulamalarındaki bu bilgiye sahip olmak için web uygulamalarına yapılan saldırılar ise her geçen gün artmaktadır. Kişiler veya kurumlar web uygulamalarına yapılan bu saldırıları önlemek amacıyla güvenlik önlemlerine gereksinim duymaktadırlar. Web uygulamalarının geliştirilmesi aşamasında ne kadar önlem alınırsa alınsın bazı güvenlik açıkları kaçınılmazdır. Bu nedenle geliştirme aşamasında alınacak önlemlerin yanında, web uygulamalarının sürekli kontrol ve denetim altında tutulması gerekmektedir. Web uygulamalarını test etmek için birçok yazılım geliştirilmiştir. Ancak bu testlerin gerçekleşmesi kadar web uygulamalarının güvenliğinin sürekliliğinin de sağlanması gerekmektedir. Web uygulamalarının sürekli olarak kontrolünün bireysel olarak yapılması neredeyse imkânsızdır. Bu kontrollerin testi gerçekleştiren yazılım tarafından planlanması sürekliliği sağlayacaktır.

Bu çalışmanın genel amacı web uygulamalarının güvenliğini denetim altına alacak bir süreç modeli geliştirmektir. Bu anlamda web uygulamalarını test eden ve bunu süreçler haline getirebilen bir yazılım geliştirilmiştir. Geliştirilen yazılım, web uygulamaları üzerindeki güvenlik açıklarını bulan testleri gerçekleştirmektedir. Ayrıca bu yazılım, üzerinde bulunan süreç yönetimi bölümü ile bu testlerin planlanmasını ve kontrolden sorumlu kişilerin otomatik olarak bilgilendirilmesini sağlamaktadır.

Anahtar Kelimeler: Bilgi Güvenliği, Web Uygulamaları, Web Saldırıları, Süreç Etkinliği, Web Güvenlik Yazılımları

Development on Focus of Security and Process Effectiveness for Web Applications: DEBSA

Abstract: *The spread of internet usage has been increased the usage of web applications with regards to both individuals and organizations. Attacks on web applications are increasing day by day in order to have this knowledge in web applications. Some security measures are needed to*

[1]*Bu çalışma Prof. Dr. Yılmaz GÖKŞEN danışmanlığında Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Yönetim Bilişim Sistemleri Anabilim dalında yürütülen "Web Uygulamalarında Güvenlik ve Denetim Kapsamında Bir Araç Geliştirme" adlı yüksek lisans çalışmasından türetilmiştir.*

[2]*Arş. Gör., Dokuz Eylül Üniversitesi, İzmir Meslek Yüksekokulu, İktisadi ve İdari Programlar Bölümü, https://orcid.org/0000-0001-9550-3345*

[3]*Prof. Dr., Dokuz Eylül Üniversitesi, İktisadi ve İdari Bilimler Fakültesi Yönetim Bilişim Sistemleri Bölümü, https://orcid.org/0000-0002-2291-2946*

prevent these attacks on web applications by people or organizations. During development of web applications, some security holes are inevitable although how measures are taken. Therefore, besides these measures, web applications should keep control and audit continuously. Many software has been developed to test web application. However, besides these tests, it is necessary to provide the continuity of security of web applications. Continuity of control of web applications is almost impossible on an individual basis. Planning these controls by software that performs tests, provides continuity.

The general purpose of this study is to develop a process model that will control the security of web applications. In this sense, a software has been developed that tests web applications and can turn it into processes. The developed software carries out tests that find vulnerabilities on web applications..Also, this software provides planning tests by means of process management part on it and informing people who are responsible for control automatically.

Keywords: *Information Security, Web Applications, Web Attacks, Process Effectiveness, Web Security Software's*

EXTENDED SUMMARY

Research Problem

Today, the internet is often used for many purposes. There are many websites belonging to businesses or individuals. Websites belonging to public or private businesses are especially at risk from various aspects. In order to prevent these risks, various tests should be done periodically.

The purpose of this study is to develop a process model that will control the security of web applications. In this sense, a software has been developed that tests web applications and turns into processes. The developed software carries out tests that find security gaps on web applications. Also, this software provides planning of these tests and automatic notification of the people who responsible for control thanks to the process management section.

Literature Review

Research and experience show that websites are at risk; According to the Risk Based Security Report, 7,098 attacks were carried out in 2019, and 15.1 billion records are thought to be affected by these attacks. The number of records affected increased by 284% compared to 2018. The biggest target attacked was the information sector and the health sector (Risk Based Security Raporu, 2020).

It may take time for organizations to notice gaps in their websites. The average time to detect a violation in 2019 was 276 Days (IBM Security, 2019). Some organizations are not even aware of the websites openly. 64% of Americans never checked if they were affected by data breach, and 56% of Americans don't know what steps to take in case of data breach (Sobers, 2020). 66% of businesses hacked by hackers were not sure they could recover (Roberts & Lashınsky, 2017).

These attacks on websites can cause serious material and moral losses. The average cost of the data breach was calculated as $ 3.9 million. (IBM Security, 2019). Cybercrime has cost the world about $ 600 billion in 2018 (Lau, 2018). Cyber worldwide is estimated to reach $ 133.7 billion in 2022 (Moore and Keen, 2018).

The procedures and technologies used to access, disclose and abuse this information contained in web applications without permission, are protected as information security (UNCTAD, 2005). Information security consists of three basic elements. Fulfilling these basic elements means ensuring information security (TSE, 2006). In their report published in 2017, 10 major security risks were listed as follows (OWASP, 2020).

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access control
- Security misconfigurations
- Cross Site Scripting (XSS)
- Insecure Deserialization
- Using Components with known vulnerabilities
- Insufficient logging and monitoring

Applications similar to DEBSA;

Application Name	**Works on Platform**	**License**
Paros	Windows, Linux, Unix	Free
Firebug	Windows, Linux, Unix	Free
Acunetix Web Vulnerability Scanner	Windows	Free
WebInspect	Windows	Paid
WebScarab	Windows, Linux, Unix	Free
Nessus	Server: Linux, Client: Windows, Linux, Unix	Free for Individual Use
OpenVAS	Windows, Linux, Unix	Free

Methodology

Today, the internet is often used for many purposes. There are many websites belonging to businesses or individuals. Websites belonging to public or private businesses are especially at risk from various aspects. In order to prevent these risks, various tests should be done periodically.

The purpose of this study is to develop a process model that will control the security of web applications. In this sense, a software has been developed that tests web applications and turns into processes. The developed software carries out tests that find security gaps on web applications. Also, this software provides planning of these tests and automatic notification of the people who responsible for control thanks to the process management section.

In this study, a new application named DEBSA (Dokuz Eylul University Baseline Security Analyzer) was developed. DEBSA is a basic application test software, but unlike other applications, it contains user management and process management features. User management aims to provide isolation among users for multi-user organizations. In this sense, it enables different users to test different websites and create different reports. DEBSA aims to be able to apply

tests applied to web applications continuously. The software has its own process management section. This section enables the users to operate every work through a process and automate it if required. The tests to be made and the reports that take place take place automatically at the given time and the users are informed. The design of the process can be done with simple drag and drop operations. The actions put on the screen can be turned into a process and these processes are repeated at the desired dates. This autonomous system makes automatic testing of continuously developed web software provides instant action against possible troubles.

Results and Conclusions

There are many software in the industry, such as test software examined in this study. Some of these software are produced for commercial purposes, while others are open source software. These softwares are generally presented to the user by testing and recording the tests. However, these test tools have deficiencies in terms of continuity and user differentiation. This study aims to develop a new software under the name of Dokuz Eylul University Baseline Security Analyzer (DEBSA) considering these deficiencies. The software has been tested in terms of security and some additions have been made regarding the parts that are missing in existing software. The software has been tested for security and also some additions have been made regarding the parts that are missing in existing software.

DEBSA software consists of two parts. The first part is the design part and runs on the Windows platform. In this section, the user makes the program settings. Process design screen is also made in this section. The second part works on the web. In this part, the user can view the processes and related reports from any point.

In future similar studies, besides testing the web applications, it can be emphasized that innovations related to the continuity of the tests. Effective flows can be created by developing different process elements in the process design part of DEBSA software. In addition, algorithms that test web applications from different directions can be developed or improvements can be made on existing algorithms.

1. Giriş

İnsanlar hem kurumsal anlamda hem de bireysel anlamda interneti sıklıkla kullanmaktadırlar. İnternet üzerinde yapılan her türlü işlem bir anlamda veri olarak kaydedilmektedir. İnternet kullanımı insan hayatını kolaylaştıran çok önemli bir unsur olarak görünse de güvenlik anlamında bazı sıkıntıları da beraberinde getirmektedir. Bu sıkıntıların temel nedeni internet uygulamalarının, bilgiyi evrensel bir boyuta taşıması ve böylelikle bilginin de dış tehditlere açık bir hale gelmesidir. Farklı nedenlerden dolayı kötü niyetli insanlar web uygulamalarına saldırılar düzenleyebilirler. Özellikle büyük ölçekli ve marka değeri yüksek olan firmalar hem önemli bilgilere sahip olmaları hem de saldırganın elde edeceği tanınma gücü nedeniyle hedef olarak seçilebilmektedir.

Yapılan çalışmalar ve deneyimler web sitelerinin ciddi riskler altında olduğunu göstermektedir; Risk Based Security Raporuna göre 2019 yılında 7,098 saldırı düzenlenmiştir ve bu saldırılardan 15.1 Milyar kayıt etkilendiği düşünülmektedir. Etkilenen kayıt sayısı 2018 yılına göre % 284 artmıştır. Saldırılan en büyük hedefi bilgi sektörü ve sağlık sektörü olmuştur (Risk Based Security Raporu, 2020).

