Sızma Testi Raporu

Test Tarihi :

Rapor Tarihi :

İçindekiler

UYARI

Rapor içeriği gizli olup iki tarafın yazılı mutabakatı olmadan üçüncü taraflara basılı olarak ya da elektronik ortamda transfer edilemez veya paylaşılamaz. Rapor, tarama süresi içinde varlığı bilinen veya tarafımızdan tespit edilen güvenlik açıklıklarını içerecektir. Tarama işlemi bittikten sonra rapor teslim edilene kadar geçen süre içerisinde çıkabilecek yeni güvenlik açıklarına dair eksikliklerden dolayı raporu hazırlayan firma sorumlu tutulamaz.

Rapor içinde yer alan çözüm önerilerine konu hakkında fikir verme amaçlı yer verilmiştir. Çözüm önerilerinin uygulanması sebebi ile çıkabilecek problemlerden raporu hazırlayan firma sorumlu tutulamaz. Önerilerde sunulan değişikliklerden gerçekleştirilmeden önce konu hakkında uzman kişilerden destek alınması tavsiye edilir.

1. YÖNETİCİ ÖZETİ

Web Uygulaması Sızma Testi ve dış ağ testinde internet üzerinden erişim sağlayan anonim bir saldırgan bakış açısıyla kapsam dahilindeki web uygulamalarına ve dış ip adresine yönelik “Web Uygulama Sızma Testi” ve "Dış Ağ Sızma Testi" gerçekleştirilmiştir.

Otomatize tarama araçlarıyla yapılan taramaları müteakip bu araçlarla kontrol edilemeyecek açıklık çeşitleri manuel olarak denenmiştir. **OWASP İlk 10 API Güvenlik Riski**, **OWASP İlk 10 WEB Güvenlik riski** kapsamındaki tüm açıklık çeşitlerine detaylı bir şekilde bakılmıştır.Tüm testler MITRE ATT&CK ve OWASP metodolojilerine dayandırılmıştır. PCI DSS Penetration Testing Guidance ile uyumlu bir süreç izler ve BDDK Penetrasyon Testi Yaptırımları baz alınarak yapılmıştır.

Test kullanıcısı ile erişim sağlanan bir web uygulaması içerisinde 2 farklı arayüzde SQL Enjeksiyonu (SQLi) açıklığından etkilenen parametrelerin olduğu tespit edilmiş, açıklık başarıyla sömürülmüş ve veritabanına erişim sağlanmıştır.

Bunun yanı sıra, uygulama üzerinde **Yetki Atlatma ve Doğrudan Nesne Referansı Kontrolü (IDOR)** açıklığı bulunmuştur. Bu açıklık, bir kullanıcının başka kullanıcıların verilerine izinsiz erişim sağlamasına olanak tanımaktadır. Sömürü senaryosunda, oturum doğrulaması olmaksızın belirli bir kullanıcıya ait verilerin erişilebilir olduğu tespit edilmiştir. Bu durum, kullanıcı gizliliğinin ihlal edilmesine ve veri bütünlüğünün tehlikeye girmesine sebep olabilmektedir.

Yerel Ağ Sızma Testinde, ağ üzerinde bulunan bilgi sistem varlıklarına (İletişim Altyapısı ve Aktif Cihazlar, DNS Servisleri, Etki Alanı ve Kullanıcı Bilgisayarları, Veri tabanı Sistemleri vb.) bir kurum çalışanının yapabileceği saldırı senaryoları da uygulanarak “Yerel Ağ Sızma Testi” gerçekleştirilmiştir.

Otomatize tarama araçlarıyla yapılan taramaları müteakip bu araçlarla kontrol edilemeyecek saldırı senaryoları manuel olarak yapılmıştır.

Yerel ağ üzerinde varsayılan kimlik bilgileri kullanılarak erişilebilen yazıcı, IP Santral gibi web arayüzleri tespit edilmiştir. Bu uygulamaların güvenlik etkenlerine daha fazla dikkat edilmelidir.

