



T.C.
SELÇUK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

TÜRKİYE'DE EN ÇOK ZİYARET EDİLEN BAZI WEB SİTELERİN GÜVENLİK DEĞERLENDİRMESİ

Atakan DAŞDEMİR

YÜKSEK LİSANS TEZİ

Bilişim Teknolojileri Mühendisliği Anabilim Dalı

Mayıs-2018
KONYA
Her Hakkı Saklıdır

ÖZET

YÜKSEK LİSANS TEZİ

TÜRKİYE'DE EN ÇOK ZİYARET EDİLEN BAZI WEB SİTELERİN GÜVENLİK DEĞERLENDİRMESİ

Atakan DAŞDEMİR

Selçuk Üniversitesi Fen Bilimleri Enstitüsü
Bilişim Teknolojileri Mühendisliği Anabilim Dalı

Danışman: Dr. Öğr. Üyesi Humar KAHRAMANLI
Öğr.Gör.Dr. Mustafa Nevzat ÖRNEK

2018, 72 Sayfa

Jüri
Dr.Öğr.Üyesi Humar KAHRAMANLI
Dr.Öğr.Üyesi Ayşe ELDEM
Dr.Öğr.Üyesi Selahattin ALAN

Günümüzde kurumlar işleyişlerini, gelişimlerini devam ettirmek, bireyler günlük yaşamlarını daha rahat sürdürmek için bilgi ve teknolojik araçlara ihtiyaç duymaktadır. Bu teknolojik araçların merkezinde ve büyük bir veri havuzu olan İnternet'e erişim her geçen gün vazgeçilmez olmaktadır. Web ile internet üzerindeki uygulamalar zaman ve mekân gözetmeksizin, basit ve hızlı erişimi ile günlük yaşamı kolaylaştırmıştır. Geniş kullanım alanı ve dünya nüfusunun yarısından fazla kullanıcı erişimi ile Web uygulamaları kötü niyetli kullanıcılar için popüler bir hedef haline gelmiş, güvenlik riski artmıştır. Bu çalışmada bilgi güvenliği ve Web güvenliği ile ilgili tehdit unsurlardan bahsedilmiş, bilgi ve Web güvenliği için vazgeçilmez olan ve sistem veya uygulamadaki mevcut riskleri tespit için gerekli olan sızma testlerine değinilmiştir.

Symantec firması 2016 yılında uluslararası çapta yaptığı Web güvenliği analizi çalışmasında incelediği sitelerin % 76'sında en az bir zafiyet bulmuştur. Bu sonuç Web uygulamaları güvenliğindeki vahim durumu göstermek için yeterlidir. Bu çalışmada ülkemizdeki Web sitelerinin genelinin durumu hakkında bir güvenlik değerlendirmesi yapmak düşüncesiyle her gün binlerce ziyaretçisi olan beş farklı kategoride en çok ziyaret edilen sitelerden 60 tanesi belirlenmiştir. İnceleme için haber, e-ticaret, devlet, üniversite ve diğer kategorilerinde güvenlik altyapısının sağlam olduğu düşünülen büyük siteler tercih edilmiştir. Bu sitelerin halka açık kısmında ne tür bilgilerin toplanabileceği, kullandıkları teknolojiler ve altyapısıyla ilgili hangi bilgilerin bulunabileceği araştırılmıştır. Araştırma sonucunda incelenen sitelerin %62'sinin kullandıkları işletim sistemi, %87'sinin kullandıkları Web sunucu bilgileri elde edilebilmiştir. Yapılan zafiyet tarama testleri ile zafiyet haritası çıkartılmış, en çok tespit edilen zafiyetler ile ilgili bilgi verilmiştir. Bu zafiyetleri ortadan kaldıracak yöntemlerden bahsedilmiştir. Tespit edilen tehditlere bakıldığında tüm sitelerin en az bir orta dereceli zafiyet içerdiği tespit edilmiş olup başlık probleminin genel bir zafiyet olduğu bulunmuştur. Ayrıca incelenen sitelerin kullanıcı için tehdit içerip içermediği tespit edilmeye çalışılmıştır.

Bilgi toplama veya saldırı geliştirilmiş araçlarla daha kolay hale gelmiştir. Düşük seviyedeki kullanıcılar bile saldırı araçlarını kullanarak saldırı gerçekleştirebilmektedirler. Çalışmada herkes tarafından kolay erişilebilen bu araçlar kullanılarak bir güvenlik değerlendirilmesi hedeflenmiştir.

Not: Yapılan çalışmada ilgili site sahiplerinden izin almayı gerektirecek bir faaliyet yürütülmemiş olup yapılanlar, sıradan kullanıcıların herhangi bir sitenin halka açık kısmında yapabilecekleri ile sınırlıdır.

Anahtar Kelimeler: Bilgi güvenliği, Sızma testleri, Web güvenliği, Zafiyet analizi.

ABSTRACT

MS THESIS

EVALUATION OF SOME MOST VISITED WEB SITES IN TURKEY IN ASPECTS OF SECURITY

Atakan DAŞDEMİR

THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCEOF SELÇUK UNIVERSITY
THE DEGREE OF MASTER OF SCIENCE INFORMATION TECHNOLOGY ENGINEERING

Advisor: Asst.Prof.Dr. Humar KAHRAMANLI
Dr. Mustafa Nevzat ÖRNEK

2018,72 Pages

Jury
Asst.Prof.Dr. Humar KAHRAMANLI
Asst.Prof.Dr. Ayşe ELDEM
Asst.Prof.Dr. Selahattin ALAN

Today, institutions to maintain their functioning, their development, and individual to make the daily life more comfortable need information and technological tools. Access to the Internet, which is at the center of these technological tools and as a large data pool, is becoming more and more indispensable day by day. With the World Wide Web (briefly Web), applications on the internet have facilitated daily life with simple and fast access regardless of time and place. With widespread use and over-user access from half of the world's population, Web applications have become a popular destination for malicious users and the security risk has increased. In this study, threats related to information security and Web security are mentioned, and penetration tests are described which are indispensable for information and Web security and are necessary to detect existing risks in the system or application.

The Symantec Company found at least one vulnerability in 76% of the sites reviewed in its internationally conducted Web security analysis study in 2016. This result is sufficient to demonstrate the serious situation in the security of Web applications. In this study, 60 of the most visited sites were identified in five different categories to consider a safety assessment of the general situation of the Web sites in our country. For the review, large sites in news sites, e-commerce, government, universities and other categories have been selected that are thought to have strong security infrastructure. In the public part of these sites, what kinds of information can be collected, and what information about the technologies and infrastructure they use can be found have been investigated. As a result of the research, 62% of the reviewed sites using operating system information and 87% of the reviewed sites using web server information were obtained. With the vulnerability screening tests, weakness map revealed and information about the most identified weaknesses was given. Methods to eliminate these weaknesses have been mentioned.

When look at all the detected threats, has been found that all sites have at least one medium weakness and it is found that the title problem is a general weakness. In addition, surveyed sites examined to determine whether it contains a threat to the user or not.

Information gathering or attack has become easier with improved tools. Even low-level users can attack using attack tools. In this study, a security assessment was aimed at using these tools, which are easily accessible for everyone.

Note: No activity has been conducted in this study that will require permission from the relevant site owners and it is limited to what ordinary users can do in the public domain of any site.

Key Words: Information security, Penetration testing, Web security, Weakness analysis.

ÖNSÖZ

Bu çalışmanın gerçekleştirilmesinde, desteğini her zaman hissettiğim, eğitim hayatıma önemli katkıları olan saygıdeğer hocalarım; Dr. Öğr. Üyesi Humar KAHRAMANLI ve Dr. Mustafa Nevzat ÖRNEK'e, eğitim hayatım süresince tüm zorlukları benimle göğüsleyen aileme sonsuz teşekkürlerimi sunarım.

Atakan DAŞDEMİR
KONYA-2018

İÇİNDEKİLER

ÖZET iv

ABSTRACT vi

ÖNSÖZ viii

İÇİNDEKİLER ix

SİMGELER VE KISALTMALAR xi

1. GİRİŞ 1

1.1. Bilgi Güvenliği 3
1.2. Web Güvenliği 7
1.2.1. OWASP 8
1.2.1. NIST 10

2. KAYNAK ARAŞTIRMASI 13

3. MATERYAL VE YÖNTEM 15

3.1. Materyal 15
3.1.1.Web Platformu ve Uygulama Yapısı 15
3.1.2. Sızma Testleri 21
3.1.2.1. Bilgi Toplama 22
3.1.2.2. Zafiyet Taraması ve Analiz 23
3.1.2.3. Sömürü 23
3.1.2.3.1. XSS 23
3.1.2.3.2. CSRF 25
3.1.2.3.3.SQL Enjeksiyonu 26
3.1.2.4. Erişimin Devam Ettirilmesi 27
3.1.2.5. Raporlama 28
3.1.3. Kullanılan Yazılımlar 28
3.1.3.1. Kali Linux 28
3.1.3.2. Acunetix 28
3.1.3.3. Nessus 29
3.1.3.4. Nikto 30
3.1.3.5. Paros 30
3.2. Uygulamada İzlenecek Yöntem 31
3.2.1. Planlama 32
3.2.2. Bilgi Toplama 32
3.2.3. Zafiyet Taraması 33
3.2.4. Zararlı Yazılım Tespiti 34

4. ARAŞTIRMA SONUÇLARI VE TARTIŞMA 35

4.1. İncelenen Sitelerin Web Uygulama Yapısı İle İlgili Sonuçlar 35
4.2. İncelenen Sitelerin Zafiyet Açısından Sonuçları 38

4.2.1. Risk Derecelerine Göre Toplam Zafiyet 38
4.2.2. Grup Bazında Zafiyet Analizi 39
4.2.3. Karşılaşılan Zafiyetler ve Önlemler 41

4.3.İncelenen Sitelerin Zararlı Yazılım Açısından Değerlendirilmesi 43

5. SONUÇLAR VE ÖNERİLER 44

5.1 Sonuçlar 44
5.2 Öneriler 44

KAYNAKLAR 46

ÖZGEÇMİŞ 47

SİMGELER VE KISALTMALAR

Kısaltmalar

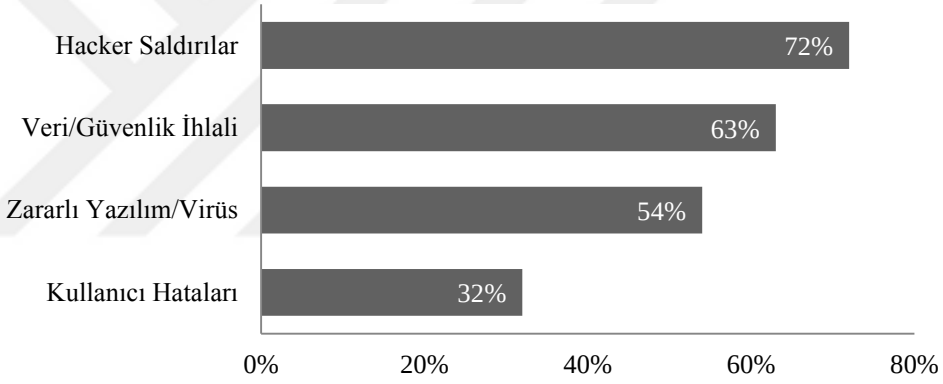
API	:Uygulama programlama arayüzü (Application Programming Interface)
ARPANET	:Gelişmiş araştırma projeleri dairesi ağı (Advanced Research Projects Agency Network)
BGYS	:Bilgi güvenliği yönetim sistemi
CAPTCHA	:İnsan ve bilgisayar ayrımı amaçlı tam otomatik genel Turing testi (Completely Automated Public Turing test to tell Computers and Humans Apart)
COBIT	:Bilgi ve ilgili teknolojiler için kontrol hedefleri (Information Systems Auditand Control Association)
CSRF	:Siteler arası istek sahteciliği (Cross-Site Request Forgery)
CSS	: Basamaklı Stil Şablonları (Cascading Style Sheets)
DoS	:Hizmet Aksattırma (Denial of Service)
DDOS	:Dağıtık hizmet dışı bırakma (Distributed Denial of Service attack)
DNS	:Alan ismi sistemi (Domain Name System)
DOM	:Belge nesne modeli (Document Object Model)
FTP	:Dosya transfer protokolü (File Transfer Protocol)
GWT	:Google Web aracı (Google Web Toolkit)
HTML	:Hipermetin İşaret Dili (Hypertext Markup Language,)
HTTP	:Hiper metin transfer protokolü (Hyper-Text Transfer Protocol)
HTTPS	:Güvenli hiper metin transfer protokolü (Secure Hypertext Transfer Protocol)
IDS	:Saldırı tespit sistemleri (Intrusion Detection Systems)
IEEE	:Elektrik ve Elektronik Mühendisleri Enstitüsü (The Institute of Electrical and Electronics Engineers)
IP	:İnternet protokolü
ISO	:Uluslararası Standartlar Organizasyonu (International Organization for Standardization)
IoT	:Nesnelerin interneti (Internet of Things)
LDAP	:Basit dizin erişim protokolü (Lightweight Directory Access Protocol)
MAC	:Ortam erişim yönetimi (Media Access Control)
NIST	:Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology)
NTT	:Uluslararsı bilişim firması (Nippon Telegraphand Telephone Corporation)

OWASP	:Açık Kaynak Web Uygulama Güvenliği Projesi (The Open Web Application Security Project)
PHP	:Hipermetin Ön İşlemci Betik Dili (Hypertext Preprocessor)
POP3	:Postane protokolü (Post Office Protocol)
RPC	:Uzaktan işlem çağrısı (Remote Procedure Call)
PUKÖ	:Planla – Uygula – Kontrol et – Önlem al.
SMTP	:Basit posta transfer protokolü (Simple Mail Transfer Protocol)
SNMP	:Basit ağ yönetim protokolü (Simple Network Management Protocol)
SOAP	:Basit Nesne Erişim Protokolü (Simple Object Access Protocol)
SQL	:Yapılandırılmış sorgu dili (Structured Query Language)
SSL	:Güvenli giriş katmanı (Secure Sockets Layer)
SYMANTEC	:Siber güvenlik firması
TCP/IP	:İletim kontrol protokolü/İnternet protokolü (Transmission Control Protocol/Internet Protocol)
TLS	:Taşıma Güvenlik Katmanı (Transport Layer Security)
TÜİK	:Türkiye İstatistik Kurumu
UDDI	:Evrensel Tanım, Keşif ve Entegrasyon (Universal Description, Discovery and Integration)
URL	:Tek düzen kaynak bulucu (Uniform Resource Locator)
WAF	:Web Uygulama Güvenlik Duvarı (Web Application Firewall)
WSDL	:Web Servis Dili Açıklaması (Web Service Language Description)
XLM	:Genişletilebilir İşaretleme Dili (eXtensible Markum Language)
XSS	:Çapraz betik çalıştırma (Cross site scripting)

*Metin içinde geçen firmalara ait logo ve marka ilgili firmaların tescilli markasıdır.

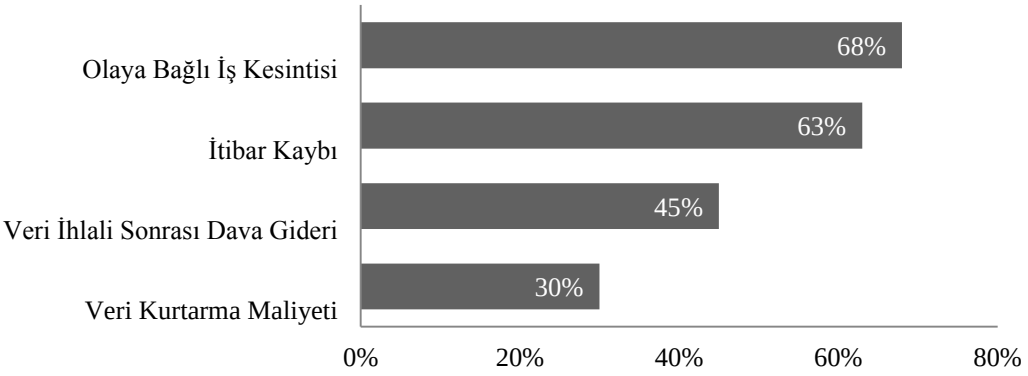
1. GİRİŞ

Yaşadığımız bilgi çağında bilgi ne kadar önemli ise onun gizliliği, bütünlüğü ve erişe bilirliği yani güvenliği de bir o kadar önemlidir. Akıllı evler, arabalar, cihazlar, uygulamalar hayatımızda artan bir şekilde yer almaya devam etmekte, teknolojik gelişmeler insan yaşamıyla daha çok bütünleşik hale gelmektedir. Günümüzde dünya nüfusunun yarısından fazlası büyüklükte kullanıcıya sahip akıllı telefon ve nesnelerin interneti (IoT) ile bilgi güvenliğin önemi gün geçtikçe artmakta, buna yönelik tehditler ile daha sık karşılaşır hale gelinmektedir. Bilgi güvenliğinin önemi uluslararası çapta büyük firmaların bu konuyla ilgilenmesini gerekli kılmıştır. Bu firmalardan birisi olan ve dünya genelinde özellikle kurumsal firmalar ile çalışma yapan Allianz Global Corporate & Specialty firması destek verdiği firmalar arasında her yıl bilgi güvenliği araştırması yapmaktadır. Bu firmanın 2016 yılı güvenlik raporuna göre kurumsal firmalar için bilgi güvenliği tehditleri Şekil 1.1'de verilmiştir.



Şekil 1.1. 2016 yılında karşılaşılan bilgi güvenliği olayları (Anonim, 2017-9)

Şekil 1.1'de görüldüğü gibi araştırmaya katılan kurumsal firmaların %72 si dış tehditler başlığı altındaki hacker saldırıları ile karşı karşıya kaldığını bildirmiştir. Oluşan bilgi güvenliği olayları kişisel maddi ve manevi zararlara neden olabildiği gibi ulusal ekonomiyi de olumsuz etkilemektedir. Allianz Global Corporate & Specialty firmasının 2016 yılı aynı güvenlik raporuna göre bilgi güvenliği olayları sonucu meydana gelen maddi kayıplar ve oranları Şekil 1.2' de gösterilmiştir.

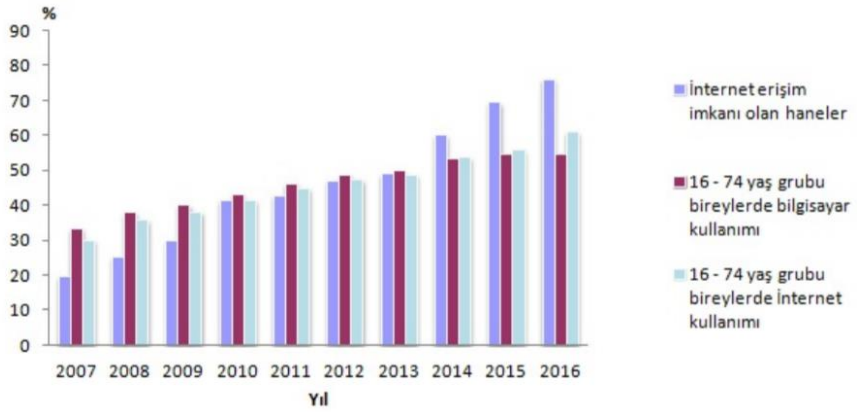


Şekil 1.2. Bilgi Güvenliği olayları sonucu meydana gelen ekonomik kayıpların dağılımı (Anonim, 2017-9)

Şekil 1.2'de görüldüğü gibi özellikle kurumsal firmalar için başarıyı destekleyici unsurlardan biri olan işin sürekliliği, bilgi güvenliği olayları sonucunda sekteye uğramaktadır. Araştırmaya katılanların %68'i bilgi güvenliği ihlalleri sonucu iş kesintisi yaşadığını yani firma faaliyetlerinin yapılamadığını belirtmiştir.

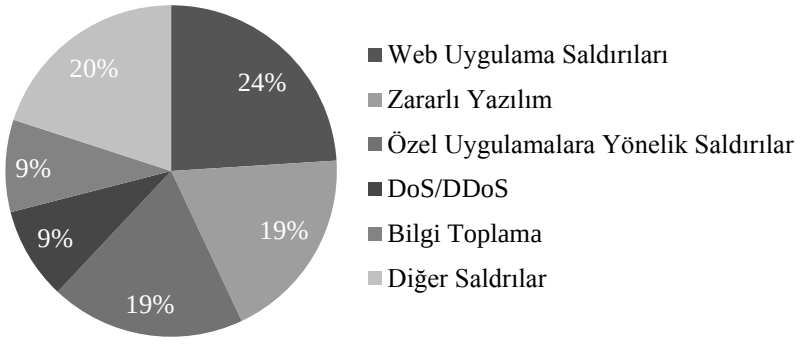
Bilgi güvenliği tehditleri kurumsal firmaların yanı sıra kişisel kullanıcıları da tehdit etmektedir. İnternet kullanan cihazların gün geçtikçe artmasıyla özellikle kişisel bilgi güvenliğine yönelik tehditler hem çeşitlilik kazanmakta hem de sayıca çoğalmaktadır. Symantec firması tarafından yayınlanan Norton Cyber Security Insights raporu küresel bazda 2016 yılında 594 milyon kişinin internet istismarı ile kurban durumuna düştüğünü ve 158 milyar dolarlık maddi kayıp meydana geldiğini belirtmektedir.

Bilgi güvenliği ihlalleri sonucu oluşan maddi ve manevi kayıpların büyük kısmını Web tabanlı saldırılar oluşturmaktadır. Bilgi güvenliğinde önemli bir yer tutmakta olan Web uygulamaları internet sayesinde zaman ve mekândan bağımsız kolay erişimi ile oldukça fazla kullanıcıya sahiptir. Türkiye İstatistik Kurumunun 2017 yılında yayınladığı "Hanehalkı Bilişim Teknolojileri Kullanım Araştırması" raporuna göre internet kullanıcı sayısı Şekil 1.3'te gösterilmiştir.



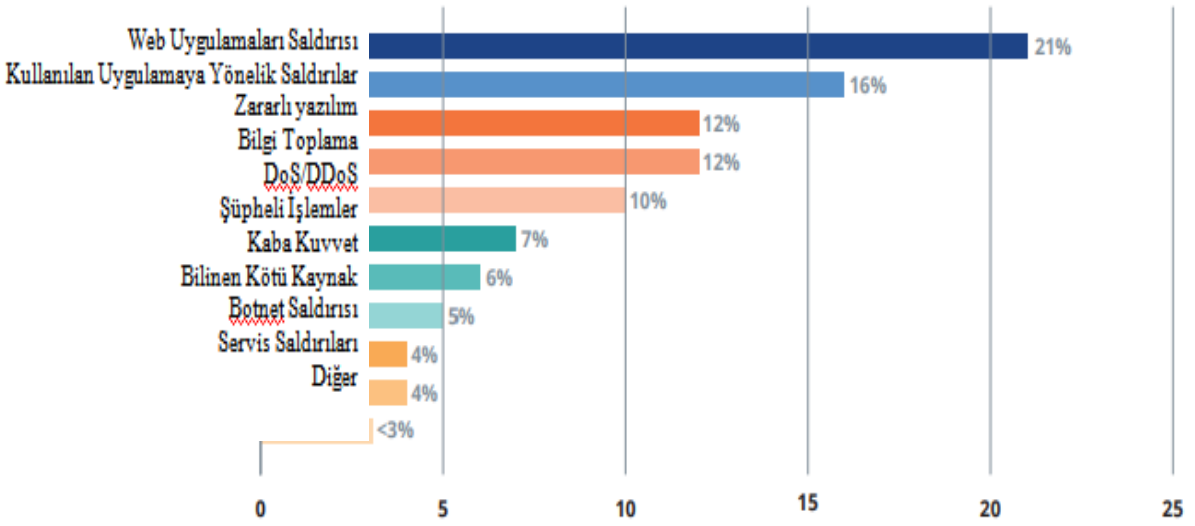
Şekil 1.3. Hanehalkı bilişim teknolojileri kullanımı (Anonim, 2017-10)

Şekil 1.3'de görüldüğü gibi bilgisayar ve internet kullanımı 2017 yılında 16-74 yaş grubundaki bireylerde sırasıyla %56,6 ve %66,8 oranındadır. Bu oranlar 2016 yılında sırasıyla %54,9 ve %61,2 idi. Yine BTK 2017 verilerine göre bilgisayar ve internet kullanım oranları 16-74 yaş grubundaki erkeklerde %65,7 ve %75,1 iken, kadınlarda %47,7 ve %58,7 dir. Hanehalkı bilişim teknolojileri kullanım araştırması sonuçlarına göre 2017 yılı Nisan ayında hanelerin %80,7'si evden internete erişim imkânına sahip olmuştur. Bu oran 2016 yılının aynı ayında %76,3 idi. Geniş bant internet erişim imkânına sahip hanelerin oranı 2017 yılı Nisan ayında %78,3 tür. Bu oran önceki yıl %73,1 idi. Geniş bant internet erişimde hanelerin %40'ı sabit geniş bant bağlantı (ADSL, kablolu İnternet, fiber vb.) ile internete erişim sağlarken, %72,4'ü mobil bağlantı ile erişim sağlamıştır. Kullanıcı sayısının bu büyüklüğü Web uygulamalarında bilgi güvenliğinin önemini göstermektedir. Ülkemizde olduğu gibi dünyada da milyonlarca ziyaretçisi olan bu uygulamalar hassas veriler içerebilmekte, herkes tarafından erişim olanağı ile saldırılara daha çok maruz kalabilmektedir. Symantec 2017 verilerine göre dünyada 6,4 milyar cihaz internete erişmekte ve bu sayı her geçen gün artmaya devam etmektedir. Aynı raporda 2016 yılında her gün 229.000 Web saldırısı gerçekleştiği ve taranan Web sitelerinin %76'sının zafiyet içerdiği belirtilmiştir. NTT Security firmasının 2017 raporuna göre 2016 yılının ikinci çeyreğindeki bilgi güvenliği olayları Şekil 1.4' de gösterilmiştir.