Organizasyonların kendi web sitelerindeki açıkları fark etmeleri ve önlem alabilmeleri zaman alabilmektedir. 2019 yılında bir ihlali tespit etmek için ortalama süre 276 Gün olarak tespit edilmiştir (IBM Security, 2019). Amerikalıların %64'ü veri ihlalinden etkilenip etkilenmediğini hiç kontrol etmedi ve Amerikalıların %56'sı veri ihlali durumunda hangi adımları atacaklarını bilmiyor (Sobers, 2020). Bilgisayar korsanları tarafından saldırıya uğrayan işletmelerin %66'sı iyileşebileceklerinden emin değildi (Roberts ve Lashınsky , 2017).

Web sitelerine yapılan bu saldırılar maddi ve manevi ciddi kayıplara neden olabilmektedir. Veri ihlalinin ortalama maliyeti 3.9 Milyon Dolar olarak hesaplanmıştır. (IBM Security, 2019). Siber suçlar 2018'de dünyaya yaklaşık 600 milyar dolara mal olmuştur (Lau,2018). Veri ihlalleri 2019'un ilk yarısında 4,1 Milyar'ı geçmiştir (Risk Based Security Raporu, 2020). 2020'de Veri ihlallerinin maliyeti 150 milyon dolara yükseleceği (Smith, 2019) ve bu rakamın Dünya genelinde siber 2022'de 133,7 milyar dolara ulaşacağı tahmin edilmektedir (Moore ve Keen, 2018).

Bu sebepten, web uygulamalarının saldırılara karşı korunması amacıyla birçok önlem alınmaktadır. Web uygulamalarının barındırdığı bu bilgilere izinsiz şekilde erişilmesi, ifşa edilmesi ve kötüye kullanılmasına, değiştirilmesine veya zarar ve kayıptan korumak için yapılan işlemler ve kullanılan teknolojilere bilgi güvenliği adı verilmektedir (UNCTAD, 2005). Bilgi güvenliği için üç temel unsurun sağlanması çok önemlidir. Bu unsurlar; gizlilik, bütünlük ve erişilebilirliktir. Bu unsurların yanında yardımcı unsurlar da bulunmaktadır. Tüm bu unsurlardan herhangi birinin olmaması bilgi güvenliğinin tam anlamıyla sağlanamaması ile sonuçlanır. Örneğin yeterli gizliliğe sahip bir bilginin bütün olarak görüntülenememesi bilgi güvenliğinin sağlanmadığı anlamı taşımaktadır.

Dinamik yapıya sahip web uygulamaları daha sıklıkla saldırganların hedefi olmaktadır. Günde ortalama 30 Bin web sitesinin hacklendiği tahmin edilmektedir (Smith, 2019). Web uygulamalarının bilgileri genel olarak veritabanlarında tutulduğundan, saldırganlar hem uygulama hem de bilgi deposu rolündeki veritabanına saldırı düzenlemeyi hedeflemektedir. Saldırganlar birçok teknikle saldırılar düzenlemektedirler. Bu açıkların bazıları direk uygulamanın kendisini, bazıları da uygulamayı kullanan kişileri etkilemektedir. Web sitelerinin % 46 'sında yüksek güvenlik zafiyeti, %87 sinde orta güvenlikte zafiyeti bulunmaktadır (Acunetix, 2019).

Web sitelerinin güvenliğinin ne denli önemli olduğunu görmek açısından bir çok örnek incelenebilir; 2017 yılında Friendfinder'ın sitelerinden 412 milyon

kullanıcı hesabı çalınmıştır. (McMillan, 2016). 2017 yılında 147,9 Milyon tüketici Equifax İhlali'nden etkilendi (Gutzmer, 2017). Under Armour, 2018 yılında "My Fitness Pal" inin saldırıya uğradığını ve 150 milyon kullanıcıyı etkilediğini bildirmiştir. (Under Armour, 2018). 2017 yılında Yahoo'nun açıklamasına göre 2013 de yapılan saldırılar sonucunda 3 Milyar hesap etkilenmiştir (Perlroth, 2017). Equifax'tan 209 Bin ödeme kartı numarası ve son kullanma tarihi çalınmıştır (BBC, 2019). 2018 yılında Marriott 500 Milyon kullanıcıların bilgileri ele geçirildi (Fruhlinger,2020). Bilgisayar korsanları Hindistan'daki Cosmos Bank'tan 13.4 milyon dolar çektiler (Inamdar, 2018). Carbanak hacker çetesi toplamda 1 milyar doların üzerinde para çaldı (Meyer, 2018).

Web uygulamalarına yönelik yapılan saldırılara karşı, bu uygulamaların geliştirilmesi aşamasında önlemler alınabilir. Ancak gözden kaçırılan bazı durumlar veya bilgi eksikliği nedeniyle bazı açıkların oluşması olasıdır. Araştırmalara göre, finansal kurumların veri ihlalini tespit etmesi ortalama 98 gün sürüyor ve perakendeciler için bu süre 197 güne kadar sürebilmektedir (Osborne, 2020). Bu açıkları saptayabilmek ve bunları kapatabilmek için web uygulamaları test edilmektedir. Bu testleri gerçekleştirmek için çeşitli yazılımlar geliştirilmiştir. Bu yazılımların bazıları ticari amaçlı, bazıları ücretsiz olarak kullanıcılara sunulmaktadır. Bu yazılımlar çalışabildikleri ortamlar anlamında da farklılıklar göstermektedirler. Windows, Linux veya Macintosh gibi farklı işletim sistemleri üzerinde çalışabilmektedirler.

Çalışmada DEBSA (Dokuz Eylul University Baseline Security Analyzer) ismi verilen yeni bir uygulama geliştirilmiştir. DEBSA temel anlamda bir uygulama test yazılımı olmakla beraber diğer uygulamalardan farklı olarak içerisinde kullanıcı yönetimi ve süreç yönetimi özelliklerini barındırmaktadır. Kullanıcı yönetimi çok kullanıcılı organizasyonlar için kullanıcılar arasında yalıtım sağlanması hedeflemektedir. Bu anlamda farklı kullanıcıların farklı web sitelerini test edebilmelerini ve farklı raporlar oluşturabilmelerini sağlamaktadır.

DEBSA, web uygulamalarına uygulanan testlerin sürekli olarak uygulanabilmesini sağlamayı hedeflemektedir. Bu anlamda kendine ait bir süreç yönetimi bölümü bulunmaktadır. Bu bölüm kullanıcıların yapılan her işi bir süreç üzerinden işletebilmesini ve istenildiği durumda otomatik hale getirmesini sağlamaktadır. Yapılacak testler ve ortaya çıkan raporlar, otomatik olarak verilen zamanda gerçekleşmekte ve kullanıcılar bilgilendirilmektedir. Sürecin tasarımı basit sürükle bırak işlemleri ile yapılabilmektedir. Ekrana koyulan işlemler bir süreç haline getirilebilmekte ve bu süreçler istenilen tarihlerde tekrarlanabilmektedir. Bu otonom sistem, sürekli geliştirilen web yazılımlarının testlerinin otomatik yapılması ile oluşabilecek sıkıntılara karşı anlık önlem almayı sağlayabilmektedir.

DEBSA yazılımı süreç tasarımı ve planlamasını Windows tabanlı bir yazılım ile yaparken, süreçlerin yönetilmesi ve planlanması web uygulaması gerçekleştirilebilmektedir. Kullanıcı işlemleri, raporları, süreçleri web

uygulaması üzerinden kontrol edebilir. Kullanıcı istediği testi yapabilir, raporları izleyebilir. Bu şekilde platform üzerinde bağımsız işlemler yapılabilmesi sağlanmıştır.

2. Bilgi Güvenliği

Organizasyonlar için bilgi; mevcut sistemlerini yönetmek, geleceğe dair uzun veya kısa vadeli planlamalar yapmak açısından çok önemlidir. Özellikle stratejik seviyedeki yöneticilerin alacağı kararlar firmanın geleceğini belirmesi açısından ayrıca önem arz etmektedir. Bu anlamda bu seviyedeki bilgiyi elde etmek ne kadar değerliyse onu korumak da onun kadar değerlidir. Bilginin korunması için yapılan işlemlere, kullanılan teknolojilere verilen genel isim bilgi güvenliğidir. Bilgi güvenliğinin farklı kaynaklardaki tanımları Tablo 1 de bir araya getirilmiştir.