Testler sırasında yerel ağ veya web uygulamaları üzerinde artık üreticisi tarafından uygulama ve güvenlik destekleri sona ermiş işletim sistemleri veri tabanları ve güncel olmayan uygulama versiyonları tespit edilmiştir. Güncelleme ve son sürümlerin kullanılması güvenlik için çok önemlidir.

Ayrıca Web uygulamalarının SSL sertifikasının hali hazırda geçerli olduğu ancak geçerliliğinin bitmesine kısa bir zamanının kaldığının dikkatlerden kaçmaması önemlidir.

Test süresince tespit edilen tek başına kullanılamayacak ancak bir saldırgan için yapabileceği farklı tür saldırıla kaynak teşkil etmesi muhtemel orta seviye açıklıkların da potansiyel risklerinin kaldırılması, uygulamalarınızın ve sistemlerinizin genel güvenlik seviyesinin daha da artmasını sağlayacaktır.

1.1.GENEL BİLGİLER

Bu rapor, **Bilisim Academy Eğitim ve Danışmanlık Ltd. Şti** tarafından tarafından **ÖRNEK A.Ş** üzerindeki güvenlik açıklarını ortaya çıkarmak amacı ile **1.1.202*** - **2.2.202*** tarihleri arasında gerçekleştirilen sızma testleri ve güvenlik değerlendirmeleri çalışmalarının detaylı sonuçlarını içermektedir.

Sızma testi kapsamında **ÖRNEK A.Ş** altyapısı ve sunucularının çalışmasını etkileyecek araçlar kurum yetkililerinin bilgisi olmadan kullanılmamış, hizmetin aksamasına neden olabilecek herhangi bir işlem gerçekleştirilmemiştir.

Test ile kapsam dahilindeki sistemler üzerinde bulunabilecek muhtemel güvenlik açıklıklarının kötü niyetli saldırganlardan önce ortaya çıkartılması ve önlem alınması amaçlanmaktadır.

Rapor, bulunan her güvenlik açığının risk derecesini, açıklık hakkında açıklamaları, daha detaylı bilgi bulabileceğiniz bağlantıları, güvenlik açığının nasıl kapatılabileceği hakkında gerekli bilgiyi, açığın nasıl kötüye kullanılabileceği hakkında örnekleri ve uzman personelin yorum ve önerilerini içermektedir.

Açıklıkların kapatılmasında izlenecek sırayı belirlerken teknik raporda belirtilen açıklık önem dereceleri öncelikli rol oynamalıdır.

Rapor okuyucunun TCP/IP ve kullanılan teknoloji hakkında temel bilgilere sahip olduğu düşünülerek hazırlanmıştır. Bu sebeple raporlarda kullanılan terimler ile ilgili herhangi bir açıklama yapılmayacaktır.

Sızma testinde; Kara Kutu sızma testi, Gri Kutu sızma testi ve Beyaz Kutu sızma testi olmak üzere üç yaklaşım vardır.

Kara kutu olarak adlandırılan test, sistemi ilk kez keşfeden bir bilgisayar korsanı gibi herhangi bir bilgiye sahip olmadan bir sisteme sızabilme çalışmasıdır. Sızma testi ekibi ortam hakkında hiçbir bilgiye sahip değildir ve testlerini kör bir şekilde gerçekleştirir. Sızma testi ekibine herhangi bir bilgi, herhangi bir mimari şema veya kaynak kodu verilmez.

Gri kutu testinde, bilgi sistemine sınırlı miktarda yetkiler ile saldırmaya çalışmaktan ibarettir. Bu durum, kuruluş içinde sistemin bazı noktalarına içeriden erişebilen kurumun çalışanı olabilecek bilgisayar korsanını başlangıç noktası olarak konumlandırarak sistemin test edilmesini mümkün kılar. Bir gri kutu sızma testinde test ekibi potansiyel olarak bir sistemde çeşitli seviyelerde ayrıcalıklara sahip bir kullanıcının erişim yetkilerine sahiptir.