Şekil 1.4. 2016 yılının ikinci çeyreğindeki bilgi güvenliği olayları (Anonim, 2017-3)

Şekil 1.4'de görüldüğü gibi kamuoyuna açık olması ve mobil cihazlarla bile kolay erişilebilir olması sebebiyle Web uygulamalarına yönelik saldırılar bilgi güvenliği olaylarında ilk sırayı almaktadır. Bunu gösteren bir diğer grafik Şekil 1.5' de verilmiştir.



Şekil 1.5. 2017 yılı ikinci çeyreğinde meydana gelen bilgi güvenliği olayları (Anonim, 2017-3)

NTT Security firmasına göre 2016 yılının ikinci çeyreğinde olduğu gibi 2017 yılının ikinci çeyreğinde de Web uygulamalarına yönelik saldırılar %21 ile bilgi güvenliği olaylarında ilk sırayı almıştır.

Çalışmanın konusu temel olarak Web güvenliği dolayısı ile bilgi güvenliği olduğundan bu kavramlardan biraz daha kapsamlı bahsetmek gerekir.

1.1. Bilgi Güvenliği

1969 yılında ARPANET'in kurulumundan önce daha çok fiziksel anlamda önlemler olarak algılanan bilgi güvenliği kavramının, ağ teknolojilerinin gelişmesi, farklı platformlardaki cihazların ortaya çıkması, World Wide Web kısaca Web'in 1989 yılında The European Particle Physics Laboratory'de Tim Berners-Lee ve Robert Cailliau tarafından geliştirilmesiyle gün geçtikçe yaygınlaşmış ve kapsama alanı genişlemiştir.

Bilgi güvenliği denilince akla üç temel öğe olan gizlilik, bütünlük, erişilebilirlik gelir. Bilgiye olabilecek yetkisiz erişimlerin engellenmesine gizlilik, yetkili erişim sonucunda esas bilginin korunmasına bütünlük, ihtiyaç halinde kolay ulaşılabilir olmasına erişilebilirlik denir. Bunlara sonradan eklenen hesap verebilirlik, erişim denetimi, güvenilirlik ve emniyet bilgi güvenliğini destekleyen unsurlardır. Bilişim çağının en önemli problemlerinden olan bilgi güvenliği elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür (Canbek ve Sağiroğlu, 2006).

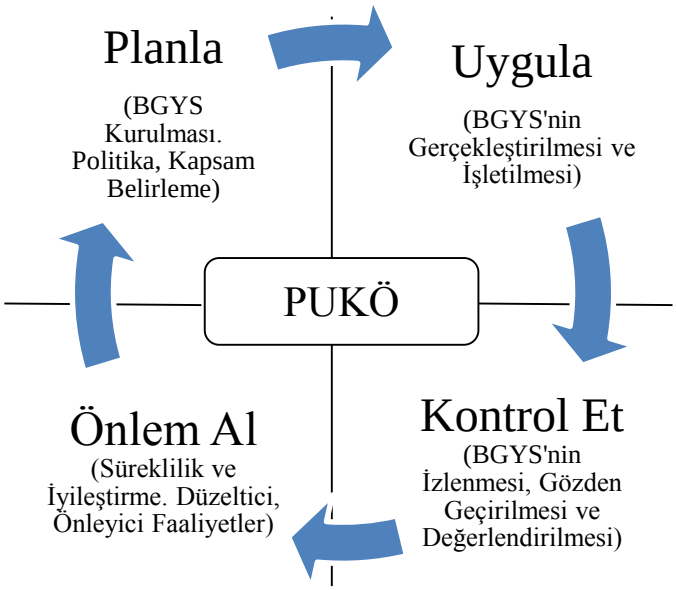
Bilgi güvenliğine olan ihtiyacın neden ortaya çıktığını anlamak için zamanında ve doğru olarak bilgi almanın önemini anlamak gereklidir. Bilgi güvenliğinin temel amacı doğru

kişinin kısa zamanda doğruluğundan emin olunan bilgiye ulaşımını garanti altına almaktır (Çetinkaya, 2008).

Her ortam ve sistem için bilgi güvenliğini sağlamada kritik rol oynayan temel güvenlik önlemleri; en az yetki, izinsiz her şey yasak, görevler ayrılığı, kullanılmayanların çıkarımı ve kullanılabilirlik-güvenlik dengesi ilkeleridir (Muharremoğlu, 2013). Bireysel kullanıcıların aksine kurumsal anlamda bilgi güvenliği daha komplikedir ve belli standartlar gerektirir. Bu standartların sağlanmasını sağlayan sistemin genel adı Bilgi Güvenliği Yönetim Sistemi (BGYS)'dir. Herkesçe genel kabul görmüş olan bir standardın kullanımı, güvenlik sistemini belirli bir referans çerçevesi içerisinde uluslararası düzeye taşır.

Kurumlar için Bilgi Güvenliği Yönetim Sistemi'nin varlığı olmazsa olmazdır. BGYS; Sadece teknik önlemlerle (güvenlik duvarları, atak tespit sistemleri, anti virüs yazılımları, anti casus yazılımlar, şifreleme, vb.) bilgi güvenliğini sağlama değil, insanları, süreçleri ve bilgi sistemlerini içine alan ve üst yönetim tarafından desteklenen bir yönetim sistemidir (Vural, 2007).

BGYS ile amaç risk yönetimi, iş sürekliliği, denetim, farkındalık, önlem ve güven olarak özetlenebilir. Standart bir kurumun BGYS etkinliğini artırmak amacıyla "Planla- Uygula- Kontrol Et- Önlem Al (PUKÖ) modeli olarak bilinen bir döngüsel model kullanılır (Evrin ve Demirer, 2011). PUKÖ döngüsü Şekil 1.6'da gösterilmiştir (Çetinkaya, 2008).



Şekil 1.6. Bilgi Güvenliği Yönetim Sistemi (Çetinkaya, 2008)

Şekil 1.6'da gösterilen ve BGYS'nin model olarak kabul ettiği PUKÖ döngüsü dört aşamadan oluşur.

a) Planla (BGYS nin kurulması): BGYS kapsamı, politikası, amaçlar, hedefler, süreçler, prosedürler ve önlemlerin geliştirilmesidir. BGYS'nin en zor ve önemli adımlarından olan risk analizi de bu aşamadadır.

b) Uygula (Uygulama ve İşletme): Belirlenen prosedürlerin uygulanması ve işletilmesi, eğitim ve farkındalık eğitimlerin verilmesi aşamasıdır.

c) Kontrol Et: İç tetkik ile politika, amaç ve süreçlerin performanslarını izleme, değerlendirme, ölçme ve rapor düzenleme aşamasıdır.

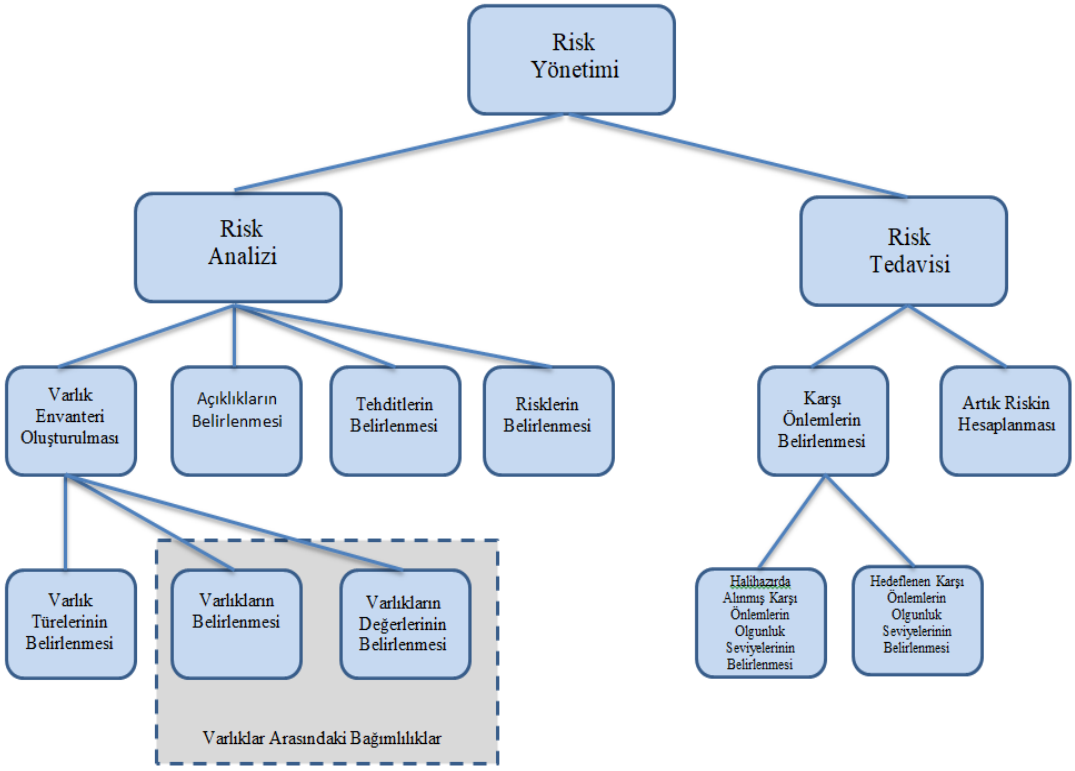
d) Önlem Al: Çıkan değerlendirme sonuçlarına göre düzeltici ve iyileştirici adımlar atılmasıdır. PUKÖ döngüsü devamlılık arz eden sürekli yenilenen bir süreçtir.

Bilgi güvenliği için en önemli adım BGYS kurulması, BGYS için ise en önemli adım risk yönetimidir. Risk, bir varlıktaki bir açıklığın bir tehdit tarafından kullanılma olasılığıdır. Risk; varlık, zafiyet ve tehdit olmak üzere üç adet girdiye bağımlıdır (Karabacak ve Özkan, 2010). Risk yönetimi, sistemi etkileyebilecek risklerin belirlenerek kontrol edilmesi ve ortadan kaldırılması veya azaltılması sürecidir. "TS ISO/IEC 27001:2005" standardı risk yönetimini bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetler olarak tanımlamıştır.

Risk yönetiminin risk analizi, risk işleme olmak üzere iki alt süreci vardır (Eskiyörük, 2007) Risk analizi, TS ISO/IEC 27001:2005 standardında kaynakları belirlemek ve riski tahmin etmek amacıyla bilginin sistematik kullanımı olarak tanımlanmıştır. Risk analizinde varlıklar bazında zafiyetler belirlenerek olasılık değerlendirmesi yapılıp tehditler belirlenir. Risk yönetiminde ikinci aşama risk işleme aşamasıdır. Bu aşama risk analizinde belirlenen risklerin nasıl işleneceğine karar verilmesi, önceliklendirilmesi ve riski azaltacak kontrollerin seçilerek uygulanmasından oluşur (Eskiyörük, 2007). Bilgi güvenliğine yönelik tehditleri Risk yönetimi ile azaltabilir veya yok edebiliriz. Risk yönetimi aşamaları Şekil 1.7'de gösterilmiştir (Anonim, 2017-8).

Günümüzde birden çok bilgi güvenliği standardı mevcuttur. Bilgi güvenliği yönetim standartlarına örnek olarak; kurum hedeflerine bilgi teknolojileri alt yapısını kullanarak ulaşmayı sağlayan COBIT, ISO/IEC 27001:2013 Bilgi Güvenliği Standardı, kartlı ödeme sistemlerinde bilgi güvenliği sağlamak için geliştirilen PCI DSS, hastaların sağlık bilgilerinin gizliliği ve güvenliği için çıkarılan HIPAA verilmektedir (Yaşar, 2014).

COBIT, 4 ana başlık altında toplanan 34 süreçten oluşmaktadır ve bu süreçler BGYS için dikkat edilmesi gereken hususları içermektedir. COBIT içerisinde var olan konu başlıkları Tablo 1'de ele alınmıştır.



Şekil 1.7. Risk Yönetimi aşamaları

Tablo 1. COBIT konu başlıkları (Boşal, 2017)

PO	**Planla ve Organize Et**	**DS**	**Teslimat ve Destek**
PO1	Stratejik BT Planının Tanımlanması	DS1	Hizmet Düzeyi Belirleme ve Yönetimi
PO2	Bilgi Mimarisinin Tanımlanması	DS2	Üçüncü Parti Hizmet Yönetimi
PO3	Teknolojik Yönün Belirlenmesi	DS3	Performans ve Kapasite Yönetimi
PO4	BT Organizasyon ve İlişkilerinin Tanımlanması	DS4	Sürekli Hizmet Sağlanması
PO5	BT Yatırımlarının Yönetimi	DS5	Sistem Güvenliğinin Sağlanması
PO6	Yönetim Hedeflerinin ve Talimatlarının İletilmesi	DS6	Harcamaların Belirlenmesi ve Bütçelenmesi
PO7	İnsan Kaynakları Yönetimi	DS7	Kullanıcı Eğitimi
PO8	Kalite Yönetimi	DS8	Kullanıcılara Yardım ve Danışmanlık
PO9	Risk Değerlendirme	DS9	Konfigürasyon Yönetimi
P10	Proje Yönetimi	DS10	Problem ve Olay Yönetimi
AI	**Tedarik ve Uygulama**	DS11	Veri Yönetimi
AI1	Otomasyon ve Çözümlerinin Belirlenmesi	DS12	Fiziksel Çevre Yönetimi
AI2	Uygulama Yazılımı Tedarik Edilmesi ve Bakımı	DS13	Operasyon Yönetimi
AI3	Teknoloji Altyapısının Tedarik Edilmesi ve Bakımı	**ME**	**İzle ve Değerlendir**
AI4	İş ve Kullanımın Etkin Kılınması	ME1	Süreç İzleme
AI5	BT Kaynaklarının Sağlanması	ME2	İç Kontrol Değerlendirme Yeterliliği
AI6	Değişiklik Yönetimi	ME3	Bağımsız Güvence Elde Edilmesi
AI7	Çözüm ve Değişikliklerin Kurulması ve Kabul Edilmesi	ME4	Bağımsız Denetim Sağlanması

Bir diğer standart olan ISO/IEC 27001:2013, 1995 yılında BS 7799 adıyla İngiltere'de kullanılan standardı temel alarak, Uluslararası Standartlar Teşkilatı (International Organization for Standardization, ISO) ve Uluslararası Elektroteknik Komisyonu (International Electrotechnical Commission, IEC) tarafından yayınlanmıştır. Uluslararası 27001 Bilgi Güvenliği Standardı; Bir Bilgi Güvenliği Yönetim Sistemi'ni (BGYS) kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model sağlamak üzere hazırlanmıştır (Çetinkaya, 2008).

Son olarak 23 Eylül 2013 yılında yayınlanan ISO/IEC 27001:2013 Bilgi Güvenliği Standardı günümüzde en yaygın kullanılan BGYS olup 14 adet güvenlik kontrol maddesi, 35 ana güvenlik kategorisi, 114 kontrol maddesi içermektedir. ISO/IEC 27001:2013 standardı kontrol listeleri ile risk analizi sonucu belirlenen riskleri ortadan kaldırmak veya kabul edilir seviyeye düşürmeyi hedefler.

ISO/IEC 27001:2013 Güvenlik Kontrol Maddeleri:

1. Bilgi Güvenliği Politikaları
2. Bilgi Güvenliği Organizasyonu
3. İnsan Kaynakları Güvenliği
4. Varlık Yönetimi
5. Erişim Kontrolü
6. Kriptografi
7. Fiziksel ve Çevresel Güvenlik
8. İşletim Güvenliği
9. Haberleşme Güvenliği
10. Sistem Temini, Geliştirme ve Bakımı
11. Tedarikçi İlişkileri
12. Bilgi Güvenliği İhlal Olayı Yönetimi
13. İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları
14. Uyum.

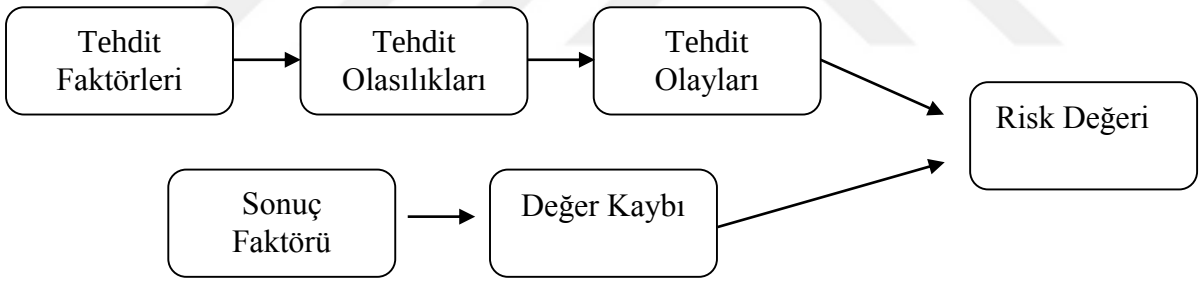
1.2. WEB Güvenliği

Bilgi güvenliğinin alt kategorisi olan Web Güvenliği, Web sitelerinin yaygınlaşması ile gün geçtikçe önem arz etmiştir. Web temel anlamda internet kullanıcıları arasında bilgi paylaşımı olarak kısaltılabilir. Bu paylaşım için Web uygulamaları kullanılmaktadır. Web

uygulamaları güvenliği zordur çünkü bu uygulamalar tanımı gereği kötü niyetli kullanıcılar da dâhil olmak üzere tüm kamuoyuna açıktır (Khochare ve ark., 2013).

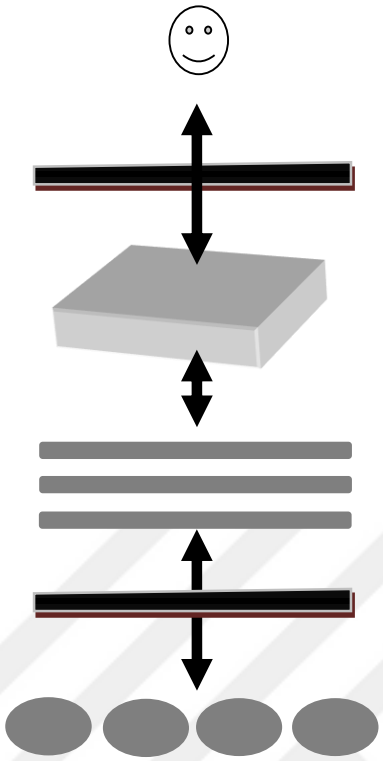
Web Güvenliğinde en önemli görev içerik sağlayıcısına yani uygulamanın sahibine düşmektedir. Günümüzde internet ağına bağlı hemen hemen tüm kurum veya kuruluşun bir Web uygulaması mevcuttur. Kurum veya kuruluşların Web uygulamaları üzerinden verdikleri hizmetler arttıkça ve dolayısı ile Web uygulamaları daha karmaşık bir hale geldikçe, söz konusu Web uygulamalarına yönelik olarak gerçekleştirilen saldırılar da her geçen gün artmaktadır. Bunun nedeni Web güvenliği ve güvenli yazılım geliştirme teknikleri konularına gereken önem verilmemesidir (Vural, 2007). Web, saldırganlara iki ana teşvik sunar. Birincisi, Web uygulamalarının finansal, tıbbi ve kişisel kayıtlar gibi hassas verileri giderek daha fazla depoluyor olması, ikincisi ise başarılı Web uygulamalarının milyonlarca kullanıcıya sahip olmasıdır (Cova, 2010).

Web güvenliğinde zafiyet ve tehditlerin tespiti için risk hesaplaması ve analizi oldukça önemlidir. Web güvenliği için risk hesaplama yöntemi Şekil 1.8'de (Zhao ve Yong, 2013), bir Web uygulama yapısındaki Web güvenlik riskleri aşamalı olarak Şekil 1.9'da gösterilmiştir (Dhingra, 2015).



Şekil 1.8. Risk hesaplama yöntemi (Zhao ve Yong, 2013)

Şekil 1.8'de görüldüğü üzere risk yönetiminde değeri olan her şey varlık olarak değerlendirilir ve her varlık bir risk değeri taşır.

Aşama		Risk
HTTP Kullanıcısı		CSS, Spoofing, Aldatma
Transport Layer		Pasif izleme. Ortadaki adam. Oturum çalma.
Firewall		HTTP engelsiz giriş.
Web Server		Bellek Taşması. Dizin Listeleme. String format. Varsayılan kullanıcı. Basit uygulamalar.
Web Uygulamaları CGI's		Manipule filtresini devre dışı bırakma. Null, meta karakterler. Bellek taşması.
Firewall		İç network
Veri Tabanı		SQL komut çalıştırma. Veri tabanı sorguları. Veri tabanı sömürüsü.

Şekil 1.9. Web güvenlik riskleri (Dhingra, 2015)

Şekil 1.9'da görüldüğü gibi Web güvenliğine yönelik risklere taşıma katmanında pasif izleme, ortadaki adam, oturum çalma gibi tehditler görülürken uygulama katmanında tehditler daha da çeşitlenmekte ve çoğalmaktadır.

Web ile ilgili güvenlik riskleri Açık Web Uygulama Güvenliği Projesi (The Open Web Application Security Project, OWASP) ve Amerika Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology, NIST) tarafından güncel olarak takip edilmektedir.

1.2.1. Açık Web Uygulama Güvenliği Projesi

Yaygın Web tehditleri ve Web güvenliği ile ilgili en kapsamlı kaynaklardan birisi 2001 yılında kurulan ve Web uygulama güvenliğinin artırılmasına yönelik ücretsiz araçlar, standartlar, formlar vs. ile ilgili hizmet sunan OWASP'dır. OWASP sunduğu geniş hizmetlerinin yanı sıra belirli sürelerle Web uygulamalarına yönelik tehditlerden en çok görülen ilk on tanesini Top 10 şeklinde yayınlamaktadır.

2017 yılı OWASP Top 10 Listesi (Anonim, 2017) ;

1. Enjeksiyon

2. Yanlış Kimlik Doğrulama ve Oturum Yönetimi

3. Çapraz Kod Çalıştırma (Cross-Site Scripting, XSS)

4. Hatalı Erişim Kontrolü

5. Yanlış Güvenlik Konfigürasyonu

6. Önemli Verilerin Elde Edilmesi

7. Yetersiz Saldırı Koruması

8. Siteler Arası İstek Sahteciliği (Cross-Site Request Forgery, CSRF)

9. Bilinen Güvenlik Açıkları Olan Bileşen Kullanma

10. Korumasız uygulama programlama ara yüzleri (API)'ler, şeklindedir.

1. *Enjeksiyon*

SQL, OS, XXE ve LDAP enjeksiyonu gibi enjeksiyon saldırıları, saldırgan tarafından üretilen kod/verilerin bir komut istemciye veya sorgunun bir parçası olarak bir yorumlayıcıya gönderildiğinde ortaya çıkar. Saldırganın istediği komutları çalıştırmasına, yetkisiz şekilde verilere erişmesine olanak tanır.