Tablo 1. *Bilgi Güvenliği Tanımları*

Kaynak	**Bilgi Güvenliği Tanımı**
(UNCTAD, 2005: 187)	Bilgiye izinsiz erişilmesi, ifşa edilmesi ve kötüye kullanılmasına, değiştirilmesine veya zarar ve kayıptan korumak için yapılan işlemlerin ve kullanılan teknolojilerin hepsidir.
(Calder ve Watkins, 2008: 4)	Bilgi hangi yapıda veya şekilde olursa olsun, onu gereken biçimlerde ve düzeyde korunması için oluşturulan süreçler ve çözümlerin tümüdür.
(Gonzales ve Sawicka, 2002: 449)	Bilgi güvenliğinin insan ve teknoloji gibi iki unsuru vardır. Bir güvenlik sisteminin ne kadar doğru şekilde tasarlanmış ve uygulanmış olsa da sonuçta bir insana bağlı olduğu ve sistemin insan tarafının da iyi anlaşılması gerekmektedir.
(Tudor, 2001: 1)	Kaydedilen, paylaşılan, elektronik ortamdan alınan veya aktarılan bilginin güvenliğidir.
(TS ISO/IEC 17799: 4)	Bilginin güvenilir olması, gizliliğinin korunması ve elverişliliğine denir.
(Özavcı, 2002).	Veri bütünlüğünün sağlanması, gizliliğin korunması, sistemin devamlılığı ve erişebilmenin denetlenebilir olması bilgi güvenliğinin amacıdır.
(Kajava v.d., 2006: 2091).	Doğru şekilde uygulanmış, kontrolleri yapılmış bir bilgi güvenliği yönetim sistemi, bir masraf olmaktan çok, organizasyona başarı sağlayacaktır.
(Bilişim Sistemleri Güvenliği El Kitabı, 2006)	Bireysel veya organizasyonel açıdan kararlara kaynak sağlayacak ve farklı şekillerde saklanan, işlem görmüş verilerin her türlü tehlikeye karşı korunmasına bilgi güvenliği adı verilir.
(Türkiye'de Bilişim Güvenliği Analizi, 2009)	Geçmiş dönemde fiziksel anlamda güvenlik sağlanması bilgi güvenliği olarak düşünülürken, şimdilerde bu durum en çok sıkıntı çektikleri durumların başında gelmektedir.
(ISO/IEC 17799:2005, 2005)	Bilginin kullanılabilirliğinin, bütünlüğünün korunması ve gizliliğinin saklanmasına bilgi güvenliği adı verilir. Bu özelliklerin yanında açıklanabilirlik, inkâr edememe ve doğruluk gibi özellikleri de sağlaması gereklidir.
(Canbek ve Sağıroğlu, 2006: 169)	Bilginin bozulmalardan korunması ve doğru şekilde, yetkili kişiler tarafından kullanılmasını sağlayan sisteme verilen isimdir.

Bilgi güvenliği, üç temel öğeden oluşur. Bu temel öğelerin yerine getirilmesi bilgi güvenliğinin sağlanması anlamına gelir (TSE, 2006). Bazı kaynaklar bu üç temel öğenin yanına yardımcı bazı öğeleri de eklemektedir.

2.1. Bilgi Güvenliğinin Temel Unsurları

Bilgi güvenliğinin temel öğeleri; gizlilik, bütünlük ve kullanılabilirlik olarak tanımlanır (Pfleeger, 2007) (Fussell, 2005). Bu üç temel unsur birlikte ele alınmalıdır. Her bir unsur diğerlerinden bağımsız bir anlam ifade etmemektedir. Erişim sağlanamayan bir bilginin gizliliğinin olması veya erişilen bir bilginin bütünlüğünün olmaması bilgi açısından güvenli olduğu anlamını taşımaz. Bu üç temel unsurun birlikte sağlanması bilginin güvenliği açısından çok önemlidir (Fussell, 2005).

2.1.1 Gizlilik

Bilgi güvenliğinin unsurlarından birincisi gizliliktir. Gizlilik, bilginin yetkisi olmayan bir kişi tarafından görülmesinin engellenmesidir (Lehtinen, 2006) (Önel ve Dinçkan, 2007). Gizlilik temel anlamda bilgiye erişmeye izni olan kişilerin bilgiye ulaşabilmesidir. Bunun dışındaki kişilerin bilgiye herhangi bir şekilde erişmesi, üzerinde değişiklik yapması bilginin gizliliğini kaybetmesine neden olur.

Bilgi güvenliğinin gizlilik ilkesi genellikle organizasyonlar tarafından kurallarla, kanunlarla sınırlandırılır. Kurum içinde herkes kendi iş tanımı dâhilinde bilgiye sahip olur. Hatta bu gizlilik kuralları çeşitli çerçeveler ile sınırlandırılır. Bazı kişiler bilgileri sadece okuma, bazıları ise hem okuyup değiştirme yetkisine sahip olabilir. Bu yetki sınırlandırmaları bilgi güvenliği için gizliliğin korunması açısından son derece önemlidir.

2.1.2 Bütünlük

Bilgi güvenliğinin temel unsurlarından bir diğeri bilginin bütünlüğüdür. Bilginin bütünlüğü, bilginin süreç içinde herhangi bir zaman aralığında bilinçli veya bilinçsiz şekilde yetkisi olmayan kişiler tarafından bilgiyi oluşturan verinin değişimini önlemek ve verinin belli bir bütün içinde korunmasını sağlamaktır (Saatçi, 2002). Bilgi bir bütün olarak anlamlıdır. Bilginin küçük bir kısmının bile zarar görmesi bilginin bütünlüğünü bozar. Özellikle bütünlüğü bozulan bir bilgi karar verme sürecinde kullanıyorsa karar vericiyi yanlış yönlendirebilir. Bilgi güvenliğinin sağlanması açısından bilginin bir bütün olarak saklanması gereklidir.

2.1.3 Erişilebilirlik

Bilgi güvenliğinin son temel unsuru erişilebilirliktir. Bilginin erişilebilir olması demek en basit anlamda, yetki dâhilinde bilginin ihtiyaç duyulan her anda kullanılabilir olmasıdır. Erişilebilirlikte yetkilendirme çok önemlidir. Doğru ve güvenli bir şekilde yapılandırılmalıdır. Aksi takdirde "Servisin Reddi (Denial of Service)" isimli sistem saldırısı ile karşılaşılabilir (Steve, 2003).

Bilgi güvenliğinin erişilebilirlik kavramı gizlilik ile karıştırılabilir. Ancak bilginin erişilebilir olması bilgiye ulaşmak ile ilgilidir. Kimin hangi düzeyde

ulaşabileceği ile ilgili bir denetim gerçekleştirmez. Sadece bilginin erişilebilir olması bu unsurun sağlanmasını sağlar.

2.2. Bilgi Güvenliğinin Yardımcı Unsurları

• Kimlik Sınama

Kullanıcının sisteme girişi sırasında giriş için izni olduğunu kanıtlamasıdır. Bu sistem özellikle bilişim dünyası için kullanılsa da fiziksel anlamda da akıllı kartlar, parmak izi gibi kimlik sınamaları kullanılmaktadır. Kimlik sınaması sisteme kullanıcının kaydedilmesi ile başlar. Kullanıcıya bir şifre veya sadece ona ait olan bir özellik atanır. Kullanıcı giriş yapacağı sırada bu özelliği veya şifreyi girerek sisteme giriş yapar.

• İnkâr Edememe

Kullanıcılar arasında yapılan işlemlerde bir kullanıcının diğer kullanıcıyla olan bilgi paylaşımı yaptıktan sonra, tarafların bu bilgi alışverişini inkâr etmesini önleyen güvenlik servisleridir. Bu işlem için haberleşme sırasında özel bazı tanımlayıcı işaretler eklenir veya bu işlemler kayıt altına alınır. Anlaşmazlık veya inkâr durumunda bu kayıtlar açılarak kontrol edilir. E-imza teknolojisi ile bu tür inkâr durumları zorlaşmıştır.

• Kayıt Tutma

Yapılan tüm işlemlerin kayıt altına alınmasıdır. Bu şekilde kim hangi sorumlulukta hangi işlemi yapmış, nasıl davranış göstermiş raporlanabilir ve oluşabilecek sorunların sorumluları ortaya çıkarılabilir. Kısacası belli sistem içerisinde yapılan tüm işlemlerin sonradan gözden geçirilmesine olanak sağlayacak şekilde kaydedilmesidir.

• Güvenilirlik

Bir sistemin belli bir şartname veya tasarım gerekliliklerini kesintisiz olarak, taviz vermeden yapabilme yeteneğine verilen isimdir.

• Emniyet

Bilgilerin tutulduğu sistemin fiziksel ortam olarak korunaklı olmasıdır. Yangın, sel, deprem gibi doğal afetlere veya insan hatasıyla ortaya çıkan çeşitli durumlara karşı bilgilerin korunması önemlidir. Bu nedenden gerekli tedbirlerin alınması işlemine emniyet adı verilir.

• Kurtarılabilirlik

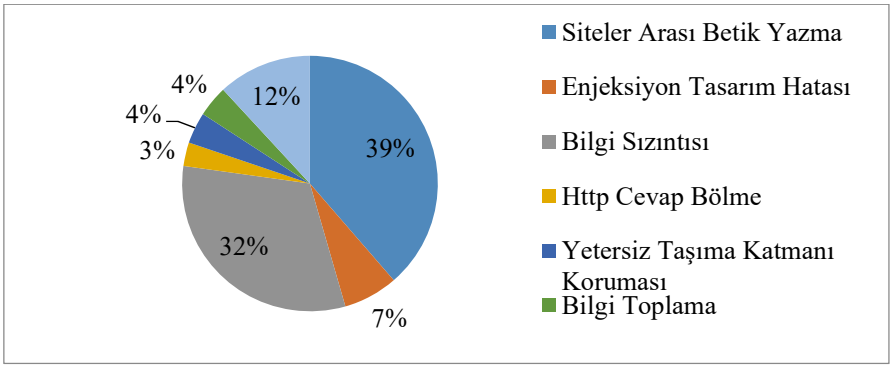
Bilginin herhangi bir durumda tekrar elde edilebilmesi işlemidir. Kayıtların belli periyotlarda yedeklenmesi ile bu işlem gerçekleştirilir. Bu yedek kayıtların farklı bir yerde olması oluşabilecek her türlü duruma karşı önlem almayı kolaylaştırır.

3. Web Uygulamaları

Kullanıcıların sunucu üzerinde kodları çalıştırması ile oluşan etkileşime verilen isimdir. Bu kodlar farklı şekillerde oluşturulabilir. Bu kodlar sitenin sahibi tarafından da yazılabilir veya ticari olarak bir firmadan alınabilir. Farklı bir tanım olarak internet ağı üzerinden belli bir amaç doğrultusunda oluşturulan ve belli kullanıcı profiline sunulan sistemler web uygulamaları diye adlandırılır (Negash, 2003).