Beyaz kutu sızma testinin yaklaşımı basittir. Sızma testi ekibi test sürecinde herhangi bir erişim kısıtlamasıyla karşılaşmaz. Sızma test ekibi bu durumda, maksimum faydalı bilgi elde etmek için kuruluşun teknik ekipleriyle iş birliği içinde çalışır. Mümkün olduğu kadar fazla güvenlik açığı tespit etmek için ihtiyacı olan her şeye erişebilir seviyededir. Bu test yaklaşımında uygulamalara veya domain yapısına erişim için kullanıcı bilgileri kuruluşun teknik ekibinden temin edilmektedir.

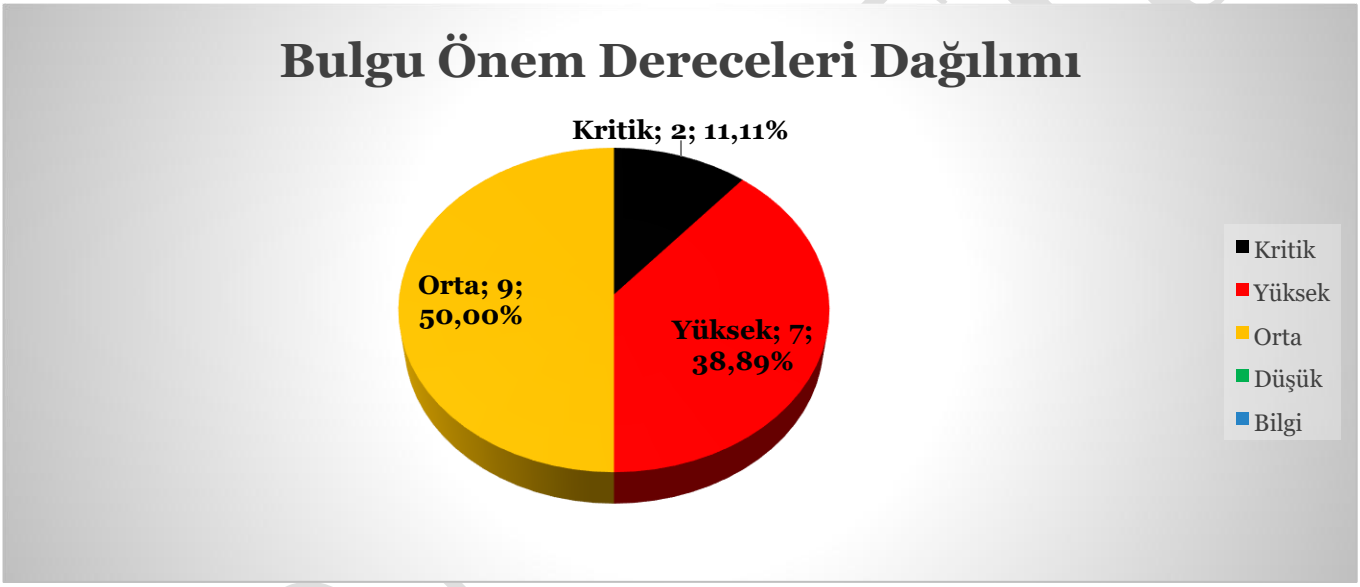
Sızma testi; **Gri Kutu Testi**, **Beyaz Kutu** Testi olmak üzere **2 evrede** gerçekleştirilmiştir.

Gerçekleştirilen güvenlik testlerin genelinde bulunan bulguların önem derecelerinin dağılım oranları Şekil-1'de belirtilmiştir. Özetle; test genelinde toplam **17** adet bulgu tespit edilmiştir.

Bu bulguların **%11.11 Kritik (2 Adet), % 38.89 Yüksek (7 Adet) ve %50.00 Orta (9 Adet)** önem derecesindedir.