2. *Yanlış Kimlik Doğrulama ve Oturum Yönetimi*

Kimlik doğrulama ve oturum yönetimi ile ilgili yanlış veya eksik uygulamalar saldırganların parolaları, anahtarları veya oturum bilgilerini ele geçirmesine sebep olur.

3. *Siteler Arası Betik Çalıştırma (XSS)*

XSS hataları uygun bir doğrulaması yapılmamış güvensiz veri içeren Web sayfasına sahip bir uygulamada veya tarayıcı API içeren ve kullanıcı taraflı verilerle güncellenen JavaScript koduna sahip Web sayfası içeren bir uygulamada meydana gelir. XSS, saldırganın kurbanının tarayıcısında kullanıcı oturumlarını ele geçirebilmesine, Web sitesini değiştire bilmesine veya kullanıcıyı kötü niyetli sitelere yönlendiren komut dizileri yürütmesine izin verir.

4. *Hatalı Erişim Kontrolü*

Kimliği doğrulanmış kullanıcıların yapmalarına izin verilen sınırlamaların doğru bir şekilde uygulanmamasıdır. Saldırganlar bu zafiyetleri, diğer kullanıcıların hesaplarına erişmek, hassas dosyaları görüntülemek, diğer kullanıcıların verilerini değiştirmek, erişim haklarını değiştirmek gibi yetkisiz işlemler için kullanabilirler.

5. *Yanlış Güvenlik Konfigürasyonu*

İyi bir güvenlik, uygulama, uygulama sunucusu, Web sunucusu, veri tabanı sunucusu gibi platformların güvenli bir şekilde yapılandırılmasıyla olur. Varsayılan değerler genellikle güvensiz olduğu için, yeni güvenlik ayarları tanımlanmalı, uygulanmalı ve devam ettirilmelidir. Buna ek olarak, yazılımlar güncel tutulmalıdır.

6. *Önemli Verilerin Elde Edilmesi*

Birçok Web uygulaması ve uygulama programlama arayüzü (Application Programming Interface, API), finansal, sağlık hizmetleri ve kişisel bilgiler gibi hassas verileri düzgün şekilde korumaz. Saldırganlar, zayıf şekilde korunan bu verileri dolandırıcılık, kimlik hırsızlığı veya diğer suçları işlemek için çalabilir, değiştirebilirler. Hassas veriler, depolama sırasında veya kullanımında şifreleme gibi ilave koruma ve güvenlik tedbirleri gerektirir.

7. *Yetersiz Saldırı Koruması*

Uygulamaların ve API'lerin çoğunun hem manuel hem de otomatik saldırıları tespit etme, önleme ve bunlara tepki verme becerisi eksiktir. Saldırı koruması, temel veri girişi doğrulamanın ötesinde otomatik olarak oturum açma, yanıt verme ve hatta sömürü girişimlerini engeller. Bu zafiyetin bir diğer nedeni uygulama yamalarının güncel olmamasıdır.

8. *Siteler Arası İstek Sahteciliği (CSRF)*

Bir CSRF saldırısı kurbanın oturum açılmış tarayıcısını, savunmasız Web sunucusuna sahte http isteği göndermeye zorlar. Bu http isteği oturum çerezleri ve otomatik kimlik doğrulama bilgilerini içerir. Böyle bir saldırı ile sunucu oturum açılmış bir kullanıcıdan gelen saldırgan isteklerinin meşru olduğunu düşünür.

9. *Bilinen Güvenlik Açıkları Olan Bileşen Kullanma*

Güvenlik açığı olan bir bileşen kullanılması, ciddi veri kayıplarına ve sunucuyu ele geçirmeye varan güvenlik açıklarına sebep olabilmektedir.

10. *Korumasız Uygulama Programlama Ara Yüzleri (API)'ler*

Modern uygulamalar çoğunlukla JavaScript ve mobil uygulamalar gibi zengin istemci uygulamaları ve Application Programming Interface (API)' ler içerir (Simple Object Access Protocol (SOAP) / eXtensible Markum Language (XML), Remote Procedure Call (RPC), Google Web Toolkit (GWT), vb.). Bu API'ler çoğu zaman korunmasızdır ve birçok güvenlik açığı içerir.

1.2.2. ABD Ulusal Standartlar ve Teknoloji Enstitüsü

Ülkemizdeki TSE benzeri Amerika Birleşik Devletlerinin standartlar ve teknoloji enstitüsüdür. Web uygulamaları için sunucu taraflı kurulum, konfigürasyon ve işletim güvenliği ile ilgili standartları mevcuttur. NIST ‘e göre sunucu taraflı tehditler;

1. Saldırganlar Web sunucu üzerindeki yazılım hatalarını sömürü amacıyla kullanabilirler veya sunucuya yetkisiz erişim için bir kod çalıştırabilirler. Bu yetkisiz erişime örnek olarak, herkes tarafından erişilebilir olmayan dosyalara veya klasörlere erişmek, komutları yürütmek ve Web sunucusuna yazılım yüklemek verilebilir.

2. Web sunucuya, sunucu altyapısına veya servislere yönelik DoS saldırılar.

3. Web sunucudaki hassas verilerin yetkisiz okunması veya değiştirilmesi.

4. Bir Web uygulamasının etkileşimli öğelerini desteklemek için kullanılan veritabanları üzerindeki hassas bilgiler, komut enjeksiyonu saldırılarına (örneğin SQL enjeksiyonu, LDAP enjeksiyonu, XSS) hedef olabilir.

5. Web sunucusu ile tarayıcı arasında şifrelenmemiş olarak iletilen hassas bilgiler engellenebilir.

6. Web sunucudaki bilgiler zararlı amaçlar için değiştirilmiş olabilir. Web sitesi tahrifatı örnek olarak verilebilir.

7. Saldırgan Web sunucu vasıtasıyla tüm ağa yetkisiz erişim hakkı elde edebilir.

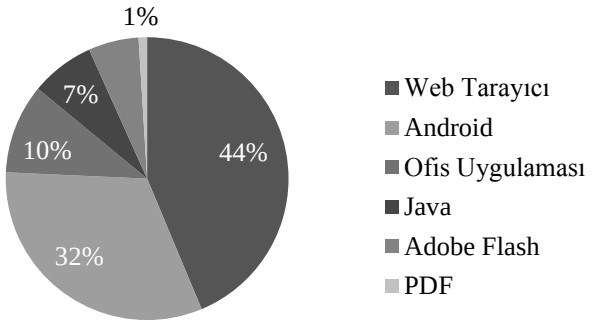
8. Saldırganlar, Web sunucuya zarar verdikten sonra harici varlıklara saldırabilir. Bu saldırılar, doğrudan (ele geçirilen sunucudan harici bir sunucuya karşı) veya dolaylı olarak (siteyi ziyaret eden kullanıcıların Web tarayıcılarındaki güvenlik açıklarını kullanmaya yetkili olan Web sunucusuna kötü amaçlı içerik yerleştirme) başlatılabilir.

9. Sunucu, saldırı araçları veya yasadışı olarak kopyalanmış yazılımlar için bir dağıtım noktası olarak kullanılabilir. NIST ana çatı yapısı Tablo 2’de gösteriliştir.

Tablo 2. NIST ana yapısı

Fonksiyon	Kategori
Tanımlama	Varlık Yönetimi İş Yönetim Risk Değerlendirme Risk Yönetimi
Koruma	Erişim Kontrolü Farkındalık Eğitimi Veri Güvenliği Bilgi Koruma Proses ve Prosedürleri Bakım Koruyucu Teknolojisi
Tarama	Anormallikler ve Olaylar Güvenlik Takibi Tespit Süreci
Müdahale	Müdahale Planlama Haberleşme Analiz Azaltma İyileştirme
Düzeltme	Düzeltme Planlama İyileştirmeler İletişimler

Web uygulamalarında en önemli güvenlik risklerinden birisi de kullanılan eklentiler veya uygulamalardır. Bir antivürüs yazılım şirketi olan Kaspersky'in web sitesindeki verilere göre 2017 yılının ilk çeyreğinde Web uygulamalarına yönelik saldırıların hangi uygulamalara yönelik olduğunun grafiği Şekil 1.10 'da gösterilmiştir.



Şekil 1.10. Web uygulamalarına yönelik saldırılar (Anonim, 2017-11)

Web güvenliği ile ilgili tehditlerden detaylıca bahsettikten sonra Web güvenliği ile ilgili tehditler için önlem veya korunma amaçlı farklı yaklaşımlardan bahsetmek gerekir. Bu temel yaklaşımlara;

1. Güvenlikle ilgili sıkıntı meydana geldikten sonra önlem alma olan pasif yaklaşım.
2. Güvenlik duvarı, SSL, antivirüs programı, Saldırı Tespit Sistemi (Intrusion Detection System, IDS) gibi güvenlik önlemleri alarak saldırılardan korunma yaklaşımı.
3. Sızma testleri olarak da tanımlanan bir diğer yaklaşım türü ise araçlar yardımıyla otomatik zafiyet taraması yapmak örnek olarak verilebilir.

2. KAYNAK ARAŞTIRMASI

Web Güvenliğinin öneminden dolayı son yıllarda bu konuda önemli çalışmalar yapılmıştır.

(Vural, 2007), bilgi güvenliği ile ilgili en kapsamlı çalışmalardan birisini yapmıştır. Bilgi güvenliğini genel olarak incelemiş, kurumsal bilgi güvenliği ve standartlarından, bilgi güvenliğini zaafa uğratan tehditlerden bahsetmiştir. Ayrıca ülkemiz bilişim hukuku ve web uygulamaları üzerine odaklanarak SQL enjeksiyonu ve sızma testlerinden bahsetmiştir.

(Obied, 2008), zararlı yazılım türlerinden bahsederek, balküpü tekniği ile saldırganların kullandıkları teknikleri belirlemeye çalışmıştır. Bunun için, zafiyetler içeren bir uygulama geliştirdikten sonra bunu internete koyarak kendisine saldırı yapılmasına fırsat vermiştir. Böylelikle kendisine saldıran saldırganların kullandıkları teknikleri belirlemeye çalışmıştır.

(Cova, 2010), çalışmasında günümüzde mevcut Web güvenlik sorunlarına yönelik geliştirdiği yaklaşımlar ve tekniklerden bahsetmiştir. Geliştirdiği tekniklerde statik analiz yöntemini ele almış olup kimlik avı ve botnet bağlamında gerçekleştirdiği ölçümleri değerlendirmiştir.

(Shahriar, 2011), Web zafiyetlerinden en yaygın olan XSS ve CSRF üzerine kapsamlı bir çalışma yapmıştır. Bu çalışmada XSS ve CSRF'in çeşitlerinden, neden kaynaklandığından detaylı olarak bahsetmiş, bu zafiyetlerin tespitine yönelik uygulama geliştirerek diğer hazır araçlar ile karşılaştırmalar yapmıştır.

(Yalçınkaya, 2012), Türkiye'deki kamu kurumlarının TÜRKSAT'ın yayınladığı standart ile uyumluluğunu analiz etmiştir. Bu çalışmada TÜRKSAT standardından 32 kural seçmiş ve belirlenen 50 kamu kurumu üzerinde bu kuralları kontrol ederek bulduğu sonuçları yayınlamıştır.

(Utku, 2012), Web servislerin otomatik olarak test edilmesi için bir yöntem geliştirmiş, bu yöntemde semantik bağımlılık tabanlı ve veri mutasyon tabanlı teknikler kullanılarak, web servislerin analizi ve değişik test senaryolarının üretilmesini sağlamıştır.

(Martirosyan, 2012), bir Web uygulaması geliştirerek Qualys Guard ve Acunetix programları ile değerlendirmesini yapmıştır. Ayrıca Web güvenliği standartlarına göre geliştirdiği Web uygulamasının eksikliklerini belirlemiştir.

(Ruse, 2013), Web uygulamalarına yönelik en yaygın saldırı türlerinden enjeksiyon ve XSS saldırılarını ele almıştır. Bu iki saldırı türünün çeşitlerinden ve uygulama örneklerinden bahsederek korunma yöntemlerini detaylı olarak ele almıştır. Ayrıca enjeksiyon ve XSS açıklarını tespit etme yöntemlerinden bahsetmiştir.

(Akyıldız, 2013), sızma testlerinin öneminin vurgulanması açısından, gerekli servis, sunucu ve ağ kurulumlarını yaparak oluşturduğu bu laboratuvar ortamında sızma testleri için bir uygulama benzetimi hazırlamıştır. Uygulama alanında gerçek hayatta karşılaşılan saldırıların uygulamasını yapmıştır. Böylelikle gerçek ortamda karşılaşıla bilecek saldırı türlerini örneklemeye çalışmıştır.

(Muharremoğlu, 2013), kurumsal bilgi teknolojilerinde sık karşılaşılan güvenlik sorunlarının kök nedenlerinden bahsedip detaylandırmıştır. Bu sorunlar çerçevesinde güvenliği sağlama yöntemlerinden ve mekanizmalarından bahsetmiştir. Ayrıca saldırı türleri ve zafiyetlerden bahsederek bunların teknik yapısını incelemiştir.

(Jnena, 2013), Web uygulamaları zafiyet analizi ile ilgili çalışmasında SQL enjeksiyonu ve XSS ile ilgili bilgilendirme kapsamında çeşitlerinden, yöntemlerinden ve korunma önerilerinden bahsederek kendi oluşturduğu bir araç ile diğer araçları karşılaştırmış, bulduğu sonuçları yayınlamıştır.

(Doğan, 2013), popüleritesi gün geçtikçe artan sızma testleri kapsamında Web sızma testleri ile ilgili 2000-2013 yılları arası yayınlanmış olan ulusal ve uluslararası 193 makaleyi incelemiş ve test yaklaşımları, hata modelleri, araçlar, metrikler ve deneysel kanıtlar hakkında bilgiler sunmuştur.

(Hassan, 2013), Web güvenliği zafiyetlerinden bahsederek Web güvenliği tehditlerini azaltmaya yönelik teknikleri anlatmıştır. Web güvenlik zafiyetini bulmaya yönelik teknikler geliştirmiştir. Web güvenliğinde sunucu ve istemci tarafına yönelik zafiyetlerden bahsetmiştir.

(Ajaj, 2013), yaygınlaşmakta olan bulut teknolojisinde Web uygulamalarının kullandığı Web servislere değinerek bu servislerin bulut teknolojisinde kullanım standartlarından, bulut teknolojisi için kullanılması gerekli yazılımlardan ve alınması gereken güvenlik önlemlerinden bahsetmiştir.

(Arsoy, 2014), Web siteleri için yayınlanan Uluslararası standartlardan bahsederek ülkemizdeki e-devlet Web sitelerinin bu standartlara uygunluğu yönünden değerlendirmesini yapmış, genel olarak kullanılabilirlik problemleri olduğu sonucuna varmıştır.

(Fung, 2014), yaygın olan Web güvenliği zafiyetlerinden bahsederek bu Web zafiyetleri ile ilgili mevcut güvenlik açıklarının azaltılmasına yönelik tekniklerden bahsetmiş, çok yönlü savunma sistemlerine değinmiştir. Ayrıca SSL kullanmanın Web güvenliği için önemini vurgulamıştır.

(Doupe, 2014), bilgi güvenliği için vazgeçilmez olan sızma testlerinde kullanılan yöntemlerden detaylı olarak bahsetmiştir. Ayrıca zafiyet algılama algoritmalarından

bahsederek özellikle siyah kutu sızma testi üzerinde durmuş XSS ile ilgili çeşitlerinden, önlemlerden bahsederek uygulamaları üzerinde yoğun bir çalışma yapmıştır.

(Gökçay, 2014), özellikle adli soruşturmalarda kullanılması maksadıyla IP akışı (flow) ile elde edilen bilgilere dayalı Web uygulaması güvenlik açığı tarama araçlarını tespiti çalışmaları yapmıştır.

(Sarıkoz, 2015), Web uygulamaları iletişiminde kullanılan Web Servisler konsepti hakkında detaylı bilgi vererek yapıları hakkında çalışma yapmıştır. Bir işletme ağında bulunan web servisinin bütün güvenlik durumunun sağlanılması için bir bilgi güvenliği çerçevesi önermiş, bir bilgi güvenliği modellemesi sunmuştur.

(Giannini, 2015), çalışmasında kendi geliştirmiş olduğu Web uygulama oluşturma aracı ile bir Web uygulaması oluşturmuştur. Oluşturulan bu uygulamanın güvenlik değerlendirmelerini yaparak bulduğu riskler hakkında detaylı bilgiler vermiş bunların giderilmesine yönelik öneriler sunmuştur.

(Atıcı, 2015), dinamik Web uygulamalarının vazgeçilmez unsurlarından olan JavaScript kütüphanelerini detaylı bir şekilde incelemiş, yaygın kullanımı sebebiyle saldırganların ilgisini çekmekte ve kullanımı ile bazı zafiyetler oluşturabilmekte olan JavaScript kütüphanelerini sınıflandırmıştır.

(Mussa, 2016), yazılım güvenliği ile ilgili standartlardan bahsederek matematiksel ve istatistiksel modelleme, veri analizi ve ölçüm yöntemlerini kullanarak, verilen bir yazılımdaki zayıf noktaların sayısına dayanarak güvenlik açıkları riskini hesaplayan yeni bir güvenlik açığı bulma modeli geliştirmiştir.

(Polat, 2016), sızma testleri ile ilgili türlerinden, çalışma metodolojisinden ve uygulama şekillerinden bahsederek bilgi güvenliği için özellikle kurumsal ağlarda aralıklarla yapılması gereken sızma testlerinin önemini vurgulamış, hangi testlerin yapılabileceğinden bahsetmiştir.

(Pelizzi, 2016), sık karşılaşılan Web uygulamaları güvenlik açıklarından bahsetmiş, Web uygulamalarında karşılaşılan bu güvenlik açıklarının oluşması sebeplerinden bahsederek örnekler ile açıklamıştır. Ayrıca bu güvenlik açıklarının azaltılmasına yönelik yeni teknikler önermiştir.

(Zhang, 2016), Web tarayıcılarında ve bulut hizmetlerinin yaygınlaşması ile bulut hizmetlerinde sağlanan ilerlemelerden ve yeni teknolojilerden bahsederek, Web uygulamalarının mevcut olan temel mimarisini yeniden değerlendirmeği amaçlayarak yeni teknikler sunmuştur.

3. MATERYAL VE YÖNTEM

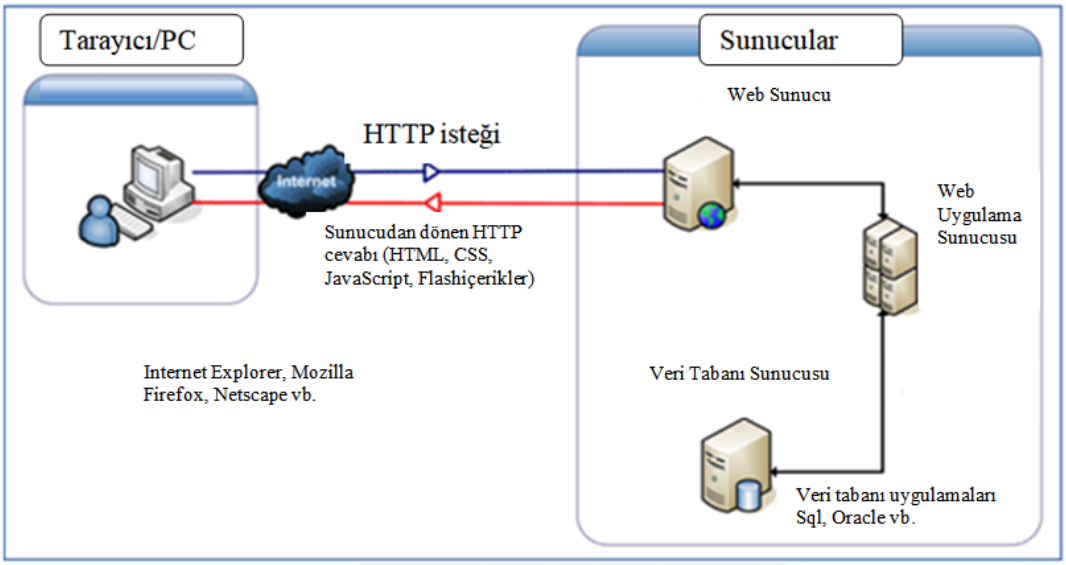
Çalışmanın bu bölümünde Web uygulamaları ve Web güvenliği ile ilgili başvurula bilinecek bilgiler verildikten sonra kullanılan materyallerden ve çalışmanın nasıl bir metot izlenerek gerçekleştirildiğinden bahsedilmiştir.

3.1. Materyal

Sızma testleri temel alınarak yürütülen çalışmada Web platformu ile ilgili gerekli bilgilendirmeler yapıldıktan sonra sızma testleri yöntemlerinden, Web uygulamalarında sıkça karşılaşılan zafiyetlerden bahsedilmiş ve çalışmada kullanılan işletim sistemi ile programlar tanıtılmıştır.

3.1.1. Web platformu ve uygulama yapısı

Genel bir standardı olmamakla birlikte Web uygulamaları karmaşık bir yapıya sahiptir. İstemci (Web istemci) – sunucu (Web sunucu) modeli ile çalışan Web uygulamalarında tarayıcı aracılığı ile sunucuya bilgi girişi de dâhil HTTP isteği gönderir. Sunucu gelen isteği yerine getirir, tarayıcıya geri gönderir veya depolar. HTML veya XHTML formatlı dokümanlar kullanılır. Web uygulamaları genel çalışma prensibi Şekil 3.1‘ de gösterilmiştir.



Şekil 3.1.Web uygulamaları çalışma prensibi (Stuttard ve Pinto, 2011)

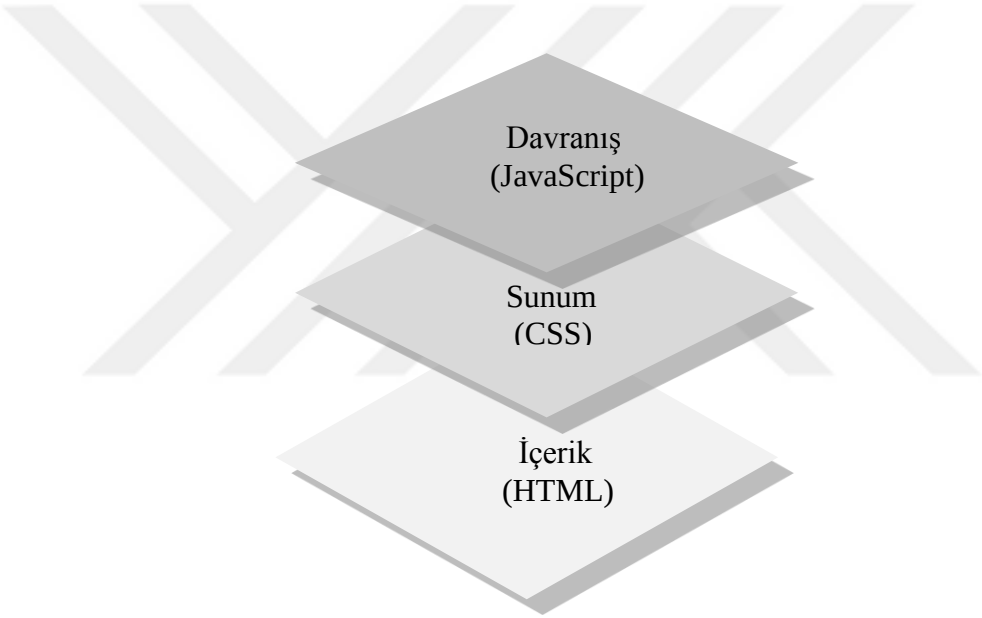
Web uygulamaları sunucu tarafında çalışan ve istemci tarafında çalışan olmak üzere ikiye ayrılır (Stuttard ve Pinto, 2011). Sunucu tarafında kullanılan uygulamalar:

- PHP, VBScript ve Perl gibi script dilleri
- Platform olarak ASP.NET, Java
- Web sunucu olarak Apache, IIS ve Netscape Enterprise
- Veri tabanı olarak MS-SQL, Oracle, MySQL
- Web Servisleri

İstemci tarafı uygulamalar:

- HTML, CSS, JavaScript, VBScript
- AJAX
- Java applets, ActiveX, Flash' dır.