Web uygulamaları amaçları doğrultusunda içerik olarak büyük miktarda bilgi bulundurabilirler. Farklı amaçlarla bu bilgiye sahip olmak isteyen insanlar olabilir. İnternetin sağlamış olduğu her yerden erişim imkânı da bu bilgiyi daha cazip hale getirir ve web uygulamalarını çeşitli tehditlerle karşı karşıya bırakır.

WASC organizasyonun 2008 yılında yaptığı bir çalışmada 12.186 web sitesi taranmış ve ortaya çıkan açıklıklar Şekil 1 de gösterilmiştir (Gordeychik, 2018).



Şekil 1. *Yapılan Saldırıların Dağılımı*

Benzer bir çalışma Open Web Application Security Project (OWASP) tarafından yapılmıştır. OWASP 2007, 2010 ve 2013,2017 yıllarında "OWASP TOP 10" adlı bir raporlarını yayınlamıştır. 2017 yılında yayınladıkları raporda 10 önemli güvenlik riskini olarak aşağıdaki gibi listelenmiştir (OWASP, 2020).

- ✓ SQL Enjeksiyon
- ✓ Hatalı Kimlik Doğrulama
- ✓ Hassas Veri Teşhiri
- ✓ XML Dış Varlıklar (XXE)
- ✓ Hatalı Erişim Kontrolü
- ✓ Güvenlik Ayarları Hataları
- ✓ Siteler Arası Betik Yazma (XSS)
- ✓ Güvensiz Deserizasyon
- ✓ Bilinen Güvenlik Açıkları Olan Bileşenleri Kullanma
- ✓ Yetersiz Kayıt Tutma ve Görüntüleme

4. Web Uygulamalarını Denetlemek İçin Kullanılan Yazılımlar

Web uygulamalarını denetlemek için birçok yazılım kullanılmaktadır. Bu yazılımların bazıları ticari amaçlarla üretilirken bazıları ücretsiz bir şekilde sunulmaktadır. Web uygulamalarını denetlemek için kullanılan yazılımlar Tablo 2 de verilmiştir.

Tablo 2. *WEB Uygulamaları Denetim Yazılımları*

Uygulamanın Adı	Çalıştığı Platform	Lisans
Paros	Windows, Linux, Unix	Ücretsiz
Firebug	Windows, Linux, Unix	Ücretsiz
Acunetix Web Vulnerability Scanner	Windows	Ücretli
WebInspect	Windows	Ücretli
WebScarab	Windows, Linux, Unix	Ücretsiz
Nessus	Sunucu: Linux, İstemci: Windows, Linux, Unix	Bireysel Kullanım İçin Ücretsiz
OpenVAS	Windows, Linux, Unix	Ücretsiz

5. Dokuz Eylul Unıversıty Baselıne Securıty Analyzer (DEBSA)

Web sitelerini güvenlik açıklarını denetlemek ve bu işlemi bir süreç haline getirerek için bir uygulama geliştirilmiştir. Uygulamanın adına Dokuz Eylul University Baseline Security Analyzer (DEBSA) ismi verilmiştir. Geliştirilen bu yazılım sadece web uygulamalarının güvenlik testlerini yapmakla kalmayıp, bu tür testlerin yönetici açısından raporlanabilmesini ve üzerinde bulunan süreç yönetimi bölümüyle planlanabilmesini sağlamaktadır. Süreç yönetimi kısmı testlerin bir süreç ile tasarlanmasını ve bu sayede hem testlerin yapılmasını hem de gerekli kişilere bilgi de sağlamaktadır.

Geliştirilen yazılım, mevcut güvenlik test araçları incelenerek ve güncel saldırı türleri ele alınarak geliştirilmiştir. Yazılım Visual Studio kullanılarak, C# dilinde yazılmıştır. Veritabanı olarak Microsoft SQL Server (MSSQL) kullanılmış ancak diğer veritabanı yönetim sistemleri ile çalışabilecek şekilde tasarlanmıştır.

Yazılım iki kısımdan oluşmaktadır. Birinci kısım Windows üzerinde ikinci kısım ise web üzerinde bağımsız platform olarak çalışmaktadır.

5.1. DEBSA Yazılımı – Windows

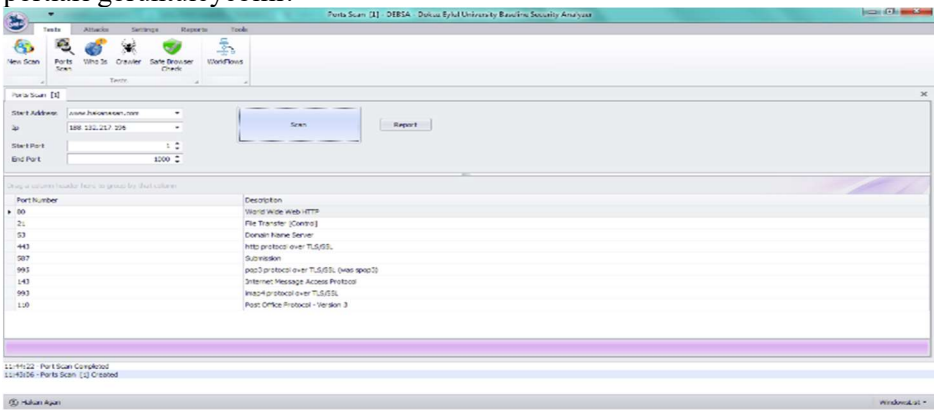
DEBSA yazılımının bu kısmında kullanıcı gerekli ayarlamaları yapabilmekte, testleri gerçekleştirmektedir. Ayrıca süreç yönetimi bölümü ile de belli periyotlarda gerçekleştirilebilecek süreçleri tasarlayabilmektedir.

Şekil 2. *DEBSA Ana Ekran*

DEBSA ana ekranı (Şekil 2) farklı pencerelerin açılabileceği şekilde tasarlanmıştır. Bu şekilde aynı anda birden fazla test yapılabilmesi sağlanmaktadır. Ekranın üst kısmında menü bulunmakta, menü ekranı dokunmatik ekranlı bilgisayarlarda kullanılmak üzere büyük düğmelerden oluşmaktadır. Menü kısmının farklı kullanıcıların yetkilendirmelerine göre bazı bölümleri görünür veya kapanır şekilde ayarlanabilir. Menünün alt kısmında sayfaların açılacağı bölüm bulunmaktadır. Bu bölüm sayfa sayfa ekranları sıralar bu şekilde farklı sayfalar açık olarak işlem yapılabilir. Alt kısımda logların gösterildiği bir kısım bulunmaktadır. Bu log ekranı yapılan her işlemi gösterir. Kullanıcı hangi işlemleri yaptığını log kayıtlarına bakarak anlayabilir. Yönetici olan kişi altındaki kişilerin loglarını da görebilir. Bu şekilde yöneticinin kontrol mekanizması oluşmaktadır.

5.1.1. Port Tarama Ekranı

Uygulamaya giriş yapan kullanıcı menüden testler sekmesinde Port Tarama ekranı (Şekil 3) açarak web uygulamasının bulunduğu sunucudaki açık portları görüntüleyebilir.

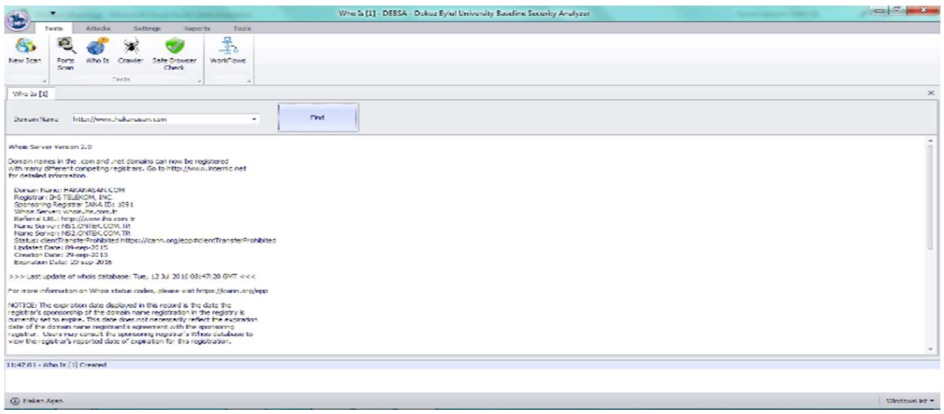


Şekil 3. *DEBSA Port Tarama Ekranı*

Port taraması yapabilmek için web uygulamasının adresi veya ip' si, tarama yapılacak port başlangıç numarası ve bitiş numarası girilir. Sonrasında tarama başlatılır. Tarama sırasında altta bulunan gösterge ile ilerleme izlenilebilir. Açık olan portlar anında listeye düşmeye başlar. Yazılımın kanallı bir sistemde tasarlanması nedeniyle kullanıcı tarama sırasında farklı işlemler yapabilir, birkaç tane tarama başlatabilir. Bulunan portlar özel olarak ayrılmış ise karşılığı ekranda gösterilir.

5.1.2. Alan Adı Sorgu Ekranı

Alan adı sorgu ekranı (Şekil 4) web site ile ilgili alan adı bilgilerini sunar.