	KRİTİK	YÜKSEK	ORTA	DÜŞÜK	BİLGİ	TOPLAM
Kara Kutu	0	0	0	0	0	0
Gri Kutu	0	7	9	0	0	16
Beyaz Kutu	2	0	0	0	0	2
TOPLAM	2	7	9	0	0	18

Tablo 1 – Zafiyetlerin Test Tiplerine Göre Dağılımı



ŞEKİL 1 – Bulgu Önem Dereceleri Dağılımı

Risk	Güvenlik Açığı	Etkilenen Sistemler	Test Tipi
Kritik	SQL Enjeksiyonu (SQLi)	https://örnek.com/	Beyaz Kutu Testi
Kritik	Güvensiz Doğrudan Nesne Referansı Kullanımı (IDOR)	https:// örnek.com/:8001/	Beyaz Kutu Testi
Yüksek	Web Sunucusu Desteklenmeyen Sürüm Tespiti	**PORT 80 / TCP :** 192.168.4.71 https:// örnek.com/:8001/, https://örnek.com/:8005/	Gri Kutu Testi
Yüksek	Open Relay'e Açık SMTP Sunucusu	**PORT 25 / TCP :** 192.168.4.95	Gri Kutu Testi

Yüksek	PHP Desteklenmeyen Sürüm Tespiti	https://örnek.com/	Gri Kutu Testi
Yüksek	Microsoft SQL Server Desteklenmeyen Sürüm Tespiti	**PORT 51093 / TCP:** 192.168.4.40 **PORT 50025 / TCP:** 192.168.4.4 **PORT 54831 / TCP:** 192.168.4.4	Gri Kutu Testi
Yüksek	Varsayılan Kimlik Bilgileri	**IP Santral:** 192.168.4.6, 192.168.4.8 **Yazıcı ve Tarayıcı:** 192.168.4.18, 192.168.4.19	Gri Kutu Testi
Yüksek	SSL Medium Strength Cipher Suites Supported (SWEET32)	**PORT 3389 / TCP:** 192.168.4.57 **PORT 51093 / TCP:** 192.168.4.40 **PORT 54831 / TCP:** 192.168.4.40	Gri Kutu Testi

Risk	Güvenlik Açığı	Etkilenen Sistemler	Test Tipi
		PORT 1433 / TCP: 192.168.4.65, 192.168.4.70, 192.168.4.73	
Yüksek	SSL Versiyon 2 ve 3 Protokol Tespiti	**PORT 54831 / TCP:** 192.168.4.40	Gri Kutu Testi
Orta	Zafiyetli JavaScript Kütüphaneleri	https://api. örnek.com/:441/	Gri Kutu Testi
Orta	cPanel XSS (CVE-2023-29489)	https://örnek.com/ https://örnek.com/:2083/ https://örnek.com/:2087/ https://örnek.com/:2096/	Gri Kutu Testi
Orta	Güvensiz HTTP Yanıt Başlığı Yapılandırması	https://örnek.com/ https://örnek.com/ https://örnek.com/:442 https://örnek.com/:441 https://örnek.com/:8001/ https://örnek.com/:8005/	Gri Kutu Testi
Orta	Web Uygulaması Clickjacking'e Karşı Potansiyel Olarak Savunmasız	https://örnek.com/:8001 https://örnek.com/:8005	Gri Kutu Testi

Orta	SMB İmzalama Gerekli Değil	**PORT 445 / TCP :** 192.168.4.4, 192.168.4.20, 192.168.4.25, 192.168.4.26, 192.168.4.32, 192.168.4.38, 192.168.4.40, 192.168.4.42, 192.168.4.46,192.168.4.47,192.168.4.48, 192.168.4.51,192.168.4.57,192.168.4.58, 192.168.4.65, 192.168.4.67, 192.168.4.70, 192.168.4.73, 192.168.4.74, 192.168.4.75, 192.168.4.80, 192.168.4.90, 192.168.4.92,	Gri Kutu Testi
Orta	Terminal Hizmetleri Yalnızca Ağ Düzeyinde Kimlik Doğrulamayı (NLA) Kullanmaması	**PORT 3389 / TCP :** 192.168.4.16, 192.168.4.25, 192.168.4.38, 192.168.4.46	Gri Kutu Testi
Orta	TLS Versiyon 1.0 Protokol Tespiti	**PORT 3389 / TCP:** 192.168.4.46, 192.168.4.57 **PORT 51093 / TCP:** 192.168.4.40 **PORT** **14222 / TCP:** 192.168.4.90 **PORT 54831 / TCP:** 192.168.4.40 **PORT 54818 / TCP:** 192.168.4.90 **PORT 1433 / TCP:** 192.168.4.65, 192.168.4.70, 192.168.4.73	Gri Kutu Testi
Risk	**Güvenlik Açığı**	**Etkilenen Sistemler**	**Test Tipi**
Orta	SNMP Ajanı Varsayılan Topluluk Adı (genel)	**PORT 161 / UDP:** 192.168.4.54	Gri Kutu Testi
Orta	SMB Servisi Zayıf Parola Güvenliği Yapılandırması	**PORT 445 / TCP:** 192.168.4.20	Gri Kutu Testi