Temel bir Web sayfa yapısı ve sayfada HTML, CSS, JavaScript kullanımı Şekil 3.2'de gösterilmiştir.



Şekil 3.2. Web sayfa yapısı (Atıcı, 2015).

Web Sunucu: İnternetin bilgi kaynağı ve depolama alanı olan Web sunucular, istemcilerin Web sayfası, dosya, fotograf, video gibi veri isteklerine cevap vermektedir (Endraca ve ark., 2013). Nihai hedefi istemcilere hizmet vermek olan Web Sunucular Apache HTTP Server, Microsoft Internet Information Server (IIS) gibi Web sunucu yazılımlarını üzerinde barındırır.

Web İstemci: İstemci tarafında çalışan Microsoft Internet Explorer, Mozilla Firefox, Chrome ve Apple Safari gibi örnekleri olan bir Web sunucu ile haberleşme ara yüzüdür. Çalışma prensibi beş maddede toplanabilir. (Obied, 2008).

1. DNS vasıtasıyla IP adrese göre Web sunucu adresine bağlantı sağlar

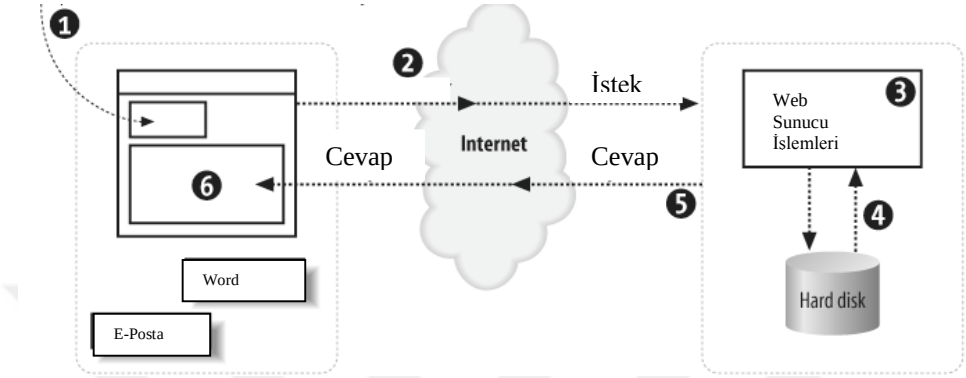
2. Web sunucu ile TCP bağlantısı kurar.

3. Web sunucuya HTTP GET request mesajı gönderir.

4. Sunucudan gelen HTTP response mesajını çalıştırır.

5. Web sunucu ile kurulan TCP bağlantısını sonlandırır.

Web istemci çalışma prensibi Şekil 3.3'de gösterilmiştir.



Şekil 3.3. Web istemci çalışma mantığı (Anonim, 2017-4).

Web Servisleri: Web servisleri farklı platformlar ve diller arası iletişimi sağlamak amacıyla kullanılan ve protokoller aracılığı ile iletişim kuran ağ erişim ara yüzüdür. Web servisleri SQL enjeksiyonu, XPath enjeksiyonu, kod çalıştırma, bellek taşması, kullanıcı adı/şifre elde etme, sunucu yol (path) unun elde edilmesi gibi zafiyetlere neden olabilmektedir (Vieira ve ark., 2008). Günümüzde yaygın olarak dört çeşit Web servis tipi kullanmaktadır (Sarıkoz, 2015).

1. XML (eXtensible Mark-up Language); Platformdan bağımsız ve kolay veri erişimi için kullanılır. XML veri depolama formatı oluşturur ve veriyi işleyecek Web servisi belirler.

2. SOAP (Simple Object Access Protocol); XML tabanlıdır. XML'i destekleyen gelişmiş HTTP protokolü diyebiliriz.

3. WSDL (Web Service Language Description); XML tabanlıdır. Web servisleri için iletişim yolu ve protokol belirlemek için kullanılır.

4. UDDI (Universal Description, Discovery and Integration); Web servisler için kayıt ve keşif mekanizmasıdır. Hangi Web servisin hangi Web uygulamasıyla çalıştığını keşfeder.

Protokol: Web uygulamaları için temel protokol transport katmanında çalışan ve TCP/IP kullanan HTTP protokolüdür. HTTP; Web uygulamalarında istemci ile sunucu arasındaki özellikle statik veri transferi için kullanılır. HTTP protokolünü kullanarak "HTTP

Requests" denilen istemciden gönderilen istek mesajlarına karşı sunucu "HTTP Response" yani cevap mesajı gönderir. Tipik bir HTTP Requests isteği Şekil 3.4' de, HTTP Response isteği Şekil 3.5'de gösterilmiştir (Stuttard ve Pinto, 2011).

```
GET /auth/488/YourDetails.ashx?uid=129 HTTP/1.1
Accept: application/x-ms-application, image/jpeg, application/xaml+xml,
image/gif, image/pjpeg, application/x-ms-xbap, application/x-shockwave-
flash, */*
Referer: https://mdsec.net/auth/488/Home.ashx
Accept-Language: en-GB
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64;
Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
3.0.30729; .NET4.0C; InfoPath.3; .NET4.0E; FDM; .NET CLR 1.1.4322)
Accept-Encoding: gzip, deflate
Host: mdsec.net
Connection: Keep-Alive
Cookie: SessionId=5B70C71F3FD4968935CDB6682E545476
```

Şekil 3.4. HTTP İstek (Stuttard ve Pinto, 2011)

```
HTTP/1.1 200 OK
Date: Tue, 19 Apr 2011 09:23:32 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Set-Cookie: tracking=tI8rk7joMx44S2Uu85nSWc
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 1067
```

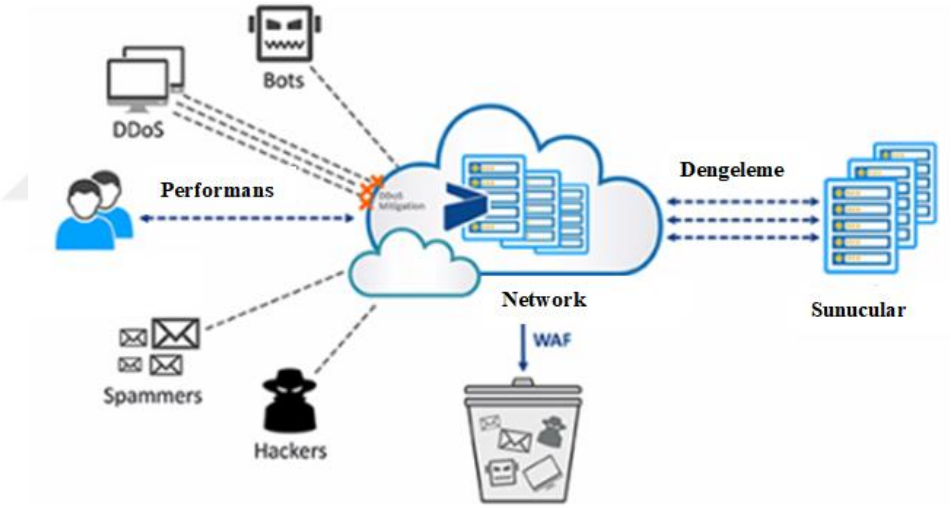
Şekil 3.5. HTTP Cevap (Stuttard ve Pinto, 2011)

2015 yılında HTTP 2 yayınlanmış olmakla beraber HTTP 1.1 yaygın olarak kullanılmaktadır. Tez çalışmasında incelediğimiz tüm sitelerin HTTP 1.1 protokolünü kullandığı tespit edilmiştir. HTTP'nin varsayılan olarak kullandığı port "80" dir. Sunucuya yük bindiren ve özellikle bankacılık ve alışveriş siteleri gibi internetin daha güvenlik gerektiren işlemleri için Secure Socket Layer (SSL) / Transport Layer Security (TSL) teknolojilerini ve 443 portunu kullanan HTTPS protokolü kullanılmaktadır. SSL, 128 bitlik şifreleme ile uçtan uca güvenli bağlantı sağlayan bir tünel teknolojidir. SSL teknolojisinde en büyük risk SSL tünelin ele geçirilmesi ile MITM (Man in The Middle) yani aradaki adam saldırılarıdır. Bu saldırılar için TSL teknolojisi çözüm olabilmektedir. SSL/TSL yapısı Şekil 3.6'da gösterilmiştir (Haque, 2016).

SSL Handshake Protokolü	SSL Change Ciper Spec Protokolü	SSL Alarm Protokolü	HTTP
SSL Kayıt Protokolü			
		TCP	
IP			

Şekil 3.6. SSL yapısı (Haque, 2016)

WAF: Web Uygulama Güvenlik Duvarı (Web Application Firewall) istemci ile sunucu arasında konumlanmış ve HTTP trafiğini analiz ederek olabilecek Web saldırılarına karşı sistemi koruyan cihazlardır. Sunum katmanında çalışmaktadır. WAF, gelen paketlerin sunucuya ulaşmadan önce veri kısmı da dâhil paket içeriğini inceleyerek paket türünü belirler erişime izin verir veya engeller. Şekil 3.7'de WAF çalışma prensibi gösterilmiştir (Anonim, 2017-5).



Şekil 3.7. WAF çalışma prensibi

HTML: Hyper Text Markup Language kelimelerinin baş harflerinden oluşan HTML basit, statik bir Web sayfasının temel kodudur. HTML dili ile bilgiler tarayıcının çalıştırabileceği şekilde bir formata dönüştürülür. XML desteği sağlayan XHTML in geliştirilmesi ile daha çok özellik kazanmıştır.

Metotlar: Metotlar Web uygulamalarında istemci tarafından sunucuya gönderilir. İstemcinin sunucudaki bilgiye erişim yöntemini belirlemeye yarar. HTTP en çok kullanılan GET ve POST metotlarına ilave olarak birçok metot kullanmaktadır (Anonim, 2017).

1. PUT: Bu metot istemci tarafından sunucuya yeni dosya yüklemek için kullanılmaktadır. Dolayısıyla saldırgan tarafından zararlı dosyaların sunucuya yüklenmesine neden olabilmektedir.

2. DELETE: İstemcinin sunucudan dosya silmesine olanak tanır.

3. CONNECT: İstemcinin Web sunucuyu vekil sunucu olarak kullanmasına imkân sağlar.

4. TRACE: Daha çok hata bulma amaçlı kullanılan bu metot istemci tarafından sunucuya gönderilen her bir verinin geri yansımasıdır. Sömürüye açık bir metottur.

5. GET: Sunucudan dosya veya veri almak veya göndermek için kullanılan GET metodunda sunucudan gönderilen cevapta içerik kısmı da olur. Gönderilen veri kullanıcı tarafından görülebildiği için güvenli değildir.

6. HEAD: GET ile özellikle sunucu tarafında aynı mantıkla çalışan HEAD metodunda sunucudan gönderilen cevapta sadece başlık kısmı olur, içerik kısmı olmaz.

7. POST: PUT metoduna benzer özellik gösteren POST sunucuya veri göndermek için kullanılır. Gönderilen veriler başlık (header) kısmında değil içerik (body) kısmındadır. Bu yüzden tarayıcıda görünmez. Genellikle form işlemleri için kullanılır.

8. OPTIONS: Sunucunun hangi metotları desteklediğini öğrenmek için kullanılır.

Başlık: İstemci – sunucu arasındaki karşılıklı gönderilen istek ve cevap gerçek verinin başlık kısmında bulunan ve kritik bilgiler içeren bölümüdür. HTTP birden çok HEADER yapısını desteklemektedir. Bazıları HTTP request veya HTTP response olabildiği gibi bazıları da özel mesaj içerikli olabilmektedir (Stuttard ve Pinto, 2011).

Oturum ve Çerezler: Web uygulamalarında en önemli güvenlik riski kritik verilerin istenmeyen kişilerin kontrolüne geçmesi olan yetkisiz erişimdir. Bilgi güvenliğinin temeli olan gizlilik, bütünlük ve erişebilirlik ilkeleri doğrultusunda yetkilendirme, erişim denetimi ve oturum yönetimi bir Web uygulamasının güvenlik açısından vazgeçilmezidir. Bilgiye erişimin kontrol altına alınması olan yetkilendirmede amaç özellikle hassas bilgilere kim ne yapmak için erişebilir şeklinde açıklanabilir. Web uygulamalarında kullanıcı adı, şifre uygulamaları erişim denetimine örnek olarak verilebilir. Erişime izin verilen kullanıcı aynı Web uygulamasında birden fazla HTTP isteğinde bulunabilir. HTTP protokolü rezerve sistemi ile çalışmadığı için ikinci bir istekte kullanıcı bilgisine tekrar ihtiyaç duyar. Bu durumdan kurtulmak için "Session" yani oturum yönetimi devreye girer (Giannini, 2015). Oturum yönetimi ile sunucu tarafından kullanıcıya özel jeton (token) üretilir ve kullanıcının aynı Web uygulamasındaki birden çok HTTP isteği için kullanılır. Diğer bir session yöntemi olan HTTP "cookies"ler yani çerezler sunucu tarafından oluşturulup gönderilen HTTP cevap mesajının

“Header” kısmından oluşur ve boyutu en fazla 4096 byte olan text dosyası olarak istemci Web tarayıcıda depolanır, sunucu her istekte bulunduğunda isteğin “Header” kısmına eklenerek geri gönderilir (Giannini, 2015). Çerezler (Cookies) oturum yetkisi almak, devam ettirmek ve geçici kullanıcı verisi tutmak için kullanılırlar. İstemciden gelen birden çok isteğe karşı oturum bilgisinin korunması günümüzde geniş kullanım alanına sahip Web uygulamaları için kritik öneme sahiptir. İçerdiği hassas verilerden dolayı ve oturum hırsızlığına sebep olabildiğinden Cookie kullanımında güvenlik önlemlerine dikkat etmek gerekmektedir. OWASP standartlarında belirtilen Cookie güvenliği maddeler halinde;

1.“Secure” bayrağının set edilmesi yani oturum açıldıktan sonra oluşturulan çerezin kriptolu şekilde gönderilmesinin sağlanması.

2.Cookie bilgisinin istemci tarafındaki zararlı bir script tarafından ele geçirilmesini önlemek için HTTPOnly etiketinin kullanılması.

3.Domain adının zafiyete sebep olmayacak şekilde tam yazılması

4.Domain adında olduğu gibi sunucudaki yolun özellikle kök dizini belirtmeyecek şekilde tam olması.

5.Cookilerin bir yaşam süresinin olmasının sağlanmasıdır.

3.1.2. Sızma testleri

Genel anlamda sızma testleri, bir saldırgan (Saldırgan (hacker), eski çalışan, hacker olmayan tehlikeli kişi (Script Kiddie), vb.) veya zararlı bir yazılım (Solucan, Virus, Truva Atı, casus yazılım (Spyware), vb.) tarafından bilgi teknolojileri altyapısına ve kurumun bilgi akışına gelebilecek zararların önceden tespit edilmesini sağlayan testler bütünüdür (Muharremoğlu, 2013). Bilgi güvenliğine yönelik dış tehdit unsurlarından zararlı yazılım yani "Malicious Programs" kötü niyetli kişilerin bilgi güvenliğine yönelik, izinsiz veri bozma, silme veya çalma işlemleri ile internet cihazına zarar vermesi olarak tanımlanabilir. Malware olarak kısaltılan zararlı yazılımlar kişisel bilgisayarlara zarar verdiği gibi şirket veya devlet kuruluşlarına da zarar verebilmektedir. McAfee verilerine göre 2014 ün son çeyreğinde 50 milyonu yeni olmak üzere 350 milyon zararlı kod tespit edilmiştir (Saleh, 2016). Zararlı kodlara Adware, Spyware, Virüs, Worm, Trojan, Rootkit, Logic Bombs, Backdoor, Keylogger, Ransomware, Browser Hijacker, Botnet örnek olarak verilebilir.

- *Adware;* Özellikle bedava programlarda olan istenmeyen reklamlar olarak kısaltabiliriz.
- *Spyware;* Adware benzeri fakat ondan farklı olarak hangi sitelere girildiği, ne tür içerikle ilgilenildiği hatta kredi kartı numarası, internet şifreleri gibi kişisel bilgileri daha

önceden belirlenmiş bir sunucuya gönderen, ajanlık eden programlardır. Casus yazılımlar olarak bilinir. Kısaca bir sistemden veri toplamak için tasarlanmış çeşitli zararlı yazılımlardır (Kobus, 2016).

- *Virüs;* Kullanıcının izni ya da bilgisi dâhilinde olmadan bilgisayarın çalışma şeklini değiştiren ve kendini diğer dosyaların içerisinde gizlemeye çalışan aslında bir tür bilgisayar programıdır. Virüsün özelliği kendi kendine çalışabilmesi ve çoğalabilmesidir (Anonim, 2017-6).
- *Worm;* Milyonlarca sistemi etkileyebilecek basit bir malware yazılımıdır. Bir bilgisayar solucanı iki parçaya sahiptir; İlk olarak, sistemde kendini kopyalar ve farklı sistemlerde çoğalmaya devam eder. Ardından, bu zararlı yazılımın çoğaltılması sistemin belleğini ve işlem gücünü bozar ve sistem çökmesine neden olur (Kobus, 2016).
- *Trojan;* Truva atı olarak bildiğimiz trojanlar paylaşım dosyalarından veya e-mail aracılığı ile bulaşabilmektedirler. Görünüşte zararsız gibi dursa da içerisinde zararlı kodlar bulundurur. Kullanıcı zararlı yazılımın çalıştığının farkına varmaz. Barındırdığı zararlı kodun amacı kullanıcının erişim hakkını kullanarak koruma sistemini devre dışı bırakıp uzaktan erişimi mümkün kılmak ve dosyalar üzerinde istenilen işlemlerin yapılmasına olanak sağlamaktır.
- *Rootkit;* Kendini en iyi saklayan ve en tehlikeli yazılımlardan olan rootkit programının asıl amacı yayılmak değil saldırganın vereceği komutları çalıştırmaktır.
- *Logic Bombs;* Herhangi bir programın içerisine yerleştirilmiş ve çalışma zamanı planlanmış sisteme zarar verebilecek yazılımlardır. Belirlenen şartlar sağlandığında isminden de anlaşılacağı gibi patlar yani aktif olurlar.
- *Backdoors;* Özellikle internet kullanıcılarına yönelik olan bu saldırı normal kimlik doğrulama prosedürünü atlatarak sızma işlemidir. Yani sisteme gizli erişim için kullanılan gizli bağlantı noktalarıdır. Belli bir kullanıcı tarafından çalıştırılınca veya belli giriş değerleri verilince tetiklenen kodlardır. En çok programcılar tarafından test işlemlerini kolaylaştırmak, hataları düzeltmek ve hata durumunda erişime izin vermek için kullanılır (Vural, 2007).
- *Keylogger*; Kullanıcı adı, şifre gibi kişiye özel gizli bilgileri toplayarak belirtilen noktaya (bu mail adresi olabilir) gönderen programlardır. Kısaca klavyeden yapılan her vuruşu kaydeden ve bu kayıtları kullanıcının kişisel bilgilerini çalmak isteyen saldırganlara gönderen programlardır.

- *Ransomware*; Özellikle mail yolu ile bulaşan ve en yaygını Eylül 2013 yılında ortaya çıkan CryptoLocker olan bir malware türüdür. Saldırgan diskteki kişiye ait dosyaları şifreleyerek kişiden dosyalarına karşılık fidye talebinde bulunur.
- *Browser Hijacker;* Özellikle İnternet Explorer başlangıç sayfasını ve arama işlemlerini saldırganın isteği doğrultusunda yönlendiren register ayarlarını değiştiren zararlı yazılımlardır.
- *Botnet;* Kullanıcının bilgisayarına haberi olmadan saldırgan tarafından yüklenen ve bilgisayarı zombi (saldırgan tarafından sistem açığı bulunarak ele geçirilen bilgisayarlar ve aynı zamanda tüm kişisel bilgiler, iletişim ve veri ağının takip edilmesine açık bilgisayarlardır.) haline getirerek saldırganın direktifleri doğrultusunda çalışmasını sağlayan zararlı yazılımlardır. Kullanıcı zararlı yazılımın çalıştığının ve bilgisayarının kötü amaçlı saldırılar için kullanıldığının farkında değildir. Özellikle DDos saldırılarında etkin olarak kullanılır.

Web uygulamalarına yönelik olan sızma testleri bilgi güvenliği sızma testleri ile aynı mantıktadır. Sızma testleri üç farklı kategoriye ayırabilir.

1.Beyaz-Kutu Sızma Testleri:

Test yapılacak sistem ve ağ hakkında her türlü bilgiye sahip olan yetkili kullanıcının yaptığı test türüdür. Az zahmetli ve hızlıdır. Bu test daha çok iç ağ çalışanlarına ve işten ayrılan daha önce sistem yetkilerini üzerinde bulunduran kişilerin saldırı yapma senaryoları üzerine gerçekleşir.

2.Siyah-Kutu Sızma Testleri:

Bu sızma testi türünde saldırganlar tarafından dışarıdan gelebilecek tüm art niyetli saldırıların bire bir örneğine karşı sistemin direnci ölçülür. Beyaz-Kutunun tam tersi elde sistem hakkında hiçbir veri olmadan dışarıdan herhangi bir saldırganın yapabileceği saldırı gibi yapılan test türüdür. Yani testi yapan bir hacker gibi davranır.

3. Gri-Kutu Testleri:

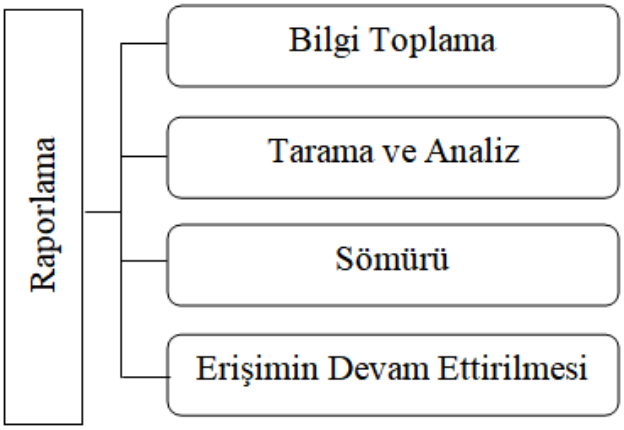
Sistem hakkında sınırlı sayıda bilgi vardır. Gri kutu sızma testi siyah kutu ile beyaz kutu sızma testleri arasında yer alan bir sızma testidir. Kurum iç ağında yer alan sistemler bilgi ve yetki verilmiş kişiler tarafından teste tabi tutulmaktadır. Gri kutu sızma testinde test edilen sistem ya da uygulama, siyah kutu sızma test türüne göre test edilir fakat test işlemi, sistem ya da ağ hakkındaki çeşitli bilgilerle desteklenmektedir.

Genel olarak sızma testleri ve kullanılan yöntemler Tablo 3'de gösterilmiştir.

Tablo 3. Sızma testlerinde kullanılan güvenlik testleri (Yaşar, 2014)

SIZMA TESTLERİ	YÖNTEMLER
Kimlik Doğrulama	Kaba Kuvvet Yetersiz Kimlik Doğrulama Şifre Kurtarma Denetimi
Yetkilendirme	Oturum Bilgisini Tahmin Etme Yetersiz Yetkilendirme Yetersiz Oturum Sonlandırma Oturum Sabitleme
Kullanıcı Taraflı	Siteler Arası Kod Yazma İçerik Sahteciliği
Komut Çalıştırma	Ara Bellek Taşması Dizgi Formatı LDAP Enjeksiyonu İşletim Sistemi Komut Enjeksiyonu SQL Enjeksiyonu SSI Enjeksiyonu XPath Enjeksiyonu
Bilgi Açığa Çıkarma	Dizin Listeleme Bilgi Sızıntısı Yol Takibi Tahmin Edilebilir Kaynak Konumu
Mantıksal	Fonksiyonellik Suiistimalleri Hizmet Aksatma Otomasyon Yetersiz Denetim

Sızma testlerinin amacı kötü niyetli kişilerin yetkisiz erişimlerini engellemek amacıyla zafiyetlerin tanımlanarak giderilmesidir (Vural, 2007). Web sızma testlerinde de kullanılan yöntem örneği Şekil 3.8'de gösterilmiştir.