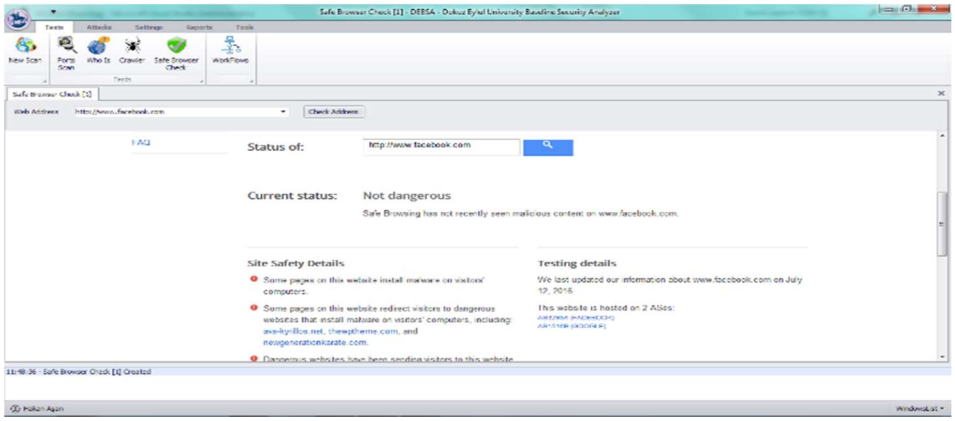


Şekil 4. *Alan Adı Sorgu Ekranı*

Kullanıcı öğrenmek istediği sitenin domain ile ilgili bilgilerine erişebilir. Web adresi sorgu ekranına girilir web uygulaması ile ilgili bilgiler ekranda gösterilir. Sitenin domainin kim tarafından alındığı, süresinin ne zaman biteceği gibi birçok bilgiye bu ekran sayesinde ulaşabilir. Alan Adı sorgu ekranı Şekil 4' de verilmiştir.

5.1.3. Güvenli Site Kontrol Ekranı

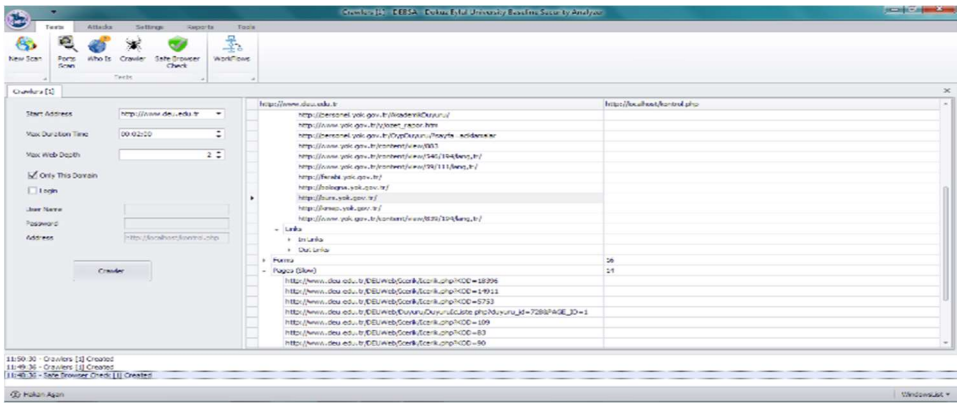
Bu ekran Google tarafından sağlanan bir hizmeti kullanır. Kullanıcı web adresini ekrana girer ve web sitesinin Google tarafından bilgileri görüntülenir. Güvenli site kontrol ekranı Şekil 5' de gösterilmiştir.



Şekil 5. *Güvenli Site Kontrol Ekranı*

5.1.4. Web Crawler (Emeklemesi) Ekranı

Kullanıcı Web Crawler ekranı (Şekil 6) ile sitenin detaylı bir haritası çıkarabilir.



Şekil 6. *Crawler Ekranı*

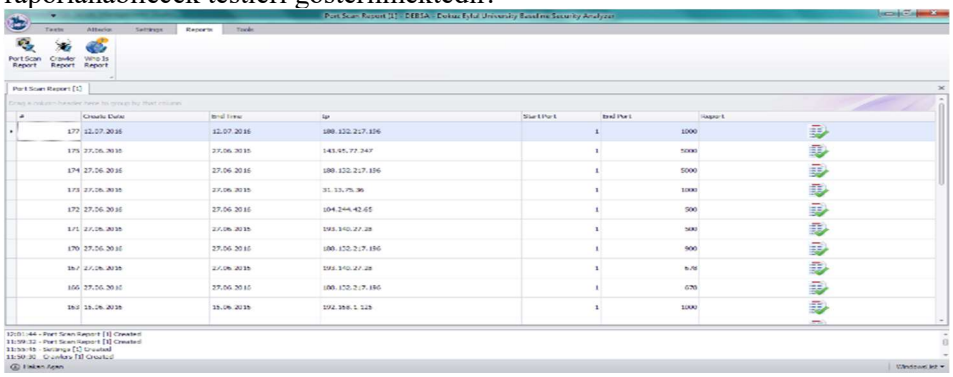
Site içerisine yollanan robotlar siteye ait sayfaları tek tek gezerek, detaylı bilgiler elde ederler. Crawler (Emeklemesi) sonucunda bulunan bazı zafiyetler;

- Yavaş Yüklenen Sayfalar, Resimler
- SQL Enjeksiyon Açığı
- Doğru Ayarlanmamış Form Elemanları
- XSS Açığı
- Bozuk Bağlantılar
- Yanlış ve Tehlikeli Bağlantılar

Crawler ekranında kullanıcıdan bazı parametreler istenir. Bunlar; işlemin ne kadar sürmesi gerektiğini gösteren maksimum bekleme zamanı, hangi derinliğe kadar tarama yapılması gerektiğini gösteren maksimum web derinliği, sadece aynı isimli domainde mi yoksa farklı domainlerde de tarama yapılması için sadece bu domain seçeneği ve kullanıcı bilgileriyle giriş yapılabilmesi için giriş bilgileridir.

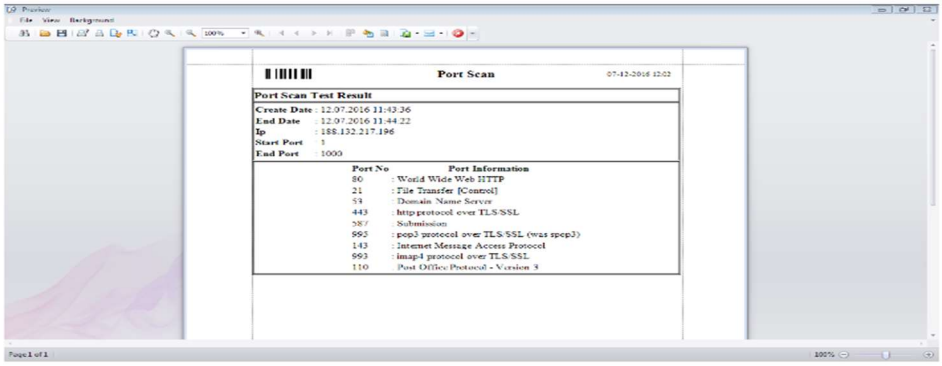
5.1.5. Raporlama Ekranları

DEBSA yazılımı geniş bir raporlama olanağına sahiptir. Her test ve işlem için geniş raporlar bulunmaktadır. Örnek olarak Şekil 7'de port tarama ekranın raporlanabilecek testleri gösterilmektedir.



Şekil 7. *Raporlama Ekranı*

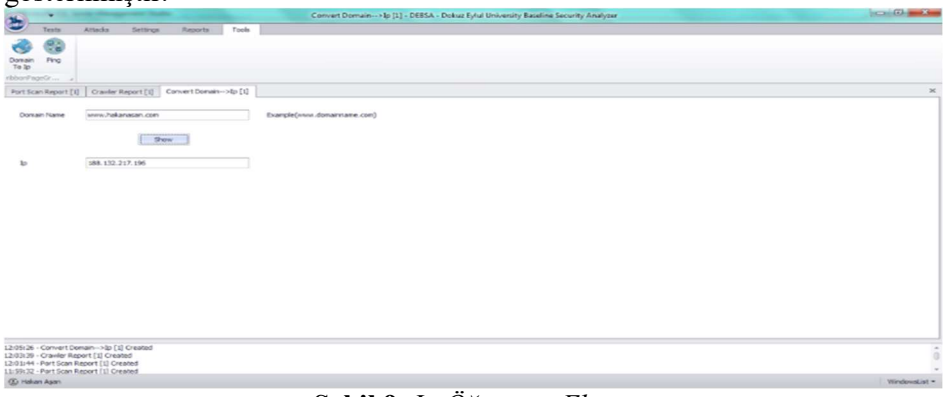
Bu ekrandan ayrıntılı bilgi alınmak istenilen port taraması seçilir. O arama ile ilgili detaylar yeni bir ekranda gösterilir. DEBSA rapor ekranının bir örneği Şekil 8'de gösterilmiştir.



Şekil 8. *Çıktı Ekranı*

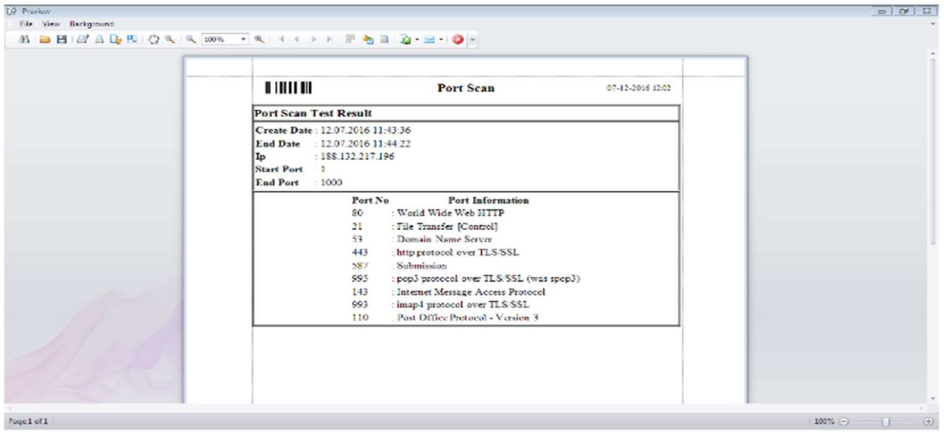
5.1.6. Yardımcı Araçlar Ekranı

DEBSA aynı zamanda kullanıcılara yönelik kolaylaştırıcı bazı fonksiyonları içerisinde barındırmaktadır. Kullanıcılar bu ekranda kendilerine yardımcı olacak işlemleri yapabilirler. Sunucu IP öğrenme ekranı Şekil 9' da gösterilmiştir.