Tablo 2 – Güvenlik Açığı ve Etkilenen Sistemler

1.1 KAPSAM VE IP ADRESLERİ

Bu tarama kapsamında taramayı yaptıran **ÖRNEK A.Ş.** tarafından belirlenen ve aşağıda listelenen sunuculara yönelik saldırı ve sızma testi gerçekleştirilmiştir. Bu testler esnasında, test edilen sunucular tarafından verilen hizmetlerin sekteye uğratılmaması amacıyla Denial of Service (DoS) saldırıları yapılmamıştır.

Çalışma/Test Alanı	Açıklama
• **192.168.4.0/25**	**Yerel Ağ**
• **https://** • **https://** • **https://** • **https://** • **https://** • **https://**	**WEB / API**
• **2*.1*.*7.***	**Dış Ağ**

1.1.1. TESTLERİN GERÇEKLEŞTİRİLDİĞİ ERİŞİM NOKTALARI

İç Ağ testleri kurumun VPN ağı üzerinden gerçekleştirilmiştir. Dış ağ ve WEB testleri internet ortamından gerçekleştirilmiştir. **IP Adresi/Adresleri: 176.*.*.*.*, 176.*.*.*.*,176.*.*.*.***

1.1.2. TESTLERİN GERÇEKLEŞTİRİLDİĞİ KULLANICI PROFİLLERİ

KULLANICI PROFİLİ	AÇIKLAMA
Yetkili Kullanıcı	Kimlik doğrulaması gerçekleştirilmiş ve sistem üzerindeki kaynaklara erişiminde yetki kısıdı minimum düzeyde olan kullanıcıları göstermek için tanımlanmış profildir.
Yetkisiz Kullanıcı	Kimlik doğrulama mekanizmasından geçen fakat sistem kaynaklarına erişimi yetkilendirme mekanizmaları tarafından kısıtlanan kullanıcıları göstermek için tanımlanmış profildir.
Anonim Kullanıcı	Kimlik doğrulama ve yetkilendirme mekanizmaları tarafından korunan kaynaklara erişemeyen kullanıcıları göstermek için tanımlanmış profildir.

1.2 TEST VE RAPORLAMA EKİBİ

Sızma Testi Ekibi	İletişim Bilgileri

Raporu Hazırlayan	Raporu Onaylayan

1.3 GENEL TEST METODOLOJİSİ

Günümüz bilgi güvenliğinde iki tür yaklaşım vardır. Bunlardan kabul göreni proaktif yaklaşımdır. Sızma testleri ve zayıflık tarama konusu proaktif güvenliğin en önemli bileşenlerinden biridir.

Sızma testleri ve zayıflık tarama birbirine benzeyen fakat farklı kavramlardır. Zayıflık tarama hedef sistemdeki güvenlik açıklıklarının çeşitli yazılımlar kullanarak bulunması ve raporlanması işlemidir. Sızma testi çalışmalarında amaç sadece güvenlik açıklıklarını belirlemek değil, bu açıklıklar kullanılarak hedef sistemler üzerinde gerçekleştirilebilecek ek işlemlerin (sisteme sızma, veritabanı bilgilerine erişme) belirlenmesidir.

Zayıflık tarama daha çok otomatize araçlar kullanılarak gerçekleştirilir ve kısa sürer. Sızma testi çalışmaları zayıflık tarama adımını da kapsayan ileri seviye tecrübe gerektiren bir süreçtir ve zayıflık tarama çalışmalarına göre çok daha uzun sürer.