Şekil 3.8. Sızma testlerinde kullanılan yöntem

Sızma testleri bilgi toplama, zafiyet taraması ve analizi, sömürü, erişimin devam ettirilmesi, raporlama olmak üzere beş aşamadan oluşmaktadır.

3.1.2.1. Bilgi toplama

Bilgi toplama, hedef hakkında olabildiğince bilgi elde etmektir. Bilgi toplama aktif ve pasif olmak üzere ikiye ayrılabilir: Hedefe bağlanarak sunucular, IP adresler ve servisler gibi özelikle ağ bileşenleri hakkında bilgi toplamaya "Aktif" (Fierce, Dig, theHarvester, SubBrute, CeWL gibi yazılımlar) ve hedef ile temas olmadan özellikle internet vasıtasıyla Web sayfaları (Shodan, Google Hack Veri Tabanı, Netcraft gibi siteler) ile elde edilen bilgi toplamaya "Pasif" denir. Aktif bilgi toplamanın pasife göre daha fazla ve etkili bilgi toplama gibi avantajına karşın hedef tarafından fark edilme gibi dezavantajı vardır. Bilgi toplamadaki amacı çalışan sistem ve yazılımların belirlenmesi, IP adresi, çalışan servislerin belirlenmesi, sosyal mühendislik ile bilgi toplama ve belge bulma olarak özetleyebiliriz (Muniz ve Lakhani, 2013). Web açısından, kullanılan Web sunucu uygulamaları ve sürümleri, http sürümü, http metodu, dizin yapısı, dosya tipleri, kullanılan Web Uygulama Güvenlik Duvarı ve vekil sunucu gibi toplanan bilgiler test aşamasında oldukça işe yarayacaktır.

Web uygulamaları ile ilgili toplanacak bilgiler sunucuya gönderilen istek sayesinde olabilmektedir. Sunucu site yapısındaki Header bölümünden aldığı bilgilerle geri cevap göndermektedir. Güvenlik anlayışının gelişmesiyle kullanılan sunucu, işletim sistemi gibi bazı bilgilere erişim engellenmiştir. Fakat bu önlem yeterli olmamaktadır. Her sunucu isteklere farklı tepkiler vermektedir. Kullanılan bilgi toplama araçları ile verilen tepkilere göre hangi sunucu yazılımının kullanıldığı elde edilebilmektedir. Diğer güvenlik önlemleri vekil sunucu kullanımı veya birden fazla sunucu (load balancing) kullanımıdır. Fakat bu önlem sitedeki çerez bilgisinin arama motorunda aranarak gerçek sunucuyu bulma yöntemi ile aşılabilmektedir. Toplanan bilgilerde en önemlileri kullanılan sunucu, işletim sistemi, proxy, firewall, uygulamalar (JavaScript, AJAX, Flash) ve genel yapı (Formlar, dizin yapısı, dosyalar, cookies vs.) hakkında bilgileridir.

3.1.2.2. Zafiyet taraması ve analizi

Toplanan bilgiler çerçevesinde sömürü için kullanılabilecek hatalar veya eksiklikler bulunur, açık portlar belirlenir. İşletim sistemine veya kullanılan herhangi bir programa ait yama eksikliği bir sistem için en önemli zafiyettir (Polat, 2016). Basit veya varsayılan şifre kullanımı, hatalı sistem politikaları, uygulama veya yazılımın tasarımdan kaynaklı sorunlar ve programların güncel olmaması veya ücretsiz elde edilmiş olmasını zafiyete yol açabilecek potansiyel tehditler olarak örneklendirebiliriz. Web uygulamaları için zafiyet taraması, manuel (Kod inceleme, komut satırı vs.) olabildiği gibi popüler olan otomatik zafiyet tarama araçları (Metasploit, nmap komutları, Nessus, Acunetix vs.) yardımıyla da yapılabilir.

3.1.2.3. Sömürü

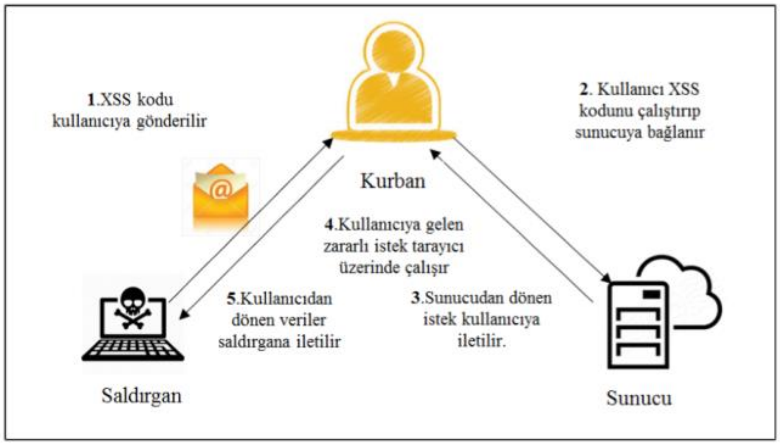
Sömürü, hedef sistem üzerinde kontrolün sağlandığı, süreçteki en önemli aşamadır. Zafiyet tarama araçları yerine burada sömürüye yönelik araçlar (Şifre kırıcı programlar, Metasploit uygulaması vs.) ve exploit adı verilen sömürü kodları kullanılmaktadır. Sömürü saldırgana hedefe sızma veya hedefte zararlı kod çalıştırma imkânı sağlayan, hedef sistemde yüklü programlardaki hataları kullanmadır (Engebretson, 2013).

OWASP 2017 yılı top 10 listesine göre Web güvenliği açısından en yaygın sömürü örnekleri XSS, CSRF, Enjeksiyon yöntemleridir.

3.1.2.3.1. Çapraz betik çalıştırma

Web uygulamalarında en yaygın olan zafiyetlerden birisi Çapraz betik çalıştırma (XSS) zafiyetidir. XSS saldırıları genelde HTML veya JavaScript bileşenlerine yönelik onaylanmamış girişler şeklinde olmaktadır. Bu girişler istek sayfalarının parçasıymış gibi oluşturulur ve istenmeyen etkilere sebep olur (Shahriar, 2011). Çapraz Betik Çalıştırma zafiyeti sonucu özellikle dinamik Web sayfalarında oturum bilgisi elde edilerek veriler üzerinde yetkisiz işlemler gerçekleştirilir. Saldırgan tarafından hazırlanan zararlı kodun kullanıcı tarafından kullanıcının tarayıcısında (hazırlanan URL'yi ziyaret ettirme, çalışan kodları manipüle etme gibi) çalıştırılmasının sağlanmasıyla kullanıcının oturum bilgisinin (cookie) saldırganın eline geçmesi sağlanır. Böylece sunucu ile güven ilişkisi kurulur. Çalışan kodun güvenilirliği gibi tarayıcı güvenlik açığı da XSS için önemlidir. Eğer Web tarayıcısı üzerinde herhangi bir kısıtlamaya gidilmemişse zararlı kod vasıtasıyla tarayıcı tarafından erişilen her türlü hassas veri okunabilir, değiştirilebilir ve e-posta aracılığıyla farklı yerlere iletilebilir veya hizmet aksattırma saldırıları yapılabilir (Vural, 2007). Tarayıcı Sömürü Projesi (The Browser Exploitation Framework Project, BeEF) ile XSS açıklarında faydalanılabilir. HTML kod enjeksiyonu olarak da adlandırılan XSS saldırıları türlerini üç başlık altında toplayabiliriz.

1-Yansıyan XSS: Genellikle yönlendirilen link ziyareti şeklinde gerçekleşen bu saldırıda kullanıcının zararlı kodu kendi tarayıcısında çalıştırması hedeflenir. Çalışma mantığı Şekil 3.9'da gösterilmiştir (Boşal, 2017).



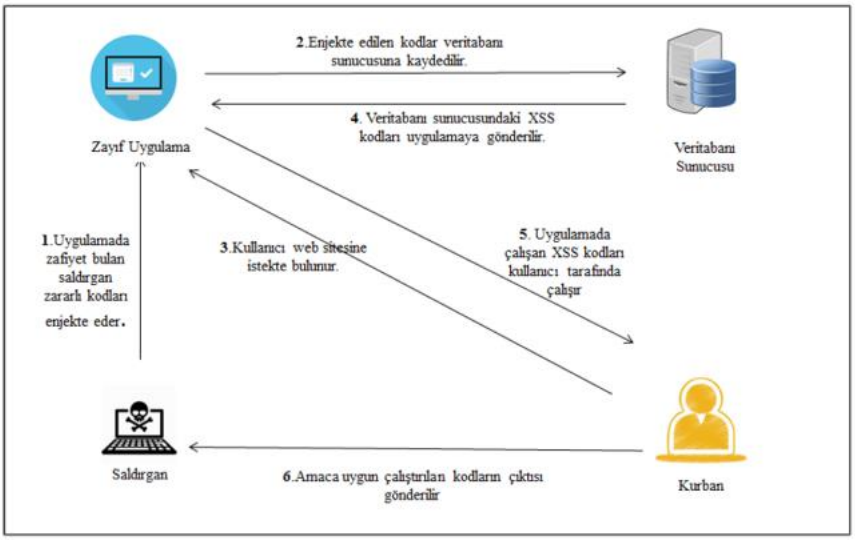
Şekil 3.9. Yansıyan XSS (Boşal, 2017)

Kullanıcıdan tıklanılması istenilen bağlantının JavaScript ile yazılmış kod örneği;

"document.location='http://ornek.com/?cookie='+document.cookie"

şeklinde olup tarayıcıdaki tüm oturum bilgisi "http://ornek.com/" adresine yönlendirilmiştir.

2- Depolanmış XSS: Tarayıcıdan ziyade sunucuya yönelik özellikle veri tabanında değişiklik ile gerçekleşir. Saldırı yapacak kişi Web sitesinde yada forumda yeni bir başlık yada alan açarak zararlı kodları, örneğin "<script>alert (document.cookie)</script>" gibi siteye gömer. Kurbanın hazırlanan yere gelmesi sonucu cookie bilgilerinin çalınması ile yapılan saldırı türüdür (Akyıldız, 2013). Depolanmış XSS çalışma mantığı Şekil 3.10'da gösterilmiştir (Boşal, 2017).



Şekil 3.10. Depolanmış XSS (Boşal, 2017)

3. DOM Tabanlı XSS: DOM (Document Object Model) tabanlı XSS diğer XSS'lerden farklı olarak sunucuya istek göndermez kullanıcının tarayıcısında çalışır. Saldırı için

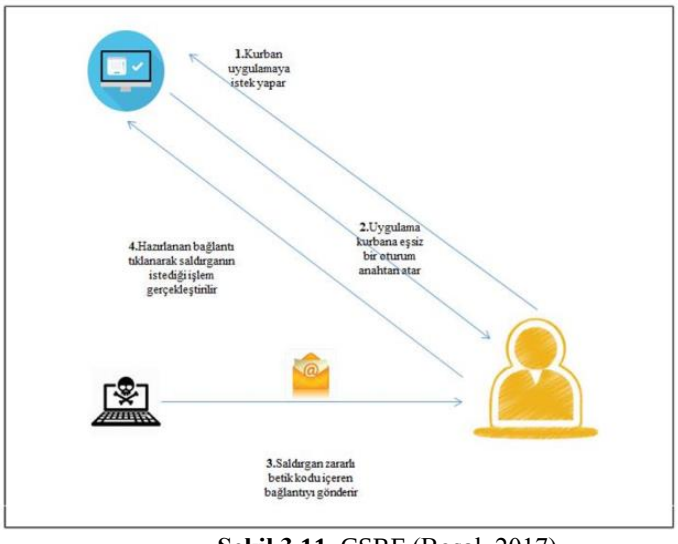
kullanıcının tarayıcısındaki DOM nesneleri (document.write vs.) betik diller vasıtasıyla kullanılır.

HttpOnly çerezleri: Amaç oturumun ele geçirilmesi olan XSS açığında JavaScript ile çerezler istenildiği gibi yönetilebilir. Bu sorunun çözümü için HttpOnly deyimi cookie parametresi olarak kullanılmakta ve özellikle tarayıcıların JavaScript komutlarıyla çerezlere erişimi engellenmektedir. Örnek kullanımı;

"Set-Cookie: Name=Value; expires=Wednesday, 01-Jan-2018 11:00:00 GMT; HttpOnly" gibi Set-Cookie kullanımına HttpOnly eklenmesi şeklindedir.

3.1.2.3.2. Siteler arası istek sahteciliği

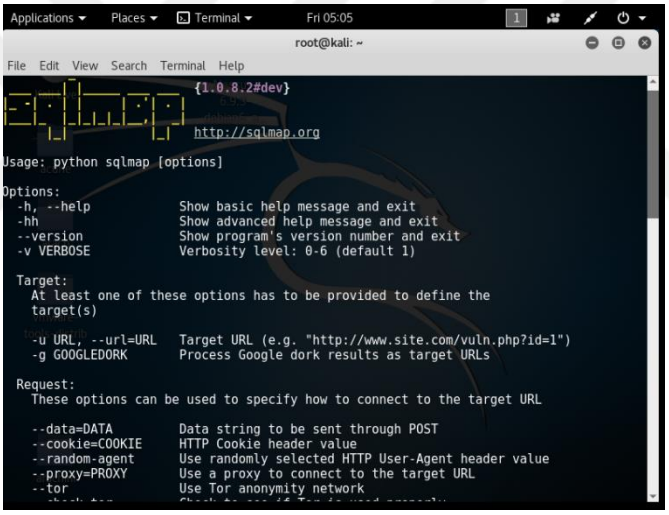
Siteler Arası İstek Sahteciliği (CSRF); son kullanıcının bilgisi dâhilinde olmadan, kullanıcıya kendi hesabı üzerinden işlemler yaptırılmasıdır (Boşal, 2017). Kullanıcıya gönderilen bir linkin tıklanması (bu link resim de olabilir) veya bir formun onaylatılması gibi kullanıcının tarayıcısında istenilen kodun çalışması sonrası önceden açık olan oturum bilgisinin doğrulanması ve bunun sonucunda istenilen saldırıların gerçekleştirilmesidir. Örnek verecek olursak; Kullanıcı bankacılık işlemi yaparken içerisinde zararlı kod veya linkin olduğu ikinci bir sayfayı açıp sayfadaki linke tıklar. Banka sayfasındaki oturum sayesinde zararlı sayfa da banka uygulamasında oturum elde etmiş olur. Bunun sonucu banka uygulamasına erişim sağlanabilir ve istenilen işlemler yaptırılabilir. CSRF çalışma prensibi Şekil 3.11'de gösterilmiştir (Boşal, 2017).



Şekil 3.11. CSRF (Boşal, 2017)

3.1.2.3.3. Sql enjeksiyonu

SQL (Structured Query Language) veri tabanlarında veri alma, silme ve değiştirme gibi işlemler için kullanılan bir dildir. SQL ifadelerini kullanarak yapılan saldırı türü olan SQL Enjeksiyonu LDAP, İşletim Sistemi gibi çeşitleri olan kod enjeksiyonunun en yaygın türüdür ve veri tabanını ele geçirmeye yöneliktir. Bu saldırı veri tabanı kullanan dinamik Web sayfalarına yönelik yapılır ve SQL sorguları kullanılır. SQL enjeksiyonu yöntemi, kullanıcı girdilerine göre SQL cümleleri oluşturan Web sitelerinde, kullanıcı kaynaklı girdilerin doğrulanmaması veya yetersiz doğrulanmasından kaynaklanan zafiyetlerin kullanılarak, SQL cümlelerinin manipüle edilmesidir (Vural, 2007). SQL Enjeksyonu 1=1 her zaman doğrudur mantığına dayanır. SQL Enjeksiyonu manuel yapılabileceği gibi çeşitli SQL saldırılarına kolaylıkla imkân sağlayan Şekil 3.12' de görülen Kali Linux üzerindeki SQLMap programıyla da yapılabilir.



Şekil 3.12. SQLMap programı seçenekleri

SQL Enjeksiyon türlerini üç başlıkta inceleye biliriz (Anonim, 2017-2).

1- In-Bound Enjeksiyon: Yaygın olarak bilinen klasik saldırı türüdür. Saldırı ve alınan sonuç aynı haberleşme kanalı üzerinden gerçekleşir.

- Union: Orijinal SQL sorgusuna başka bir SQL sorgusu eklemek suretiyle gerçekleşir. İki veya daha fazla SELECT deyiminin sonuçlarını tek bir sonuçta birleştirmek için UNION SQL operatöründen yararlanır ve daha sonra bu sonuç, HTTP yanıtının bir parçası olarak döndürülür.

- Hata Tabanlı: Hata tabanlı SQL Enjeksiyonu, veri tabanının yapısı hakkında bilgi edinmek için veri tabanı sunucusu tarafından gönderilen hata iletilerine dayanan bir SQL Enjeksiyon tekniğidir. Hatalar, bir Web uygulamasının geliştirme aşamasında çok yararlı olsa

da, canlı bir sitede devre dışı bırakılmalı veya bunun yerine erişimi kısıtlı bir dosyaya kaydettirilmelidir.

2- Kör (Blind) enjeksiyon: Blind SQL Injection, SQL Injection için gereken SQL cümleciğinin deneme yanılma yoluyla bulunması yöntemine dayanır. Sunucu üzerinde koşan SQL cümleciğinin tamamı bilinemediği zaman veya bazı özel karakterler için filtreleme aşılması gerektiği durumlarda saldırganlar Blind SQL Injection yöntemiyle yüzlerce veya binlerce SQL sorgusunu deneyerek sonuçlar almayı hedeflerler (Muharremoğlu, 2013). Blind SQL enjeksiyonu boolean tabanlı ve zaman tabanlı olmak üzere ikiye ayrılır.

- Boolean tabanlı: Boolean SQL injection, gönderilen mantıksal ifadenin True - False değeri dönme sonucuna göre oluşturulan sorgularla yapılan sql enjeksiyonlarıdır.

- Zaman Tabanlı: Zaman Tabanlı SQL injection da gönderilen sorgunun çalıştırılıp çalıştırılmadığı soru sonucuna göre tespit edilemediğinden dolayı sorgu içine sleep() gibi fonksiyonlar yerleştirilerek sistem cevabının gecikmeye uğrayıp uğramadığına bakılır (Anonim, 2017-7).

3- Out-of-band SQL injection: İstenen bilgi farklı bir veri çekme yöntemi ile elde edilir (Sorgunun sonuçlarının saldırgana eposta ile gönderilmesi gibi).

SQL Enjeksiyonuna karşı yapılabilecekler maddeler halinde:

1- HTTP Metotları ile gönderilen verilerin doğrulanması, girdi kontrollerinin yapılması

2- Hazır komut prosedürleri kullanmak (StoredProcedure)

3- Etkin yetkilendirme yapmak

4- Güvenlik testleri ve kod kontrolleri yapmak

5- Hata mesajlarının ayrıntılı görüntülenmesini engellemek

6- Önemli verileri şifrelemek'dir.

3.1.2.4. Erişimin Devam Ettirilmesi

Bu adım hedefe giriş sağlandıktan sonra izlerin mümkün olduğunca silinip, erişimin arka kapı (backdoors), kök kullanıcı takımı (rootkits), yeni kullanıcı veya meterpreter shell, tünel, yeni ağ erişim kanalı gibi yöntemlerle çok yönlü olarak devam ettirilmesi aşamasıdır.

3.1.2.5. Raporlama

Önceki aşamalarda yapılan testler sonucunda elde edilen bilgilerin yorumlanarak yazıldığı, test sonuçlarının (risk seviyeleri, sistemlere etkileri, önem sıraları, vb.) analiz edildiği, çözümler ve önerilerin yer aldığı dokümanlar ise "Raporlama" aşamasında oluşturulur (Vural, 2007).

3.1.3. Kullanılan Yazılımlar

Yapılan işlemler için Kali Linux 2016 ve Microsoft Windows 8 işletim sistemleri kullanılmıştır. Sitelerle ilgili bilgi toplamak için materyal olarak Shodan ve Netcraft analiz siteleri ve Kali Linux altındaki açık kaynak kodlu Nikto ve Paros uygulamaları kullanılmıştır.

Zafiyet taraması için popüler olan Microsoft Windows platformu üzerinde çalışan Acunetix v10 (*https://www.Acunetix.com* deneme sürümü) programı ve Nessus programının 6.10.5 deneme sürümü (*https://www.tenable.com*) kullanılmıştır.

3.1.3.1. Kali Linux

Linux tabanlı bir işletim sistemi olan Kali Linux, Backtrack 4.0 işletim sisteminin geliştirilmesi sonucu 2013 yılında yayınlanmıştır. İçerdiği geniş araç desteği ile sızma testlerinin vazgeçilmez işletim sistemidir. Kali Linux araçları Şekil 3.13' de gösterilmiştir.



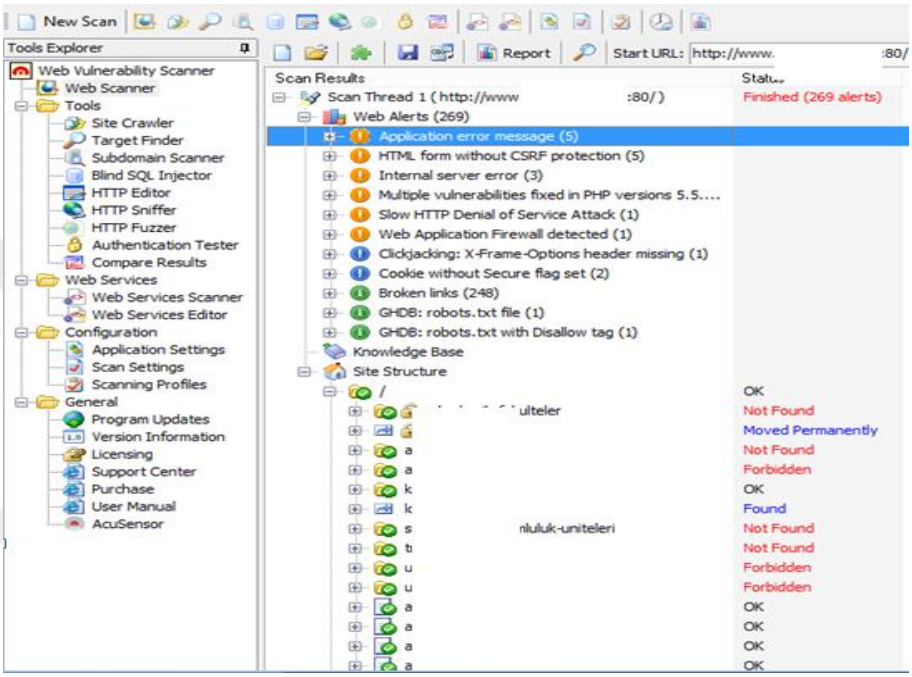
Şekil 3.13. Kali Linux araçları

Şekil 3.13'de görüldüğü gibi Bilgi Toplama, Zafiyet Analizi, Web Uygulama Analizi, Veri tabanı Değerlendirme, Şifre Saldırısı, Kablosuz Ağ Saldırısı, Sömürü Araçları, Ağ

Koklama, Sömürü Sonrası, Aldatma, Raporlama, Sosyal Mühendislik, Sistem Servisleri gibi 14 adet başlık bulunmakta ve her başlıkta ortalama on adet araç bulunmaktadır.

3.1.3.2. Acunetix

Web uygulamalarındaki zafiyetleri tespit ederek güvenlik değerlendirmesi yapmak için kullanılır. Acunetix ayrıca site bilgisi toplama, hedef bulma, blind SQL enjeksiyon, HTTP editor, HTTP koklayıcı, HTTP manipüle, yetki testleri için kullanılabilmektedir. Örnek kullanımı Şekil 3.14'de gösterilmiştir.