Şekil 9. *Ip Öğrenme Ekranı*

Örneğin kullanıcılar, sunucunun kapalı ya da açık olduğunu denetlemek veya sunucunun aldığı IP yi öğrenmek için bu ekranları kullanabilirler. Aynı zamanda sunucunun durumu ile ilgili bilgi almak için sunucu kontrol ekranı kullanılabilir. Sunucu kontrol ekranı Şekil 10' da gösterilmiştir.

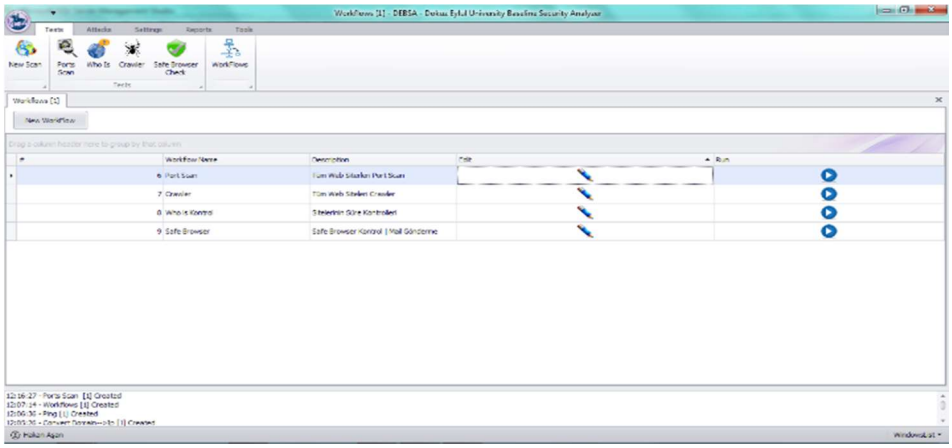


Şekil 10. *Raporlama Ekranı*

5.1.7. Süreç Yönetimi

DEBSA sadece web uygulamalarını test etmek amacıyla oluşturulmuş bir yazılım değildir. Aynı zamanda bu testleri sürekli hale getirerek, belli bir sistem içerisinde sistemlerin test edilmesini sağlamayı hedeflemektedir.

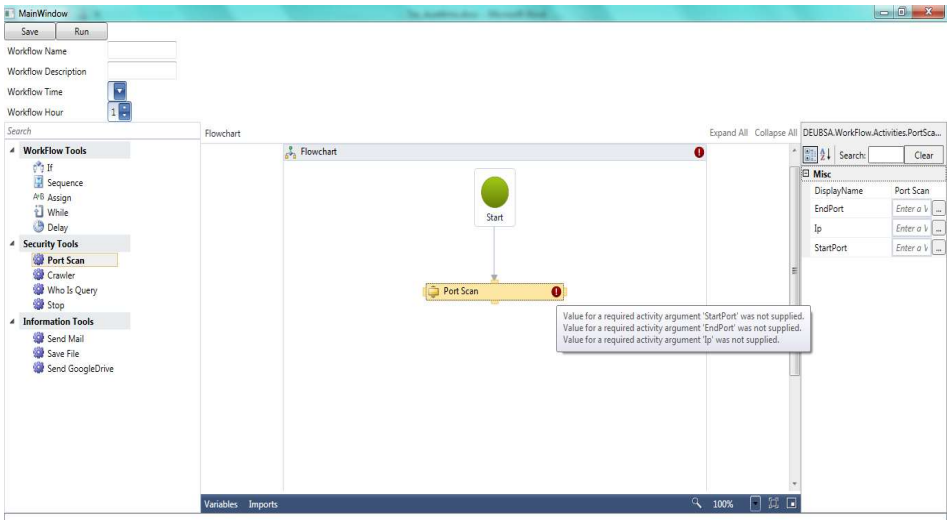
DEBSA' nın en büyük özelliklerinden birisi kullanıcı ve yöneticisi açısından sistemi sürekli takip ve denetim altında tutmasıdır. Bunu gerçekleştirmek için testleri kendi kendine gerçekleştirebilecek ve bununla ilgili bilgilendirmeleri otomatik yapabilecek bir sistemi kendi içinde barındırır. Süreç kayıtlarının listesi Şekil 11' de gösterilmiştir.



Şekil 11. *Süreçler Ekranı*

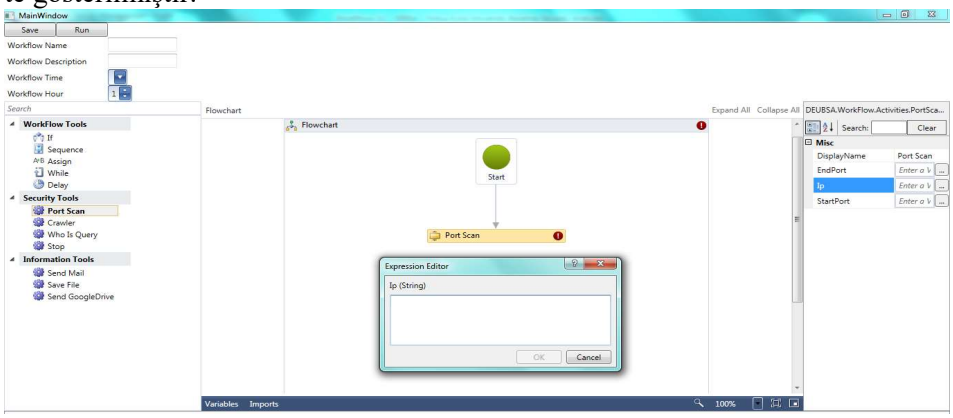
Bu sistem içerisinde DEBSA'yı kullanan kişi bir süreç tasarlayabilir ve bu sürecinin belli periyotlarda tekrarlanmasını sağlayabilir. DEBSA'nın süreç tasarlama kısmı tamamen görsel öğelerden oluşmaktadır ve kullanıcı sürükle bırak işlemi ile süreci kolaylıkla tasarlayabilmektedir.

Süreç tasarım ekranı, kullanıcının ekranın üzerine istediği test nesnesini koymasının ardından yönlendirmelere başlar. Bu yönlendirmelerde gerekli alanlar kullanıcıya direk olarak belirtilir ve kullanıcının bu alanları doldurması istenir. Süreç tasarımının yapıldığı bu ekran Şekil 12 de gösterilmiştir.



Şekil 12. *Süreç Tasarım Ekranı*

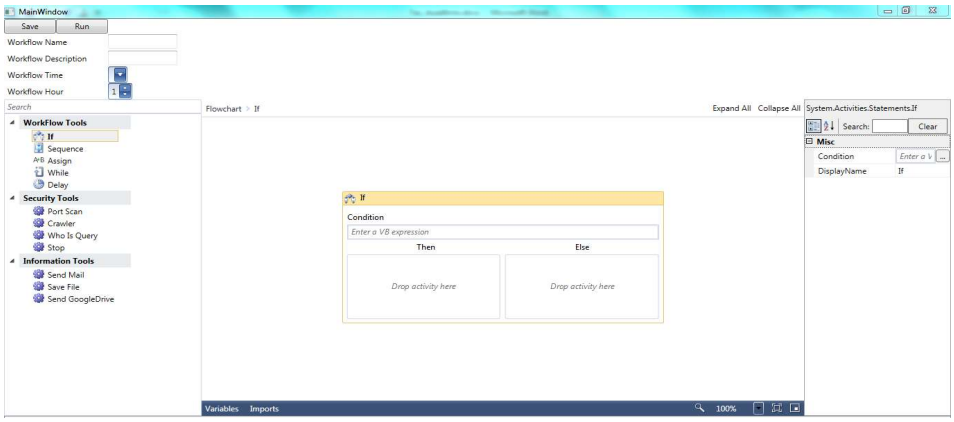
Kullanıcı nesneyi seçtikten sonra sağdan gerekli alanları doldurur. Yazılım gerekli alanın tipini göstererek kullanıcıya yardımcı olur. Bu şekilde doldurulması gereken alanın tipi kullanıcıya bildirilir ve bu doğru şekilde yapılmazsa süreç kaydedilemez. Süreç tasarımının yapıldığı bu ekran Şekilde 13 te gösterilmiştir.