1.4 RİSK DERECELENDİRME

Sızma testi çalışmalarında tespit edilen açıklar, beş seviyeli bir risk değerlendirme modeli kullanılarak sınıflandırılmıştır. Bu yaklaşım, başta CVSS (Common Vulnerability Scoring System) çerçevesi olmak üzere, PCI DSS (Payment Card Industry Data Security Standard), OWASP Risk Derecelendirme Metodolojisi, NIST SP 800-30 Risk Değerlendirme Çerçevesi ve ISO/IEC 27001 gibi birçok güvenlik standardı ve metodolojide yaygın olarak kullanılmaktadır.

Aşağıdaki tablo kullanılan seviyelendirmeyi açıklamaktadır.

ÖNEM DERECESI	CVSS-V3 SKOR ARALIĞI	AÇIKLAMA
KRITIK	9.0-10.0	Yıkıcı bir etkiye sahip olabilecek bir güvenlik açığıdır ve güvenlik açığının tanımlanması ve kullanılması kolaydır. Sömürü yöntemi basit olup genellikle sistemi ele geçirme ile sonuçlanır. Mümkün olan en kısa sürede bir eylem planı oluşturulması ve zafiyetin giderilmesi için gerekli aksiyonun alınması
		önerilir.
YÜKSEK	7.0-8.9	Sömürü yöntemi daha zordur fakat yükseltilmiş yetkilere ve potansiyel veri kayıpları ve sistem gecikmelerine neden olabilir. Kısa süre içinde bir eylem planı oluşturulup zafiyetin giderilmesi için gerekli aksiyonun alınması önerilir.
ORTA	4.0-6.9	Güvenlik açıkları mevcuttur fakat istismar edilemeyebilir veya sosyal mühendislik gibi ek adımlar gerektirebilir. Kritik ve Yüksek öncelikli sorunların çözümünden sonra bir eylem planı oluşturulup giderilmesi önerilir.
DÜŞÜK	0.1-3.9	Güvenlik açıkları istismara kapalıdır fakat şirketin saldırı yüzeyini arttırır. Bir sonraki bakım döneminde eylem planı oluşturulup giderilmesi tavsiye edilir.
BILGI	N/A	Belirlenen bir güvenlik açığı yoktur, yapılması gereken en üst seviye sıkılaştırmanın yapılmamasından kaynaklı sağlanan bilgilerdir.

ŞEKİL 2 - Raporda kullanılan risk seviyelendirmesi

1.5 GENEL BULGULAR

1.5.1.SQL Enjeksiyonu (SQLi)

SQL Injection (SQLi), bir saldırganın, uygulamanın veritabanıyla olan etkileşimini manipüle etmek için SQL sorgularını kötüye kullandığı bir güvenlik açığıdır. Bu tür saldırılar, kullanıcı girdilerinin yeterince doğrulanmaması veya filtrelenmemesi durumunda ortaya çıkar.

1.5.2.Güvensiz Doğrudan Nesne Referansı Kullanımı (IDOR)

Insecure Direct Object Reference (IDOR), web uygulamalarında, kullanıcının doğrulanmamış ve güvenlik önlemleri alınmamış bir şekilde doğrudan erişim sağladığı bir güvenlik açığıdır. Bu tür zafiyet, genellikle bir URL veya API parametresi aracılığıyla sistemdeki bir nesneye (örneğin, dosya, veri kaydı, kullanıcı bilgisi) erişim sağlanabilir. Eğer uygulama, kullanıcıların yalnızca kendilerine ait nesnelere erişimine izin vermek yerine, kimlik doğrulama veya yetkilendirme kontrolleri yapılmadan kullanıcıya farklı nesnelere de erişim izni verir, bu IDOR açığına yol açar.