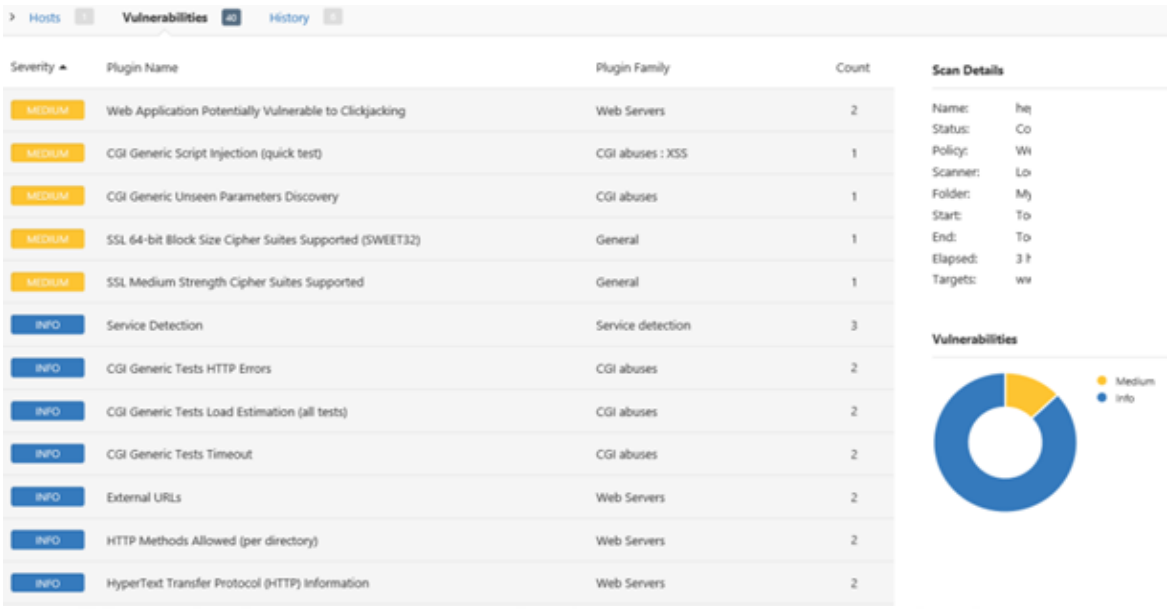


Şekil 3.14. Acunetix ile örnek tarama

Acunetix zafiyetleri Yüksek, Orta, Düşük ve Bilgi şeklinde dört gruba ayırmaktadır. Şekil 3.14'de tarama sonucunda bulunan Orta, Düşük ve Bilgi zafiyetler gösterilmiştir. Ayrıca bulunan zafiyetlerin önlenmesi ile ilgili ipuçları verilmektedir.

3.1.3.3. Nessus

Tenable firması tarafından geliştirilen ev kullanıcıları için ücretsiz olan Nessus programı genel olarak zafiyet taramasında kullanılır. Bilgi toplamak amacıyla da kullanılabilmektedir. Örnek kullanımı Şekil 3.15'de gösterilmiştir.

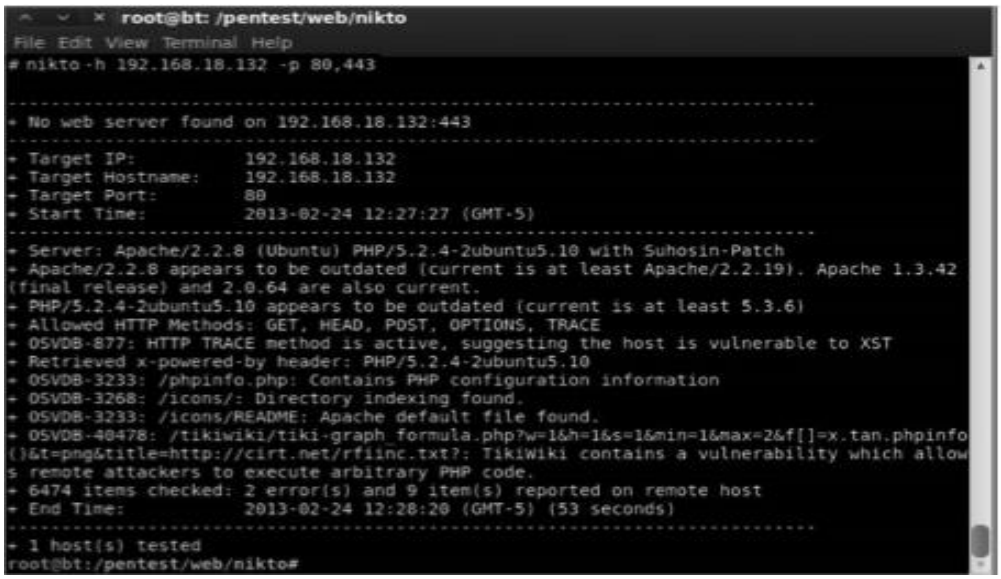


Şekil 3.15. Nessus ile örnek tarama

Nessus, Acunetix gibi zafiyetleri Yüksek, Orta, Düşük ve Bilgi şeklinde dört gruba ayırmaktadır.

3.1.3.4. Nikto

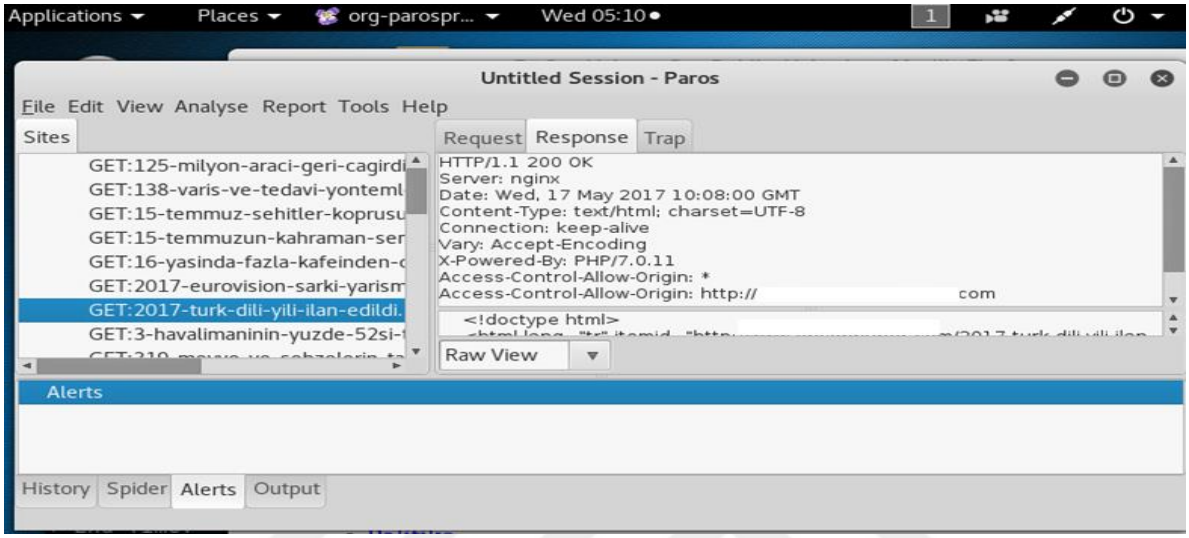
Nikto Web Sunucu zafiyet tarama programıdır. Kali Linux işletim sisteminde mevcut olarak gelmektedir. Bu program sunucu üzerinde çalışan yazılımları tespit etmenin yanında güncellenmemiş ve yama eksiği olan yazılımları bulmak için kullanılır. Kullanım örneği Şekil 3.16'da gösterilmiştir (Engebretson, 2013).



Şekil 3.16. Nikto ile örnek tarama

3.1.3.5. Paros

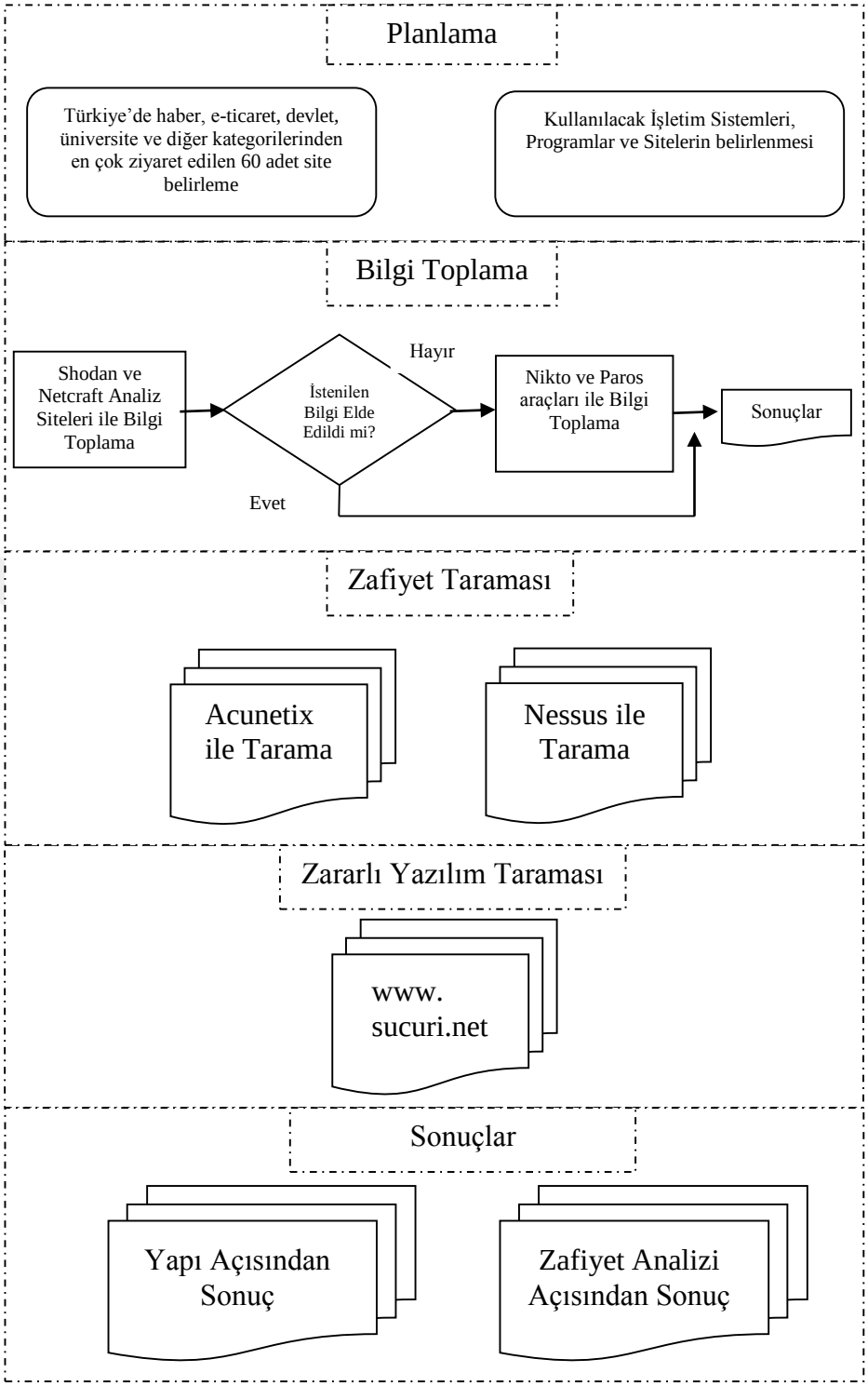
Kali Linux işletim sistemiyle gelen Paros Web uygulama güvenliği analizi ve zafiyet taraması için kullanılmaktadır. Yerel vekil sunucu şeklinde çalışarak trafiğin kendi üzerinden akmasını sağlamakta ve dolayısı ile Web trafiğini detaylı şekilde analiz edebilmektedir. Örnek kullanımı Şekil 3.17'de gösterilmiştir.



Şekil 3.17. Paros örnek kullanımı

3.2. Yöntem

Tez için sızma testi türlerinden siyah-kutu sızma testi temel alınmıştır. Yani elde hiçbir veri olmadan belirlenen sitelerin kamuya açık alanda bilgi toplanmış, zafiyet taraması yapılmıştır. Bilgi toplama işlemi için Pentium i7 işlemcili bir bilgisayar kullanılmıştır. Bu bilgisayara VMware Workstation programının deneme sürümü kurulmuştur. VMware üzerine Microsoft Windows 8 ve Kali Linux 2016 64 bit işletim sistemleri kurulmuştur. Mevcut Kablonet internet altyapısı kullanılarak *www.shodan.io* ve *www.netcraft.com* internet sitelerinde belirlenen siteler tek tek incelenmiştir. Daha sonra Kali Linux üzerindeki Nikto ve Paros Proxy programları kullanılarak siteler tekrar incelenmiştir. Bu şekilde www.shodan.io ve www.netcraft.com sitelerinden elde dilen bilgiler teyit edilmiştir. Zafiyet taraması için Selçuk Üniversitesi Teknoloji Fakültesi bilgisayar laboratuvarı kullanılmıştır. Laboratuvardaki 12 adet bilgisayara Acunetix v10 (*https://www.Acunetix.com*) programının deneme sürümü ve Nessus 6.10.5 (*https://www.tenable.com*) programının deneme sürümü kurulmuştur. Bu 12 bilgisayarda Acunetix programı ile belirlenen her site bir saat süresince taratılmıştır. Aynı işlem Nessus programı kullanılarak yapılmıştır. İzlenen yöntem Şekil 3.18'de gösterilmiştir.



Şekil 3.18. Yapılan çalışmada uygulanan yöntem.

3.2.1. Planlama

Web güvenliği kapsamında Türkiye'deki sitelerin durumu ile ilgili en çok ziyaret edilen sitelerin, Türkiye'deki tüm siteler hakkında genel bir çerçeve oluşturacağı düşüncesiyle çalışma materyali için en çok ziyaretçiye sahip siteler belirlenmiştir. Bu siteler haber, e-

ticaret, devlet, üniversite ve diğer kategorisinde olmak üzere beş farklı gruptan oluşmaktadır. Her grupta 12 adet olmak üzere toplam 60 adet site*www.alexa.com* sitesi istatistikleri temel alınarak belirlenmiştir. Özellikle büyük siteler tercih edilmiş olup bu sitelerin güvenlik alt yapılarının daha sağlam olduğu varsayılarak elimizdeki hazır araçlarla ne tür bilgiler toplanabileceği araştırılmıştır. Küçük sitelerde fazla açık olma olasılığı düşüncesiyle tarama yapılmamıştır. Gruplandırılan sitelerin hangi kategorilerde olduğu Tablo 4'de gösterilmiştir.

Tablo 4. Oluşturulan gruplar

Grup Adı	**Kategori**	**Açıklama**
Grup 1	Haber	
Grup 2	e-ticaret	
Grup 3	Devlet Kurumları	
Grup 4	Üniversite	Devlet Üniversiteleri
Grup 5	Diğer	Portal, Eğlence vs.

İncelenen haber siteleri "Grup-1", e-ticaret siteleri "Grup-2", devlet siteleri "Grup-3", üniversite siteleri "Grup-4" ve diğer siteler "Grup-5" olarak adlandırılmıştır. Üniversite grubunda devlet üniversiteleri, haber ve diğer gurubunda özel siteler incelenmiştir. Diğer grubu portal, eğlence gibi farklı kategoride özel siteleri içermektedir. Belirlenen siteler 3.1.2'de anlatılan sızma testleri temel alınarak incelenmiştir.

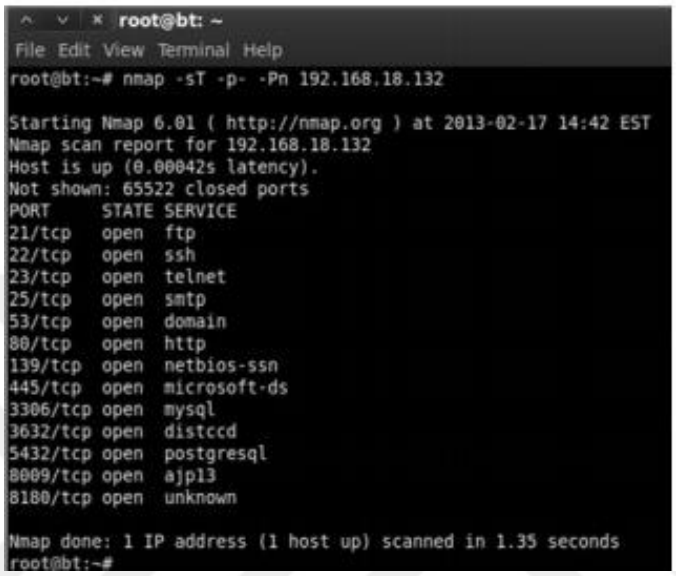
3.2.2. Bilgi toplama

Belirlenen siteler ile ilgili sızma testlerindeki bilgi toplama adımı dikkate alınarak ne tür bilgiler toplanacağı ve nasıl toplanacağı üzerinde çalışılmıştır. Çalışma sonucunda gerekli bilgilerin, var olan tüm siteler hakkında istatistiksel bilgiler tutan Shodan ve Netcraft gibi analiz sitelerinden temin edile bileceği, elde edilemeyen bilgilerin Kali Linux içerisindeki Nikto ve Paros uygulamaları ile elde edilebileceği sonucuna varılmıştır. Web güvenliğinde bilgi toplama için kullanılabilecek araçlar Tablo 5'da gösterilmiştir.

Tablo 5. Bilgi toplama araçları

Bilgi Toplama için Kullanılabilecek Siteler	Bilgi Toplama için Kullanılabilecek Programlar
Shodan.io	Fierce
Netcraft.com	Dig
Whois.net	theHarvester
Ripe.net	SubBrute
Arin.net	CeWL
Robtex.com	Nikto
WhatWeb.net	Proxy Yazılımları
intodns.com	Nmap
	Metasploit

Bilgi toplamak için internet faydalana bilinecek çok önemli bir kaynaktır. Ayrıca, özellikle Kali Linux altında çalışan ve bu iş için yazılmış programlar mevcuttur. Bunlardan en yaygın olarak kullanılan araç nmap dir. Nmap ile hedef sistemin ağ haritası çıkartılarak servislerin durumu, çalışan işletim sistemleri ve portların durumu ile ilgili bilgiler elde edilebilmektedir. Nmap ile örnek bir port taraması Şekil 3.19'da gösterilmiştir.



Şekil 3.19. Nmap port taraması

Şekil 3.19'da görüldüğü gibi nmap ile belirtilen IP adresindeki açık olan portlar tespit edilebilmektedir.

Belirlenen yöntem doğrultusunda sitelerin alt yapı ve teknolojileri hakkında bilgi toplanmıştır. Siteler ilk olarak analiz siteleri olan Shodan ve Netcraft sitelerinde taratılmıştır. Bazı sitelerle ilgili gerekli bilgiler elde edilemeyince Nikto ve Paros uygulamaları kullanılmıştır. Toplanan bilgiler başlıklar halinde Tablo 6'da gösterilmiştir.

Tablo 6. Siteler hakkında toplanan bilgiler

İncelenen Siteler İle İlgili Toplanacak Bilgiler	
1.	Sunucunun Kullandığı İşletim Sistemi
2.	Kullanılan Web Sunucu
3.	Çalışan Platform
4.	Kullanılan Uygulamalar
5.	Kullanılan Güvenlik Duvarı
6.	Lokasyon
7.	Yönlendirmeler

Tablo 6'da görüldüğü gibi sunucunun kullandığı işletim sistemi, kullanılan sunucu programı, çalışan platform ve kullanılan güvenlik duvarı gibi bilgiler hem kullanılan analiz sitelerinden hem de kullanılan nikto ve paros programları aracılığı ile tespit edilmiştir. Kullanılan uygulamalar, lokasyon ve yönlendirmeler bilgisi *www.netcraft.com* sitesi verilerine dayanarak tespit edilmiştir.

3.2.3. Zafiyet taraması

Sızma testlerinde bilgi toplamadan sonraki adım olan zafiyet taraması adımı dikkate alınmıştır. Genel olarak kullanılan Web güvenliği araçları Tablo 7'de gösterilmiştir (Baykara ve ark., 2013).

Tablo 7. Web güvenlik araçları

Web Proxy Araçları	Web Güvenlik Açığı Tarayıcıları	Web Güvenlik Açığı Sömürü Araçları
Paros	Nessus	Arachini
Fiddler	Acunetix	SqlMap
Rat Proxy	Vega	W3af
Sslstrip	Burpsuit	WebGoat
	Zed Attack Proxy	SqlNinja
	Wapiti	Canvas
	WebScarab	
	Skipfish	
	Netsparker	

Tablo 7'de özellikle Web uygulamaları için kullanılan araçlar gösterilmiştir. Buradaki Web Proxy araçları hedef site erişiminin kendi üzerinden olmasını sağlayarak site hakkında bilgi toplama ve zafiyet taraması işlemlerini yapabilmektedir. Sömürü araçları ise zafiyet tarayıcı programlar yardımı ile bulunan açıkların kullanılmasına olanak sağlamaktadır.

Çalışmada zafiyet tarama araçlarından Acunetix v10 (*https://www.Acunetix.com* deneme sürümü) programı ve Nessus programının 6.10.5 deneme sürümü (*https://www.tenable.com*) kullanılmıştır. Acunetix ve Nessus ile yapılan taramalarda her site için aynı süre kullanılmıştır. Bu adımdaki asıl hedef sitelerin zafiyet durumunu taratarak belirgin olarak görülen zafiyetleri tespit etmek olup tüm hedefler Tablo 8'da gösterilmiştir.

Tablo 8. Zafiyet taramaları

İncelenen Siteler İle İlgili Zafiyet Taraması	
1.	Risk Derecelerine Göre Toplam Zafiyet
2.	Detaylı Zafiyet Sonuçları
3.	Karşılaşılan Zafiyetler ve Önlemler

Zafiyetler hem Acunetix hem de Nessusda zayıf, orta, yüksek olarak derecelendirilmiştir. Tablo 8'de görüldüğü gibi ilk olarak derecelerine göre zafiyet adetleri, sonra bulunan

zafiyetlerin detaylı listesi, en son olarak da en çok bulunan zafiyetlerin tanıtılması ve bunlara karşı alınabilecek önlemlerden bahsedilmiştir.

3.2.4. Zararlı yazılım tespiti

Çalışmada belirlenen sitelerin zararlı kod içerip içermediği ile ilgili bir taramanın hazır bir program vasıtasıyla yapılması planlanmıştı. Bu tür bir çalışmanın çevrimiçi siteler tarafından sağlandığı görülünce program kullanmaktan vazgeçilmiştir. Siteler *www.google.com* ile aratılmış ve *www.sucuri.net* sitesi ile kontrol edilmiştir.

4. ARAŞTIRMA SONUÇLARI VE TARTIŞMA

Araştırma sonrası ortaya çıkan sonuçlar iki başlık altında toplanmıştır.

4.1. İncelenen Sitelerin Web Uygulama Yapısı İle İlgili Sonuçlar

İncelenen 60 adet sitenin yapı bakımından sonuçları maddeler halinde açıklanırsa;

1. Sunucunun kullandığı işletim sistemi: Sitelerin kullandığı sunucu işletim sistemleri Tablo 9'da gösterilmiştir.

Tablo 9. Kullanılan sunucu işletim sistemleri

	Win 2003	**Win 2008**	**Win 2012**	**Linux**	**Tespit Edilemeyen**
Grup-1		2		7	3
Grup-2	1	4		3	4
Grup-3			1	2	9
Grup-4		1	1	8	2
Grup-5		3	1	3	5
Toplam	**1**	**10**	**3**	**23**	**23**

WAF veya güvenlik duvarı gibi güvenlik önlemlerinden dolayı incelenen sitelerden %62 sinin kullandığı işletim sistemi tespit edilebilmiştir. İşletim sisteminin tespit edilememesi bir site için güvenlik açısından olumlu bir sonuçtur. Tespit edilemeyen %38 lik kısmı hariç tutulduğunda; Tablo 9'da görüldüğü gibi Grup 4 sitelerinde Linux işletim sistemi %80 oranıyla daha çok tercih edilirken Grup 2 sitelerinde %63 oranıyla Windows işletim sistemi tercih edilmiştir. Microsoft'un desteğini bitirdiği (14 Temmuz 2015) ve özellikle güvenlik yaması alamayacak olan 2003 sunucu kullanan bir adet site tespit edilmiştir. Türkiye geneline bakıldığında %62 Linux, %38 Windows işletim sistemi kullanılmaktadır. Bilgi toplamanın hacker saldırılarının ilk aşaması olduğu düşünülünce Grup-4 sitelerinin yaygın olarak bilgi toplamayı engelleyici önlem almadığı Grup-3ün bu konuda daha bilinçli olduğu görülmüştür.