Şekil 13. *Süreç Tasarım Ekranı 2*

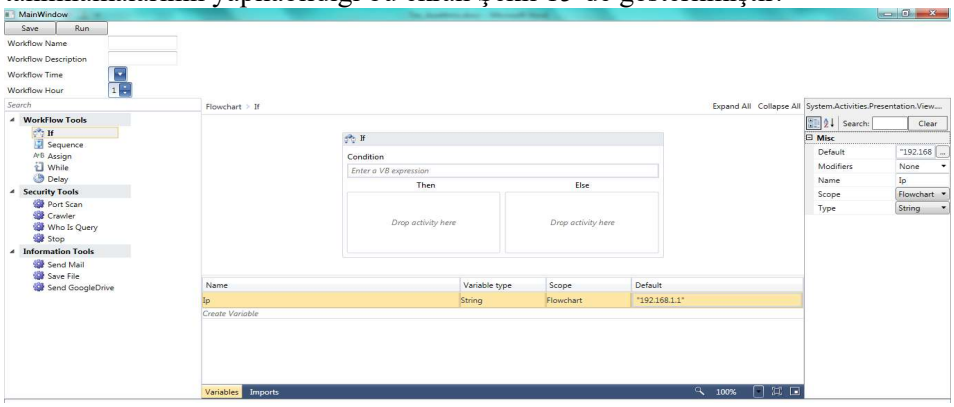
Kullanıcı istemesi halinde yazılım dilinde kullanılan koşul, atama, döngü gibi yönlendirmeleri de kullanabilir. Bunun için yapması gereken süreç tasarım ekranına gerekli nesneyi bırakmaktır. Bu özellik kullanıcının farklı algoritmalar

üretmesini sağlar. Belli koşul ve döngü hareketleri ile süreç istenilen şekilde yönlendirilir. Tasarım ekranı Şekil 14'te gösterilmiştir.



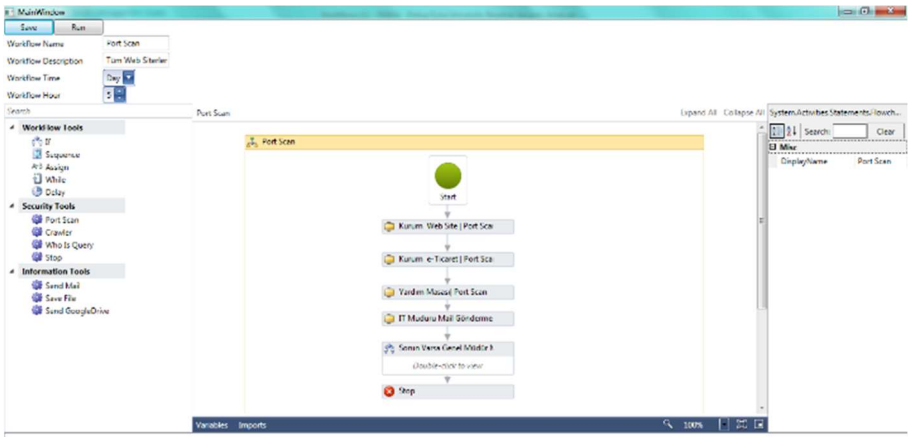
Şekil 14. *Süreç Tasarım Ekranı 3*

Süreç tasarımının alt kısmında bulunan değişken tanımlama kısmında yeni değişkenler tanımlanabilir. Bu sayede süreç içerisinde kullanılmak üzere değişkenler oluşturulması nedeniyle tasarım kolaylaştır. Değişken tanımlamalarının yapılabildiği bu ekran Şekil 15'de gösterilmiştir.



Şekil 15. *Süreç Tasarım Ekranı 4*

Kullanıcı isterse bu süreçleri belli periyotlarda tekrarlanabilir hale getirebilir. Süreç tasarım ekranının üst kısımda süreç ile ilgili bilgiler kaydedilir. Bu bilgiler ile günde, hafta, ayda veya yılda kaç defa çalışacağı bilgisi girilir. Yazılımın çalıştığı sunucuya kurulan servis bu işlemi zamanı geldiğinde tekrarlar. Bu şekilde süreç sürdürülebilir bir hale gelir. Zamanlama ayarlaması yapılan süreç tasarım ekranı Şekil 16'da gösterilmiştir.



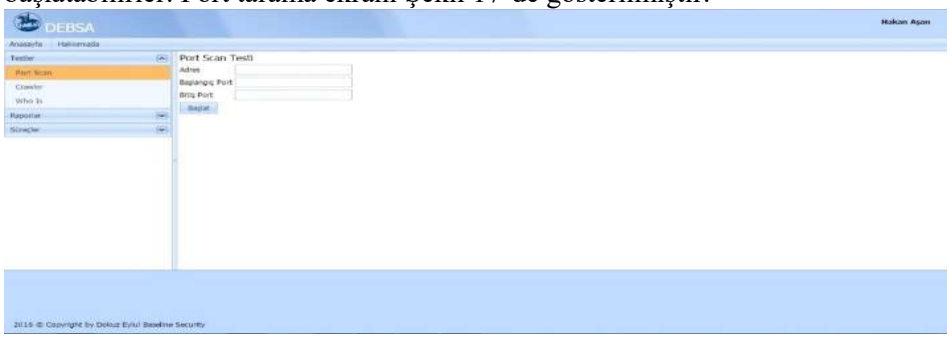
Şekil 16. *Süreç Tasarım Ekranı 5*

5.2. DEBSA Yazılımı – Web

DEBSA yazılımının web kısmı internet ortamının olduğu tüm alanlarda çalışabilir şekilde tasarlanmıştır. Bu web yazılımı ile kullanıcılar raporları görüntüleyebilir, testleri başlatabilir ve süreçleri izleyebilir. Web ve Windows ekranları ortak veritabanı kullanmaları nedeniyle kullanıcılar aynı yetki ve özelliklere sahiptirler.

5.2.1. Test Ekranı (Test Screen)

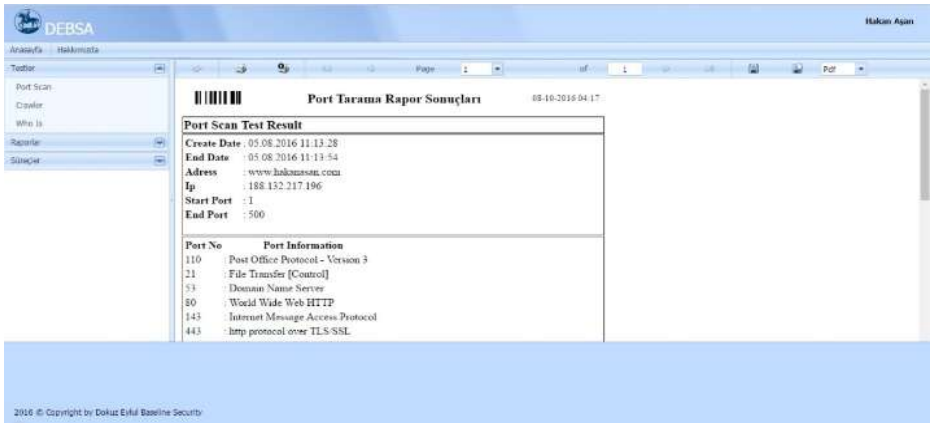
Kullanıcılar web ekranı üzerinden de eğer yetkileri var ise testleri başlatabilirler. Port tarama ekranı Şekil 17'de gösterilmiştir.



Şekil 17. *Test Ekranı*

5.2.2. Rapor Ekranı

DEBSA web uygulaması üzerinden yapılan testlere ait raporlar görüntülenebilir. Şekil 18'de port tarama raporunun bir örneği gösterilmiştir.



Şekil 18. *Rapor Ekranı*

5.2.3. Süreç Ekranı

Bu ekran üzerinden süreçler düzenlenemezler ancak süreçler başlatılabilir ve kontrol edilebilirler. Süreç ekranı Şekil 19'da gösterilmiştir.

Şekil 19. *Süreç Ekranı*

Kullanıcı web üzerinden süreçleri kontrol edebildiği için tabletinden veya mobil cihazından süreç başlatabilir. Bu şekilde her yerden istediği her zamanda süreçleri yönetme ve kontrol etme imkânı sunmaktadır.

Sonuç

İnternetin yaygınlaşması ile web uygulamalarının kullanımının her geçen gün artması, uygulamaların içerisinde yüksek miktarda bilgi bulunmasını sağlamaktadır. Web uygulamalarının içerisinde bulunan bu bilgiler, bazı kimseler tarafından elde edilmeye çalışılmaktadır. Saldırgan ismini verdiğimiz bu tür kötü niyetli kişi veya organizasyonlar, hem web uygulamaları üzerindeki bilgilere erişmek hem de kendilerini tanıtmak için web uygulamalarına saldırılar gerçekleştirmekte ve çok büyük zararlar vermektedirler.

Web uygulama kullanıcıları bireysel ve kurumsal anlamda bu tür saldırılara karşı önlemler almak zorundadır. Bu tür yazılımlar için geliştiriciler

çeşitli önlemler alsalar da bilgisizlik veya dikkatsizlik nedenleriyle web uygulamalarında çeşitli açıklar oluşabilir. Bu açıkların bulunması ve kapatılması çok önemlidir. Bunun farkında olan firmalar veya organizasyonlar bu tür açıkları bulabilmek için bulabilmek için, çeşitli yazılımlar geliştirmişlerdir. Bu yazılımların genel davranış şekli, web sitesine saldırgan gibi yaklaşarak bazı saldırılar yapar ve site üzerindeki açıkları saptar.

Çalışmada incelenen test yazılımları gibi birçok yazılım bulunmaktadır. Bu yazılımların bazıları ticari amaçlarla bazıları ise bazı organizasyonların ürettiği açık kaynak kodlu yazılımlardır. Bu yazılımlar incelenmesi sonucunda yazılımlar genel olarak testleri denemekte bunu kayıt altına alarak, kullanıcıya sunmaktadır. Ancak bu test araçlarının sürekliliği ve kullanıcı bazında farklılaşması yönünde eksikleri bulunmaktadır.