2. Kullanılan Web sunucu: Sitelerin kullandığı Web sunucular ile ilgili sonuçlar Tablo 10'da gösterilmiştir.

Tablo 10. Kullanılan Web sunucular

	IIS 7.0	**IIS 7.5**	**IIS 8.5**	**Nginx**	**Apache**	**PWS**	**Tespit Edilemeyen**
Grup-1		2	1	4		5	
Grup-2		3	2	2	2		3
Grup-3		2	2	3	1		4
Grup-4	1		2	3	5		1
Grup-5		2	3	5	1	1	
Toplam	**1**	**9**	**10**	**17**	**9**	**6**	**8**

İşletim sistemi tespitinde olduğu gibi alınan önlemlerden dolayı %13 oranında siteden kullanılan Web sunucu bilgisi elde edilememiştir. %87'lik kısımda Web sunucu yazılımı olarak IIS (son sürüm 10.0) tercih eden siteler %38 oranındadır ve tamamı eski sürüm kullanmaktadır. Mevcut bir açığı kullanma kodları gibi sömürü ile ilgili geniş bir veri havuzu olan *www.exploit-db.com*sitesi incelendiğinde özellikle IIS 7.5 ve öncesi sürümlerde sömürü kodlarının (yetkilendirmeyi aşma gibi) olduğu tespit edilmiştir. Tablo 10'da görüldüğü gibi IIS 7.5 ve altı sürümü kullanan 10 adet sitenin sömürüye açık olabileceği değerlendirilmektedir. İncelenen sitelerde, 2010 yılına kadar oldukça yaygın olan Apache programının %17 ile artık çok fazla kullanılmadığı tespit edilmiştir. Nginx (son sürümü 1.13) yazılımının %33 oranla kullanıldığı, %12 oranında PWS yazılımı kullanan sitelerin varlığı görülmüştür.

3. Çalışan Platform: İncelenen Web uygulamanın ana çatı olarak hangi platformu kullandığı Tablo 11'de gösterilmiştir.

Tablo 11. Çalışan platform

	.net	**php**	**Tespit Edilemeyen**
Grup-1	3	9	
Grup-2	7	4	1
Grup-3	8	3	1
Grup-4	3	8	1
Grup-5	6	6	
Toplam	**27**	**30**	**3**

Sitelerin hangi platformda çalıştığının %92'si tespit edilmiştir. Php platformu %53 ve .Net platformu %47 dur.

4. Kullanılan Uygulamalar: Siteler incelendiğinde tüm sitelerin dinamik içerik oluşturmak için kullanılan bir betik dili olan JavaScript ve işaretleme dili olan ve 2014 yılında yayınlanan HTML 5 teknolojilerini kullanmakta olduğu tespit edilmiştir. Ayrıca SSL, XML, Ajax, XHTML ve Flash gibi uygulamaların da kullanıldığı görülmüştür.

5. Kullanılan Güvenlik Duvarı: Güvenlik için donanım kullandığı tespit edilen site sayıları ve kullandıkları donanımlar Tablo 12'de gösterilmiştir.

Tablo 12. Kullanılan güvenlik donanımları

	F5 BigIp	CitrixNetscaler	Güvenlik Donanımı Tespit Edilemeyen
Grup-1	2	2	8
Grup-2	2	2	8
Grup-3	6	3	3
Grup-4		3	9
Grup-5	2	4	6
Toplam	**12**	**14**	**34**

Tablo 12'de görüldüğü gibi özellikle enjeksiyon ve XSS saldırıları için koruyucu olan, yük dağıtıcı olarak belirlenen sunucular arasında trafiği dağıtabilen ve Web uygulama güvenlik duvarı (Web application firewall, WAF) olarak ta kullanılan bu cihazlar hacker saldırılarının ilk aşaması olan ayak izi (footprint) denilen bilgi toplama işlemlerini önemli ölçüde engellemektedir. İncelenen 60 adet siteden %43'ü bu cihazlardan kullanmaktadır. Özellikle Grup-3 sitelerinde %75 oranıyla yaygın olarak kullanıldığı tespit edilmiştir.

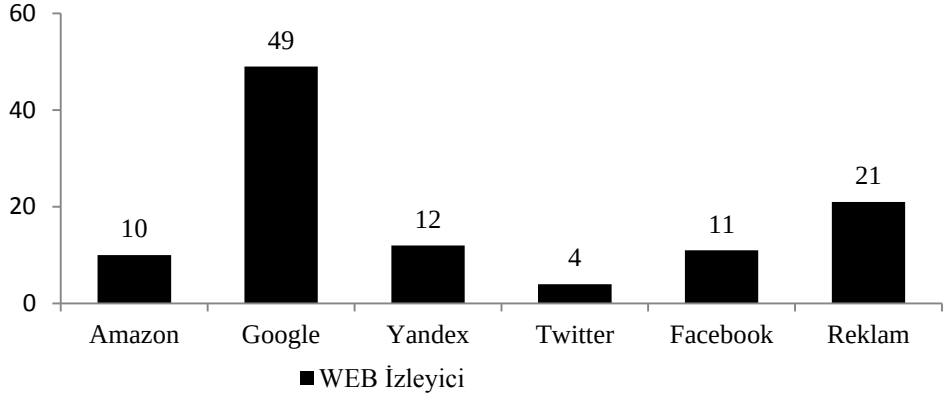
6. Lokasyon: İncelenen Web sitelerin üzerinde yüklü oldukları sunucuların nerede oldukları bilgisi netcraft sitesi verilerine dayanarak Tablo 13'de gösterilmiştir.

Tablo 13. Web sunucunun bulunduğu yer

	Lokal	Bulut Teknolojisi
Grup-1	8	4
Grup-2	9	3
Grup-3	12	
Grup-4	12	
Grup-5	7	5
Toplam	**48**	**12**

Bulut teknolojisini kullanan 12 adet site belirlenmiştir. Grup-3 ve 4 siteleri tamamen kendi lokasyonunda Web sunucu hizmeti sunarken Grup-5 %42 ile bulut hizmeti kullanmaktadır. Bu da devlet ve üniversite sitelerinin bulut teknolojisini tercih etmediğini göstermektedir.

7. Yönlendirmeler: İncelenen sitelerde hangi Web izleyici (trackers) uygulaması kullanıldığı adet olarak Şekil 4.1'de gösterilmiştir.



Şekil 4.1. Sitelerde kullanılan Web izleyici sayıları

Şekil 4.1'de gösterildiği gibi sitelerin %82'si google web izleyici uygulamasını kullanmaktadır. Reklam Web izleyicisi kullanan site oranı %35'dir.

Demografik bilgiler, satın alma alışkanlıkları, ilgi alanları ve daha fazla bilgileri üçüncü taraf siteler ile paylaşan Web izleyici (trackers) uygulaması tüm sitelerde mevcut ve reklam, istatistik/analiz, widget ve CDN (İçerik Dağıtım Ağı) amacıyla kullanılmakta olup sayıları Tablo 14'de gösterilmiştir.

Tablo 14. Web izleyici sayıları

	Analiz	**CDN**	**Widget**	**Reklam**
Grup-1	12	7	11	8
Grup-2	10	7	3	12
Grup-3	4	4	3	-
Grup-4	4	8	1	-
Grup-5	10	8	7	5
Toplam	**40**	**34**	**25**	**25**

4.2. İncelenen Sitelerin Zafiyet Açısından Sonuçları

Zafiyet taramasında Acunetix ve Nessus sonuçları ayrı ayrı detaylandırılmıştır. Derecesine göre sonuçlar sayı bazında verilmiştir.

4.2.1. Risk Derecelerine Göre Toplam Zafiyet

Acunetix uygulamasıyla incelenen sitelerde Yüksek, Orta, Düşük seviyeli zafiyetlerin yanında Bilgi kategorisi adı altında veriler de elde edilmiştir. Elde edilen bu veriler kayda değer bilgiler içermediği için Tablo 15'de gösterilmemiştir.

a) Acunetix Tarama Sonuçları:

Her biri bir saat süren toplam 60 adet sitenin Acunetix programıyla taratılması sonucu bulunan zafiyet bilgileri derecesine göre Tablo 15'de gösterilmiştir.

Tablo 15. Zafiyet dereceleri

	Düşük Zafiyet	**Orta Zafiyet**	**Yüksek Zafiyet**
Grup-1	23	17	-
Grup-2	31	9	-
Grup-3	17	8	-
Grup-4	21	13	-
Grup-5	14	24	-
Toplam	**106**	**71**	**0**

Tablo 15'de gösterildiği gibi tarama sonucunda hiçbir sitede yüksek risk derecesine sahip zafiyet bulunmamıştır. Orta derecede zafiyet alışveriş sitelerinde ve devlet sitelerinde düşük seviyede diğer grubunda en fazla bulunmuştur. Düşük dereceli zafiyet miktarları grup bazında birbirine yakın miktarda bulunmuştur.

b) Nessus Tarama Sonuçları:

Acunetix de olduğu gibi Bilgi kategorisine ait verilere yer verilmemiştir. Nessus ile yapılan her biri bir saat süren toplam 60 adet sitenin taratılmasıyla elde edilmiş veriler ise Tablo 16'da gösterilmiştir

Tablo 16. Zafiyet dereceleri

	Düşük Zafiyet	**Orta Zafiyet**	**Yüksek Zafiyet**
Grup-1	3	26	1
Grup-2	2	10	-
Grup-3	1	12	-
Grup-4	1	13	2
Grup-5	3	27	0
Toplam	**10**	**88**	**3**

Tablo 16'da gösterildiği gibi tarama sonucunda üniversite grubunda 2, haber grubunda 1 adet olmak üzere yüksek risk derecesine sahip zafiyet bulunmuştur. Nessus, Acunetix'in aksine orta derecede zafiyet miktarını fazla, düşük derece zafiyet miktarını az bulmuştur. Orta derece zafiyet bakımından alışveriş siteleri 10 adet ile en iyi durumdadır. Düşük dereceli zafiyet miktarları grup bazında birbirine yakın miktarda bulunmuştur.

Tablo 15 ve 16 incelendiğinde hem Acunetix hem de Nessus incelenen tüm sitelerde zafiyet tespit etmiştir. Düşük zafiyetlerin sitelerde bulunma sebebi olarak, site sahiplerinin bunu önemsemediğinden ziyade siteyi güncel tutmak için kullandıkları teknolojilerden kaynaklandığı düşünülmektedir. Ayrıca gruplardaki sitelerin alt yapısı benzer olduğu için düşük ve orta seviyedeki zafiyetler yakın çıkmıştır.

4.2.2. Grup Bazında Zafiyet Analizi

Acunetix ile inceleme sonuçları Tablo 17'de Nessus ile inceleme sonuçları Tablo 18'de gösterilmiştir.

Elde edilen bulgular sonucunda;

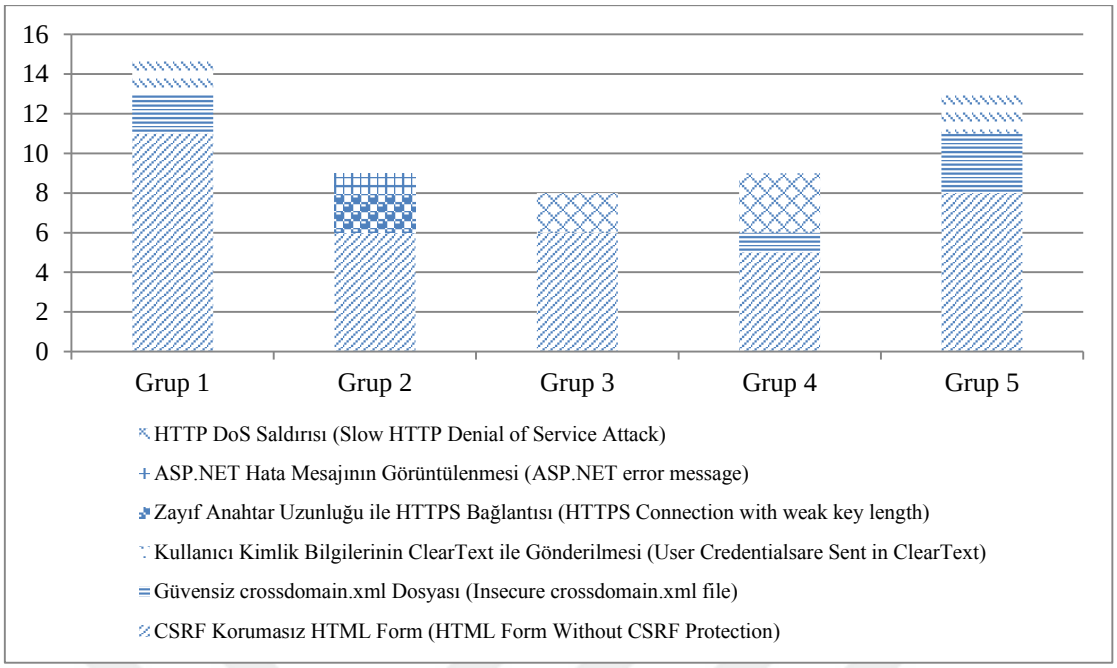
- Kritik seviyede hiçbir zafiyet bulunmamıştır.

- Orta seviye olarak özellikle formlarda CSRF sömürüsüne sebep olabilecek olan "HTML Form Without CSRF Protection" zafiyeti tüm gruplarda ve sitelerin %60'ında bulunmuştur.

- Düşük seviye olarak Tablo 17 incelendiğinde bulunan tüm risklerin büyük bir oranını Iframe/frame kullanımından kaynaklı istenmeyen yönlendirmeye sebep olan "Clickjacking:X-Frame-Option Header Missing" eksikliğinin oluşturduğu, tüm gruplarda ve sitelerin %80'inde olduğu tespit edilmiştir. Çerez kullanımı ile ilgili sadece sunucu erişimine izin veren "HTTPOnly" zafiyetinin tüm siteler bazında %50 oranında olduğu gözlemlenmiştir. Acunetix programı ile tarama sonucunda en çok karşılaşılan ilk üç zafiyet grup bazında orta seviyede Tablo 18'de, düşük seviyede Tablo 19'da gösterilmiştir.

Tablo 17. Acunetix ile inceleme sonuçları

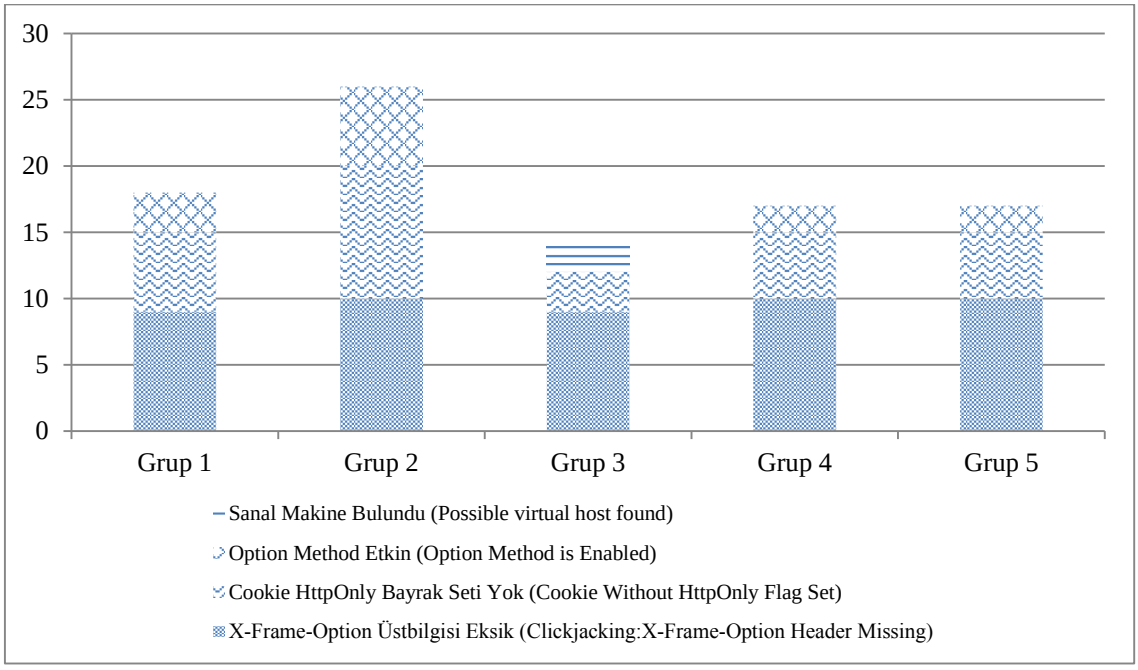
	Risk Derecesi	**ACUNETİX**	
		Zafiyet Adı	Sayı
Grup-1	Yüksek	-	
	Orta	·HTML Form Without CSRF Protection ·Insecure crossdomain.xml file ·User Credentialsare Sent in ClearText ·elmah.axd Information Discloser ·Slow HTTP Denial of Service Attack	11 2 2 1 1
	Düşük	·Clickjacking:X-Frame-Option Header Missing ·Cookie Without HttpOnly Flag Set ·Option Method is Enabled ·ASP.NET version Discloser ·Possible virtual host found	9 6 3 2 3
Grup-2	Yüksek	-	
	Orta	·HTML Form Without CSRF Protection ·ASP.NET error rmessage ·HTTPS Connection with weak key length	6 1 2
	Düşük	·Clickjacking:X-Frame-Option Header Missing ·Cookie Without HttpOnly Flag Set ·Option Method is Enabled ·ASP.NET version Discloser ·Possible virtualhost found	10 10 6 4 1
Grup-3	Yüksek	-	
	Orta	·HTML Form Without CSRF Protection ·Slow HTTP Denial of Service Attack	6 2
	Düşük	·Clickjacking:X-Frame-Option Header Missing ·Cookie Without HttpOnly Flag Set ·Sesion cookies coped to parent domain ·Login page password-guessing attack ·Possible virtual host found ·File Upload	9 3 1 1 2 1
Grup-4	Yüksek	-	
	Orta	·HTML Form Without CSRF Protection ·Insecure crossdomain.xml file ·Slow HTTP Denial of Service Attack ·Same site scripting ·ASP.NET error message ·User Credentialsare Sent in ClearText ·Apache httpOnly cookie disclosure	5 1 3 1 1 1 1
	Düşük	·Clickjacking:X-Frame-Option Header Missing ·Cookie Without HttpOnly Flag Set ·Possible sensitive directories ·ASP.NET version Discloser ·Option Method is Enabled ·File Upload ·Trace Method is Enabled	10 5 1 1 2 1 1
Grup-5	Yüksek	-	
	Orta	·HTML Form Without CSRF Protection ·User Credentialsare Sent in ClearText ·Insecure crossdomain.xml file ·Same Site Scripting	8 2 3 1
	Düşük	·Clickjacking:X-Frame-OptionHeaderMissing ·Cookie Without HttpOnly Flag Set ·Option Method is Enabled ·Possible virtual host found ·Sesion cookies coped to parent domain ·File Upload ·Trace Method is Enabled ·ASP.NET version Discloser	10 5 2 2 1 2 1 1



Şekil 4.2. Acunetix taraması sonucu orta seviyede en çok karşılaşılan zafiyetler

Şekil 4.2. incelendiğinde Acunetix tarama sonucuna göre orta seviyede en çok görülen ilk üç zafiyet ve OWASP top 10 zafiyet listesindeki karşılığı;

- HTML Form Without CSRF Protection → CSRF zafiyeti,
- Insecure crossdomain.xml file → Korumasız uygulama programlama ara yüzleri (API)'ler
- Slow HTTP Denial of Service Attack → Yetersiz Saldırı Koruması şeklindedir.



Şekil 4.3. Acunetix taraması sonucu düşük seviyede en çok karşılaşılan zafiyetler

Şekil 4.3' de görüldüğü gibi Acunetix tarama sonucuna göre düşük seviyede en çok görülen ilk üç zafiyet " X-Frame-Option Üst Bilgisi Eksik (Clickjacking:X-Frame-Option Header Missing), Cookie HttpOnly Bayrak Seti Yok (Cookie Without HttpOnly Flag Set) ve Option Metot Etkin (Option Method is Enabled)" şeklindedir.

Tablo 18. Nessus ile inceleme sonuçları

	Risk Derecesi	**NESSUS**	
		Zafiyet Adı	Sayı
Grup-1	Yüksek	·PHP 7.0.x < 7.0.12 Multiple Vulnerabilities	1
	Orta	·Web Application Potentially Vulnerable to Clickjacking ·.bash_history Files Disclosed via Web Server ·PHP expose_php Information Disclosure ·CGI Generic XSS ·CGI Generic HTML Injections ·CGI Generic Cookie Injection Scripting ·IIS Detailed Error Information Disclosure	10 1 1 5 5 3 1
	Düşük	·Web Server Transmits Cleartext Credentials ·Web Server Propfind Method Internal IP Disclosure	2 1
Grup-2	Yüksek		-
	Orta	·Web Application Potentially Vulnerable to Clickjacking ·CGI Generic HTML Injections ·CGI Generic XSS	8 1 1
	Düşük	·Web Server HTTP Header Internal IP Disclosure ·Web Server Transmits Cleartext Credentials	2 1
Grup-3	Yüksek		-
	Orta	·Web Application Potentially Vulnerable to Clickjacking ·CGI Generic XSS ·PHP expose_php Information Disclosure ·WordPress User Enumeration ·ASP.NET Debug Method Enabled	8 1 1 1 1
	Düşük	·Web Server Transmits Cleartext Credentials	1
Grup-4	Yüksek	·PHP 7.0.x < 7.0.16 Multiple Vulnerabilities ·PHP Unsupported Version Detection	1 1
	Orta	·Web Application Potentially Vulnerable to Clickjacking ·PHP expose_php Information Disclosure ·Git Repository Served by Web Server ·HTTP TRACE / TRACK Methods Allowed ·ASP.NET Debug Method Enabled ·CGI Generic XSS ·CGI Generic HTML Injections	6 1 1 1 1 1 1
	Düşük	·Web Server Transmits Cleartext Credentials	1
Grup-5	Yüksek		-
	Orta	·Web Application Potentially Vulnerable to Clickjacking ·CGI Generic XSS ·CGI Generic Path Traversal ·ASP.NET Debug Method Enabled ·PHP expose_php Information Disclosure ·CGI Generic HTML Injections ·CGI Generic Cookie Injection Scripting ·Backup Files Disclosure ·HTTP TRACE / TRACK Methods Allowed ·PHP expose_php Information Disclosure	7 5 2 1 1 5 1 1 2 2
	Düşük	·Web Server HTTP Header Internal IP Disclosure ·Web Server Transmits Cleartext Credentials	1 2

Bulunan sonuçlar incelendiğinde;

- Grup-1 ve Grup-4'de kullanılan PHP sürümünün eski olmasından kaynaklı üç adet kritik seviye zafiyet tespit edilmiştir.

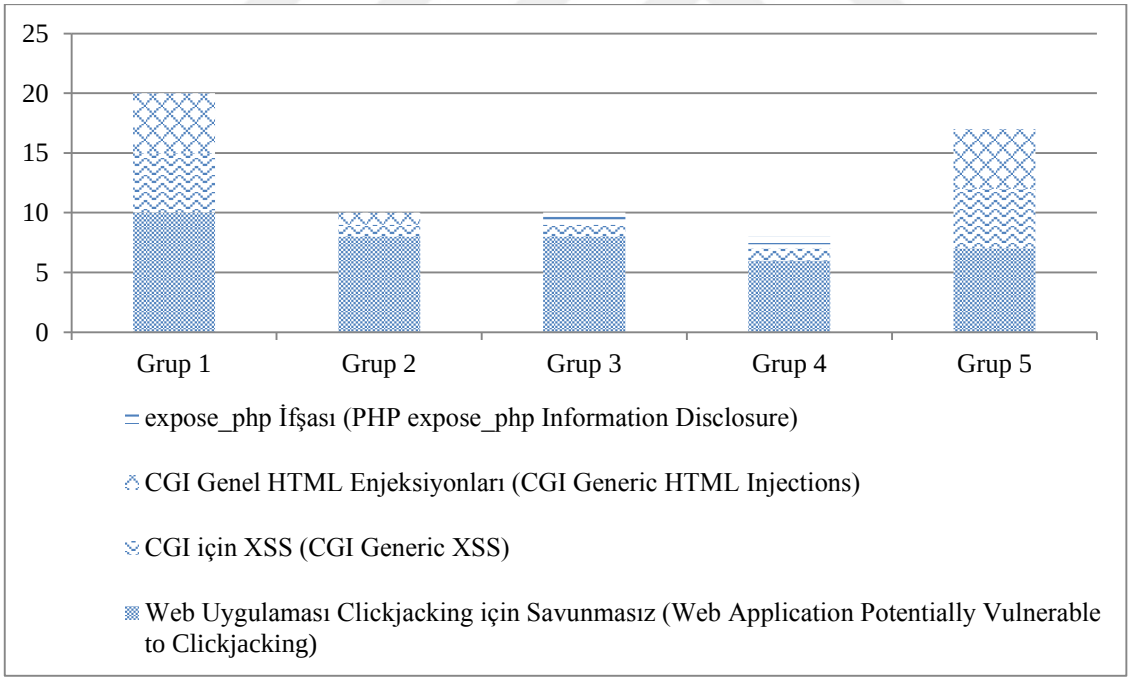
- Orta seviye zafiyet olarak, Acunetix taramasında düşük seviye tehdit olarak görülen ve istenmeyen yönlendirmelere sebep olan "Web Application Potentially Vulnerableto Clickjacking" zafiyeti tüm sitelerin %65'inde görülmüştür.

- CGI Generic ile ilgili zafiyetler orta seviyede ikinci en çok karşılaşılan zafiyet olmuştur.

-Düşük seviyeli kullanıcı bilgilerinin kriptosuz gönderimi olan "Web Server Transmits Cleartext Credentials" zafiyeti tüm gruplarda ve toplam 8 adet sitede tespit edilmiştir.

- Acunetix programının bulduğu "Header, Cookie, Method" kullanımı ile ilgili düşük seviyeli zafiyetler Nessus programında tehdit olarak değil bilgi şeklinde verilmiştir.

Nessus programı ile tarama sonucunda en çok karşılaşılan ilk üç zafiyet grup bazında orta seviyede Şekil 4.4' de düşük seviyede Şekil 4.5' de gösterilmiştir.



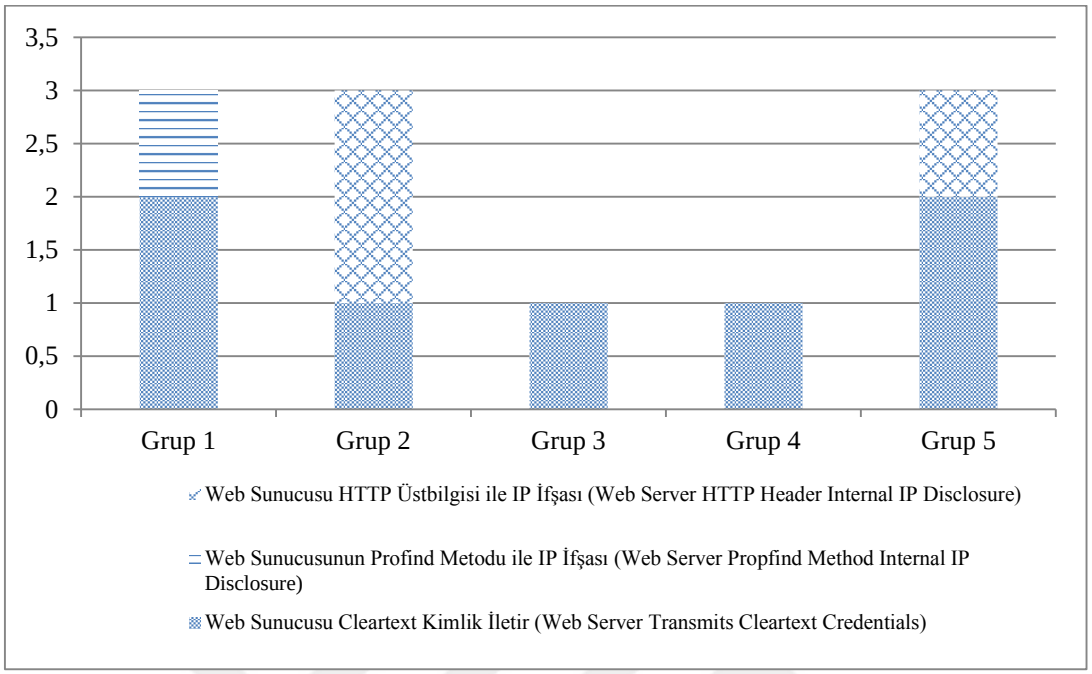
Şekil 4.4. Nessus taraması sonucu orta seviyede en çok karşılaşılan zafiyetler

Şekil 4.4' de görüldüğü gibi Nessus tarama sonucuna göre orta seviyede en çok görülen ilk üç zafiyet ve OWASP top 10 zafiyet listesindeki karşılığı;

- Web Application Potentially Vulnerable to Clickjacking → hijacking zafiyeti,

- CGI Generic XSS → XSS zafiyeti,

- CGI Generic HTML Injections → Enjeksiyon zafiyeti şeklindedir.



Şekil 4.5. Nessus taraması sonucu düşük seviyede en çok karşılaşılan zafiyetler

Şekil 4.5 incelendiğinde Nessus tarama sonucuna göre düşük seviyede en çok görülen zafiyetler " Web Sunucusunun Cleartext ile Kimlik İletmesi (Web Server Transmits Cleartext Credentials) ve Web Sunucusunun HTTP Üstbilgisi ile IP İfşası (Web Server HTTP Header Internal IP Disclosure)" şeklindedir.

4.2.3. Karşılaşılan Zafiyetlere Karşı Önlemler

Acunetix ve Nessus ile yapılan tarama sonucunda bazı zafiyetlerin yaygın olarak tüm gruplarda görüldüğü tespit edilmiştir.

- CSRF Koruması Olmayan HTML Form (HTML Form Without CSRF Protection): CSRF koruması olmayan bir form olduğunda bu zafiyet görülür. Bir saldırgan, bir Web uygulamasının kullanıcılarını kendi seçtiği eylemleri yürütmeye zorlayabilir. Başarılı bir CSRF istismarı, son kullanıcı verilerini tehlikeye atabilir. Hedeflenen son kullanıcı yönetici hesabı ise, bu tüm Web uygulamasını tehlikeye düşürebilir. Formlarda POST metodu kullanmak, XSS açığının olmadığından emin olmak, formlarda bir CSRF anahtarı, CAPTCHA (İnsan ve Bilgisayar Ayrımı Amaçlı Tam Otomatik Genel Turing Testi) veya ben robot değilim uygulamalarını kullanmak alınabilecek önlemlerdir.

- Clickjacking: X-Frame-Option Üstbilgisi Eksik (Clickjacking:X-Frame-Option Header Missing): Bir Web kullanıcısının görünüşte zararsız Web sayfalarını tıkladığını

sanarak aslında farklı bir şey üzerine tıklaması, böylece potansiyel olarak gizli bilgilerin ortaya çıkması veya bilgisayarınızın kontrolünün ele geçirilmesi tekniğidir. Sunucu, X-Frame-Options başlığını döndürmediği zaman meydana gelir. X-Frame-Options yanıt başlığı bir tarayıcıya bir frame veya iframe içinde bir sayfa oluşturmasına izin verilip verilmeyeceğini belirtmek için kullanılabilir. Siteler, içeriklerinin diğer sitelere yerleştirilmemesini sağlamak ve tıklama saldırılarını önlemek için bunu kullanabilir. Bu problemden kurtulmak için Web sunucusu bir X-Frame-Options başlığı içerecek şekilde yapılandırılmalıdır. Bu üç şekilde olabilir.

1- X-Frame-Options: DENY

2- X-Frame-Options: SAMEORIGIN

3- X-Frame-Options: ALLOW-FROM https://example.com/

Bu problemi önlemek için örnek olarak IIS kullanan bir platformda yapılandırmada `Web.config` dosyasına eklenen X-Frame-Options başlığı (Acunetix);

```
<system.WebServer>
  ...

<httpProtocol>
<customHeaders>
<add name="X-Frame-Options" value="SAMEORIGIN" />
</customHeaders>
</httpProtocol>

  ...
</system.WebServer
```

şeklinde gösterilebilir.

-HttpOnly Bayrak Seti Olmayan Cookie Kullanımı (Cookie Without HttpOnly Flag Set): Çerezlerde HTTPOnly bayrağı ayarlanmadığında ortaya çıkar. Bir tanımlama bilgisi HTTPOnly bayrağıyla ayarlandığında, tarayıcıya, tanımlama bilgisine yalnızca sunucu tarafından erişilebileceğini ve istemci tarafı komut dosyaları tarafından erişilemeyeceğini bildirir. Bu, oturum tanımlama bilgileri için önemli bir güvenlik korumasıdır. Bunu önlemek için tanımlama bilgisi için HTTPOnly bayrağı ayarlanmalıdır. Bunun için Web.config dosyasına;

```
<httpCookieshttpOnlyCookies="true" …> yazılması veya C# kodu olarak;
HttpCookiemyCookie = newHttpCookie("myCookie");
myCookie.HttpOnly = true;
Response.AppendCookie(myCookie);
```

Yazılması yeterlidir.

- Option Metodun Etkin Olması (Option Method is Enabled): Web sunucusunda etkinleştirilmiş OPTION metodu ayrıcalıklı GET isteklerinin yetkisiz olarak görülmesini sağlar. Devre dışı bırakılması gerekir.

- ASP.NET Versiyonunun İfşası (ASP.NET version Discloser): Web uygulaması tarafından döndürülen HTTP cevapları, X-AspNet sürümü adlı bir başlık içerir. Bu üst bilginin değeri, ASP.NET'in hangi sürümünün kullanıldığını belirlemek için Visual Studio tarafından kullanılır. Bu gerekli değildir ve devre dışı bırakılmalıdır. Web.config dosyasına;

```
<System.Web>
<httpRuntimeenableVersionHeader="false" />
</System.Web>
```

Yazılarak devre dışı bırakılabilir.

- CGI Kullanımına Bağımlı Zafiyet (CGI Generic): CGI programı Web Servisleri ile bu servislerin dışındaki programlar arasında etkileşim platformu oluşturmak için geliştirilmiş bir standarttır. Bu zafiyet uzak Web sunucusunun XSS, HTML ve Çerez Enjeksiyonu (Cookie Injections) zafiyetlerine sebep olabilecek CGI scriptleri içerdiğini gösterir. Bunu önlemenin en önemli adımı güncelleme yapmaktır.

- Web Sunucunun Kimlik Bilgilerini Cleartext ile Göndermesi (Web Server Transmits Cleartext Credentials): Uzak Web sunucusu, şifre bilgilerini düz metin şeklinde ileten form alanı içerdiği zaman bu uyarı alınır. Bir saldırgan, Web tarayıcısı ile Web sunucusu arasındaki trafiği dinleyerek geçerli kullanıcıların oturum bilgilerini ve şifrelerini alabilir. Bunu önlemek için HTTPS kullanılmalıdır.

4.3. İncelenen Sitelerin Zararlı Yazılım Açısından Değerlendirilmesi

Çevrimiçi hizmet veren Sucuri Site Check sitesi girilen herhangi bir sitenin spam, malware gibi zararlı yazılım içerip içermediğini kontrol edebilmektedir. Ayrıca google arama motoru da bu analizi yapabilmektedir. Ziyaret edilmek istenen site google arama motorunda aratıldığı zaman sitenin zararlı olup olmadığı ile ilgili bilgi elde edilebilir. Sucuri Site Check ile incelenen tüm siteler taratılmış hiçbir sitede kullanıcıyı tehdit edecek zararlı yazılım tespit edilmemiştir.

5. SONUÇ VE ÖNERİLER

5.1. Sonuç

Çalışmanın konusu olan Web güvenliği analizi için gerekli olan bilgi güvenliği, Web Güvenliği, sızma testleri ile ilgili temel bilgiler derlenmiş bu konularla ilgili faydalanabilecek programlardan ve çevrimiçi sitelerden bahsedilmiştir. Sıradan kullanıcı olarak bir site hakkında halka açık alanda ne gibi bilgilerin toplanabileceği ve ne gibi bir zafiyet taramasının yapılabileceği gösterilmiştir.

Yapılan çalışma Türkiye'deki en çok ziyaret edilen siteler için, gerek kullandıkları teknolojiler, gerekse zafiyetleri açısından genel bir şablon oluşturmakta, yapı ve eksiklikleri görebilmek adına örnek teşkil etmektedir. Yapılan çalışma sonucunda ülkemizde hangi programların daha çok rağbet gördüğü, teknolojik olarak nelerin tercih edildiği, yaygınlaşmakta olan bulut teknolojisine olan ilgi gibi konular hakkında temel bilgilere erişilmiştir. Bilgi toplamanın Tablo 12'de görüldüğü gibi %43 oranında önemsenmediği görülmüştür.

Web uygulamaları gerek herkese açık olması gerek zaman ve mekândan bağımsız olması sebebiyle güvenlik açıklarının büyük bir bölümünü oluşturmaktadır. Herkesin erişebileceği zafiyet tarama araçları kullanılarak ülkemiz sitelerinde domain dışından yapılan bir taramayla nasıl bir zafiyet haritasına ulaşılabileceği gösterilmiştir. İncelenen sitelerde eski program kullanma dışında kritik seviyede bir zafiyet görülmemiştir. İleri seviye saldırganların faydalanabileceği orta ve düşük seviyede zafiyetlerin her sitede mevcut ve göz ardı edilmeyecek sayıda olduğu belirlenmiştir.

5.2. Öneriler

- Bilgi güvenliği ve Web Güvenliği konuları göz ardı edilmemeli özellikle kurumsal kullanıcıların BGYS oluşturması ve uygulaması önerilmektedir.

- Web uygulamaları, olası saldırıları veya tehditleri önceden belirlemek, eksikleri görebilmek ve bu doğrultuda önlemler alabilmek için belirli aralıklarla sızma testine tabi tutulmalıdır.

-İncelenen sitelerde özellikle Grup-1 ve Grup-4'te yüksek risk seviyesine sahip zafiyetlerin oluşmasına sebep olan güncel olmayan yazılım kullanımı tespit edilmiştir. Yazılımların güncel olması ve gerekli yama ve güncellemelerinin yapılması konusu oldukça önemlidir.

- Sitelerin OWASP Top 10 listesinde belirtilen zafiyetlere karşı manuel veya program aracılığı ile kontrol edilmesi yaygın zafiyetlere karşı önlem almak için gereklidir.

- WAF kullanan sitelerden bilgi toplamanın güç olduğu tespit edilmiştir. Saldırılar için gerekli olan bilgi toplamanın önüne geçmek için WAF kullanımı önerilmektedir.

- Düşük seviye tehditlerde “Header, Cookie, Method” kullanımından kaynaklı zafiyetlerin tüm gruplarda yaygın olduğu görülmüştür. Önemsiz gibi dursa da bu konuda önlem alınması gerektiği değerlendirilmektedir.

- Orta seviyede görülen CSRF sömürü tehdidine engel olmak için sitelerde CSRF jeton veya CAPTCHA veya ben robot değilim uygulamalarının kullanımı önerilmektedir.

KAYNAKLAR

Ajaj, O., 2013, Modeling and analysis of security standards for web services and cloud computing *Florida Atlantic University* Boca Raton, FL 1-234.

Akyıldız, M. A., 2013, Siber güvenlik açisindan sizma testlerinin uygulamalar ile değerlendirilmesi, Yüksek Lisans Tezi, *Süleyman Demirel Üniversitesi*, Isparta, 1-143.

Anonim, 2017, OWASP 2017 Top 10 Tehdit Listesi, https://www.owasp.org/index.php/Top_10_2017-Top_10 [21 Eylül 2017].

Anonim, 2017-2, SQL Enjeksiyonu, https://www.Acunetix.com [30 Ekim 2017].

Anonim, 2017-3, İstatistikler, https://www.nttsecurity.com [20 Kasım 2017].

Anonim, 2017-4, Web İstemci Çalışma Mantığı, https://www.safaribooksonline.com/library/view/learning-php/9780596514013/ch01.html [25 Kasım 2017].

Anonim, 2017-5, WAF Çalışma Mantığı, https://www.drizgroup.com/how-web-application-firewall-works.html: [25 Kasım 2017].

Anonim, 2017-6, Virüs, http://www.bidb.itu.edu.tr [10 Aralık 2017].

Anonim, 2017-7, Zaman Tabanlı SQL Enjeksiyonu, http://www.lifeoverpentest.com [10 Aralık 2017].

Anonim, 2017-8, Risk Yönetim Aşamaları, [10 Eylül 2017].

Anonim, 2017-9, İstatistikler, http://www.agcs.allianz.com: [15 Eylül 2017].

Anonim, 2017-10, BTK 2017 Verileri, https://www.btk.gov.tr: [10 Ekim 2017].

Anonim, 2017-11, Kaspersky 2017 Güvenlik Raporu, https://www.kaspersky.com/: [13 Kasım 2017].

Arsoy, S., 2014, E-devlet web sİtelerİnİn kullanilabİlİrlİk yönünden standartlara ve rehberlere göre değerlendİrİlmesİ, *Yıldız Teknik Üniversitesi*, İstanbul, 1-89.

Atıcı, İ., 2015, Collection and classification of javascript libraries included in website, Master of Science, *Izmir Institute of Technology*, İzmir, 1-99.

Baykara, M., Daş, R. ve Karadoğan, İ., 2013, Bilgi güvenliği sistemlerinde kullanilan araçlarin incelenmesi. International Symposium on Digital Forensics and Security. Elazığ**:** 231-239.

Boşal, S., 2017, Kamuda bilgi güvenliği ve iller bankasi a.ş. örneği, Uzmanlık Tezi, *İller Bankasi Anonim Şirketi* Ankara, 1-109.

Canbek, G. ve Sağiroğlu, Ş., 2006, Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme, *Politeknik Dergisi*, 9 (3), 165-174.

Cova, M., 2010, Taming the malicious web: Avoiding and detecting web-based attacks, Doctor of Philosophy, *University Of California* Santa Barbara, 1-277.

Çetinkaya, M., 2008, Bilgi güvenliği yönetim sistemi altyapisinin değerlendirilmesi için bir test araci geliştirilmesi, Yüksek Lisans Tezi, *İstanbul Kültür Üniversitesi*, İstanbul, 1-71.

Dhingra, T., 2015, A Review on Web Application Security *IJCSET*, 5 (5), 127-130.

Doğan, S., 2013, Web application tesiing: A systematic literature review, *The Middle East Technical University* Ankara, 1-105.

Doupe, A. L., 2014, Advanced automated web application vulnerability analysis, *University Of California* Santa Barbara, 1-228.

Endraca, A., King, B., Nodalo, G., Maria, M. S. ve Sabas, I., 2013, Web application firewall (WAF), *International Journal of e-Education, e-Business, e-Management and e-Learning*, 3 (6), 451-455.

Engebretson, P., 2013, The Bascis of Hacking and Penetration Testing, *USA*, Syngress p.

Eskiyörük, D., 2007, Risk yönetim süreci kilavuzu, *Ulusal Elektronik Ve Kriptoloji Araştirma Enstitüsü*, BGYS-0004, 1-27.

Evrin, V. ve Demirer, M., 2011, Kurumsal bilgi güvenliği süreç çalişmalari:ISO/IRC-27001 örneği. IV. Ağ Ve Bilgi Güvenliği Sempozyumu. Ankara**:** 25-32.

Fung, P. H. A., 2014, Mitigations of web application security risks, *The Chinese University of Hong Kong*, Hong Kong, 1-163.

Giannini, N. J., 2015, Vulnerable web application framework, Master Of Science, *University Of Rhode Island* Kingston, 1-79.

Gökçay, G., 2014, Identifiying web application vulnerability scanning tools using ip flow information, *Fatih Üniversitesi*, İstanbul, 1-67.

Haque, S., 2016, Web server vulnerability analysis in the context of transport layer security (TLS), *IJCSI International Journal of Computer Science Issues*, 13 (5), 11-19.

Hassan, M., 2013, Toward automated discovery of web application security vulnerabilities, *California State University*, California, 1-59.

Jnena, R. M. F., 2013, Modern approach for web applications vulnerability analysis *The Islamic University of Gaza* Gaza, 1-94.

Karabacak, B. ve Özkan, S., 2010, Bilgi güvenliği yönetim sistemi için süreç tabanlı risk analizi, *Orta Doğu Teknik Üniversitesi Enformatik Enstitüsü Dergisi*, 1-5.

Khochare, N., Chalurkar, S. ve B.B.Meshram, 2013, Web application vulnerabilities detection techniques survey, *IJCSNS International Journal of Computer Science and Network Security*, 13 (6), 71-75.

Kobus, J., 2016, Cyberwarfare: the evolution of war, Master of Science *Utica College*, Utica, 1-64.

Martirosyan, Y., 2012, Security evaluation of web application vulnerability scanners' strengths and limitations, using custom web application, *California State University* California 1-183.

Muharremoğlu, G., 2013, Kurumsal bilgi güvenliğinde zafiyet, saldiri ve savunma öğelerinin incelenmesi, Yüksek Lisans Tezi, *İstanbul Üniversitesi* İstanbul, 1-156.

Muniz, J. ve Lakhani, A., 2013, Web penetration testing with kali linux, *Birmingham* Packt Publishing, p. 1-342.

Mussa, Y., 2016, Quantifying the security risk of discovering and exploiting software vulnerabilities, *Colorado State University* Colorado, 1-204.

Obied, A. M. A., 2008, Collection and analysis of web-based exploits and malware, Degree Of Master Of Science *The University Of Calgary* Calgary, 1-151.

Pelizzi, R., 2016, Securing web applications, *Stony Brook University*, New York, 1-163.

Polat, Ç., 2016, Penetration tests and security solutions for corporate networks, Master Science, *Dokuz Eylül University* İzmir, 1-182.

Ruse, M. E., 2013, Model checking techniques for vulnerability analysis of Web applications, *Iowa State University*, Iowa, 1-107.

Saleh, M. E., 2016, Detection and classification of obfuscated malware, Doctor Of Philosophy *The University of Texas*, San Antonio 1-93.

Sarıkoz, B. G., 2015, An information security framework for web services in enterprise networks, Master Of Science, *The Middle East Technical University*, Ankara, 1-218.

Shahriar, H., 2011, Mitigation of web-based program security vulnerability exploitations, Doctor of Philosophy *Queen's University* Kingston, 1-151.

Stuttard, D. ve Pinto, M., 2011, The web application hacker's handbook, *Indiana*, Wiley Publishing, p. 1-914.

Utku, S., 2012, Web service testing for domain specific web service discovery framework, *The Middle East Technical University*, Ankara, 1-84.

Vieira, M., Antunes, N. ve Madeira, H., 2008, Using web security scanners to detect vulnerabilities in web services, *2009 IEEE*, 978-1-4244-4421-2 (9), 566-571.

Vural, Y., 2007, Kurumsal bilgi güvenliği ve sizma (penetrasyon) testler, Yüksek Lisans Tezi, *Gazi Üniversitesi*, Ankara, 1-297.

Yalçınkaya, S., 2012, Assessing standard-compliance of public institution web sites of Turkey, *The Middle East Technical University*, Ankara, 1-100.

Yaşar, H., 2014, Kurumsal siber güvenliğe yönelik tehditler ve mücadele yöntemleri: eylem planı örneği, Yüksek Lisans Tezi, *Gazi Üniversitesi*, Ankara, 1-167.

Zhang, L., 2016, Rethinking the architecture of the web, *NortheasternUniversity*, Boston, 1-146.

Zhao, Z. ve Yong, F., 2013, Study on the security of government portal websites, *Applied Mechanics and Materials*, 380-384 (2013), 2534-2538.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

AdıSoyadı : Atakan DAŞDEMİR
Uyruğu : T.C.
DoğumYeriveTarihi : KARS 1978
Telefon : 5055142145
Faks :
e-mail : ataknet@gmail.com

EĞİTİM

Derece	Adı, İlçe, İl	**BitirmeYılı**
Lise :	G.A.M.P. Teknik Lisesi KARS	1996
Üniversite :	Selçuk Üniversitesi KONYA	2013
Yüksek Lisans :	Selçuk Üniversitesi KONYA	-
Doktora :		

İŞ DENEYİMLERİ

Yıl	**Kurum**	**Görevi**
16	Türk Hava Kuvvetleri	Asb.

UZMANLIK ALANI : Sistem**,** Network, Bilgi Güvenliği

YABANCI DİLLER : İngilizce

BELİRTMEK İSTEĞİNİZ DİĞER ÖZELLİKLER

YAYINLAR