Bu çalışma bu eksiklikleri gözeterek Dokuz Eylul University Baseline Security Analyzer (DEBSA) ismi ile yeni bir yazılım geliştirmeyi amaçlamaktadır. Yazılımın hem güvenlik testleri gerçekleştirilmiş hem de mevcut yazılımlarda eksik görülen kısımlarla ilgili bazı eklentiler yapılmıştır. DEBSA yazılımı, iki kısımdan oluşmaktadır. Birinci kısım tasarım kısmı olup Windows platformu üzerinde çalışmaktadır. Bu kısımda kullanıcı, program ayarları yapılmaktadır. Süreç tasarım ekranı da bu kısımda yapılmaktadır. İkinci kısım web üzerinde çalışmaktadır. Bu kısımda kullanıcı herhangi bir noktadan süreçleri ve buna bağlı raporları görüntüleyebilmektedir.

DEBSA içerisinde bulunan süreç yönetimi sayesinde ise istenilen testler akış diyagramı şeklinde çizilebilmektedir. Yazılımın istenilen zamanlarda çalışarak kullanıcıya otomatik olarak bilgi vermesi sağlanır. Bu şekilde kullanıcı testleri tekrar tekrar veri girişi yapmadan, kendine gelen maillerle takip edebilir. DEBSA yazılımının bir diğer önemli yeniliği de farklı kullanıcı profillerinin oluşturulabilmesidir. Kullanıcılar sadece kendileri ile ilgili bölümleri görebilir ve üzerinde işlem yapabilir. Bu da yazılım içinde gizliliğin olmasını ve kullanıcılar arasında izolasyonun olmasını sağlamaktadır. Diğer taraftan yönetici tarafından da yapılan işlemler kişi bazında izlenebilir olmaktadır.

Bu çalışmadaki temel amaç web uygulamalarını test edecek bir yazılım geliştirmektir. Aynı zamanda yapılan çalışma yöneticiye karar vermede faydalı olacak bilgiyi oluşturmanın çok önemli olduğu düşünülerek hazırlanmıştır. Web uygulamalarını test eden bu yazılım tasarlanırken hem mevcut testleri gerçekleştirebilmesi hem de yöneticilere bir karar destek sistemi oluşturacak yapıda olmasına özen gösterilmiştir. Bu nedenden sadece web uygulamalarını test edecek bir yazılım geliştirmek yerine, bu işlemi süreç etkinliği kapsamında ele alıp testleri sürekli hale getirecek ve yöneticiyi sürekli bilgi sağlayacak bir yapı kurmak istenmiştir.

Gelecekte yapılacak benzer çalışmalarda, web uygulamalarını test eden araç olmanın yanı sıra, testlerin sürekliliği ile ilgili yenilikler getirilmesi üzerinde durulabilir. DEBSA yazılımı süreç tasarımı kısmında farklı süreç elemanları geliştirilerek çizilebilecek etkin akışlar yaratılabilir. Ayrıca web uygulamalarını

farklı yönlerden test eden algoritmalar geliştirilebilir veya mevcut algoritmalar üzerinde iyileştirmeler yapılabilir.

Kaynaklar

Acunetix, 2019, *Acunetix Web Application Vulnerability Report 2019*, https://cdn2.hubspot.net/hubfs/4595665/Acunetix_web_application_vulnerability_report_2019.pdf, Web Erişim Tarihi: 17.03.2020

BBC, 2019, Equifax to pay up to $700m to settle data breach, https://www.bbc.com/news/technology-49070596, Web Erişim Tarihi: 04.03.2020

Calder, A. ve Watkins, S. (2008), *IT Governance A Manager's Guide to Data Security and ISO27001/ISO 27002*, 4th Edition. London: Kogan Page Ltd.

Canbek, G. ve Sağıroğlu, Ş. (2006), *Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme*. Politeknik Dergisi. 9(3): 165-174.

Meyer D., (2018), *A Cyber Gang Stole $1 Billion by Hacking Banks and ATMs. Now Police Say They've Caught the Mastermind,* https://fortune.com/2018/03/26/carbanak-europol-arrest-spain-malware-banks/, Web Erişim Tarihi: 29.03.2020

Fruhlinger J., (2020), *Marriott Hacking Exposes Data of Up to 500 Million Guests*, https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html, Web Erişim Tarihi: 19.05.2020

Fussell, R.S. (2005), *Protecting Information Security Availability via Self-adapting Intelligent Agents.* Military Communications Conference, IEEE.

Gonzales, J. J. ve Sawicka, A. (2002), *A Framework for Human Factors in Information Security. International Conference On Information Security*. Rio de Janerio. ss. 449 – 454.

Gordeychik S. (2016), *Web Application Security Statistics* (http://www.webappsec.org/projects/statistics, Erişim Tarihi: 11.05.2016)

Gutzmer, I., (2017), *Equifax Announces Cybersecurity Incident Involving Consumer Information,* https://investor.equifax.com/news-and-events/press-releases/2017/09-07-2017-213000628, Web Erişim Tarihi: 06.04.2020

ISO/IEC 17799:2005, (2005), *Information Technology - Code of Practice Security Mnagemant,ISO Copyright Office*, Switzerland.

IBM Security, (2019), *Veri İhlali Maliyeti Raporu*, https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf, Web Erişim Tarihi: 08.05.2020

Inamdar N., (2018), *15,000 transactions in 7 hrs: Cosmos Bank's server hacked, Rs 94 cr moved to Hong Kong*, https://www.hindustantimes.com/india-news/15-000-transactions-in-7-hrs-cosmos-bank-s-server-hacked-rs-94-

cr-moved-to-hong-kong/story-wazUXZs3LRhcbPLg7LYx5O.html, Web Erişim Tarihi: 24.04.2020

Kajava J., Anttila J., Varonen R., Savola R., ve Roning J. (2006*), Information Security Standards and Global Business*. IEEE. pp. 2091-2095.

Lehtinen, R. (2006), *Computer Security Basics*, 2nd Edition. ABD: O'Reillly Publishing.

Lau L., (2018), *Cybercrime 'pandemic' may have cost the world $600 billion last year*, https://www.cnbc.com/2018/02/22/cybercrime-pandemic-may-have-cost-the-world-600-billion-last-year.html#:~:text=Cybercrime%20'pandemic'%20may%20have%20cost%20the%20world%20%24600%20billion%20last%20year,-Published%20Thu%2C%20Feb&text=The%20global%20cost%20of%20cybercrime,according%20to%20a%20new%20report., Web Erişim Tarihi: 18.01.2020

Negash, S., Ryan, T. ve Igbaria, M. (2003), *Quality and Effectiveness In Web-Based Customer Support Systems. Journal of Information and Management*. 40: 757-768.

McMillan, R., (2016), *FriendFinder Investigates Report of Breached Accounts*, https://www.wsj.com/articles/friendfinder-investigates-report-of-breached-accounts-1479160660, Web Erişim Tarihi: 02.04.2020

Moore S., Keen E., Gartner (2019), *Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019.* https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019, Web Erişim Tarihi: 04.04.2020

OWASP. (2018), *OWASP Top 10.* 2017. (https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf).

Önel, D. ve Dinçkan, A. (2007), *Bilgi Güvenliği Yönetim Sistemi Kurumu*, Ulusal Bilgi Güvenliği Kapısı.

Osborne C., (2020), *Most companies take over six months to detect data breaches,* https://www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches/, Web Erişim Tarihi: 02.01.2020

Özavcı, F. (2002), *Bilgi Güvenliği Temel Kavramlar.* http://www.siyahsapka.com.

Perlroth N., (2020), *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*, https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html#:~:text=It%20was%20the%20biggest%20known%20breach%20of%20a%20company's%20computer%20network.&text=Verizon%20Communications%2C%20which%20acquired%20Yahoo,billion%20of%20Yahoo's%20user%20accounts., Web Erişim Tarihi: 08.03.2020

Pfleeger, C. P. (2007), *Security in Computing*, 4th edition. Prentice Hall, USA.

Risk Based Security, (2020), *2019 Year End Report*, https://pages.riskbasedsecurity.com/2019-year-end-data-breach-quickview-report

Roberts J. J. ve Lashinsky A., (2017), *Hacked: How Business Is Fighting Back Against the Explosion in Cybercrime*, https://fortune.com/2017/06/22/cybersecurity-business-fights-back/, Web Erişim Tarihi: 18.03.2020

Saatçi, A. (2002), *Bilgisayar İşletim Sistemleri*, 2. Baskı. Bıçaklar Kitapevi Yayınları, Ankara.

Smith, S., (2019). *Cybercrıme Will Cost Busınesses Over $2 Trillion By 2019,* https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion-by-2019, Web Erişim Tarihi: 08.03.2020

Sobers, R., (2020), *64% of Americans Don't Know What to Do After a Data Breach — Do You?*, https://www.varonis.com/blog/data-breach-literacy-survey/, Web Erişim Tarihi: 01.5.2020

Steve, G.W. (2008), *An Introduction to Information Security and ISO/IEC 27001*. IT Governance Publishing.

TSE. TS ISO/IEC 27001. (2006), *Türk Standartları Enstitüsü*, Ankara, Türkiye.

Tudor, J.K. (2001), *Information Security Architecture*. CRC Press, Florida.

Türkiye Bilişim Derneği. (2006), *Bilişim Sistemleri Güvenliği El Kitabı*.

UNCTAD, (2005), *Information Economy Report 2005*. Geneva: UNCTAD.

Under Armour, (2018), *Under Armour Notifies MyFitnessPal Users Of Data Security Issue*, https://www.prnewswire.com/news-releases/under-armour-notifies-myfitnesspal-users-of-data-security-issue-300621986.html, Web Erişim Tarihi: 07.06.2020