Saldırgan, genellikle URL'deki parametreleri manipüle ederek, başka kullanıcıların verilerine ulaşabilir veya yetkisiz işlemler yapabilir. Örneğin, bir URL'deki kullanıcı ID parametresini değiştirerek başka bir kullanıcının hesabına veya verilerine erişebilir. Bu durum, kişisel bilgilerin çalınmasına, verilerin değiştirilmesine veya uygulama içerisinde başka kötü niyetli işlemlerin yapılmasına sebep olabilir.

1.5.3.Varsayılan Kimlik Bilgileri

Varsayılan Kimlik Bilgisi güvenlik açığı, tüm yapılandırma ayarlarına erişmek için bazı önceden ayarlanmış (varsayılan) yönetici kimlik bilgilerine sahip cihazları (router, switch, yazıcı, kamera vs.) en yaygın şekilde etkileyen güvenlik açığıdır. Bu tür cihazların satıcısı veya üreticisi, cihaz yapılandırmalarına erişmek için önceden tanımlanmış tek bir yönetici kimlik bilgisi seti kullanır ve herhangi bir potansiyel bilgisayar korsanı, bu kimlik bilgileri tüketiciler tarafından değiştirilmezse, bu tür cihazları hacklemek için bu gerçeği kötüye kullanabilir.

1.5.4.Open Relay'e Açık SMTP Sunucusu

MTA (Mail Transfer Agent) üzerinde açık mail rölelerinin (open mail relays) etkin durumda olması, sunucunun kimlik doğrulama gerektirmeden herhangi bir kaynak üzerinden e-posta göndermesine olanak sağladığını gösterir. Bu durum, saldırganların sunucuyu kötüye kullanmasına yol açar.

1.6 GENEL DEĞERLENDİRME

Yerel Ağ Testine VPN bağlantısı dahilinde her ağa bağlanabilen kullanıcı yetkisinde bağlanılmıştır. Teste kapsamda belirtilen tüm IP bloğu otomatize tarama araçları yardımıyla hızlı bir şekilde taraması ile başlanmış, yapılan taramaları müteakip bu araçlarla kontrol edilemeyecek saldırı senaryoları manuel olarak yapılmıştır. Ayrıca ağ üzerinde yerel ağlarda en sık uygulanan saldırı senaryoları uygulanmıştır.

Bu kapsamda yüksek seviyede bazı açıklıklar tespit edilmiştir. Open Relay'e Açık SMTP Sunucusu açıklığı başarı ile sömürülerek **"info@**.net"** e-posta adresinden **"info@bilisimacademy.com"** e-posta adresine kurumun mail sunucu kullanılarak mail gönderilmiştir. Yerel ağ olması nedeniyle açıklık seviyesi kritik seviyeden yüksek seviyeye düşürülmüştür.

Yerel ağ üzerinde varsayılan kimlik bilgileri kullanılarak erişilebilen yazıcı, IP Santral gibi web arayüzleri tespit edilmiştir.

Ağ üzerinde artık üreticisi tarafından uygulama ve güvenlik destekleri sona ermiş işletim sistemleri veritabanları ve güncel olmayan uygulama versiyonları tespit edilmiştir.

Ayrıca ağ üzerinde zayıf şifreleme algoritma kullanımından kaynaklı açıklıkların da tespiti yapılmıştır.

Web uygulama testleri dışarıdan sabit IP üzerinden yapılmıştır. Web Uygulaması Güvenlik Testi, kapsam dahilinde belirlenen adresler üzerindeki web uygulamalarına test hesap bilgileri kulllanılmadan otomatize tarama araçları yardımıyla hızlı bir şekilde taranıp daha sonra otomatize araçlarla kontrol edilemeyecek açıklık çeşitleri manuel olarak denenerek gri kutu sızma testi olarak başlanmıştır. Bu testleri müteakip testler verilen test kullanıcı bilgileri üzerinden beyaz kutu sızma testi olarak devam etmiştir. OWASP İlk 10 API Güvenlik Riski, OWASP İlk 10 WEB Güvenlik riski kapsamındaki tüm açıklık çeşitlerine detaylı bir şekilde bakılmıştır.

Bu kapsamda kritik açıklık olarak SQL Enjeksiyonu (SQLi) açıklığı tespit edilmiş ve ilgili açıklık başarı ile sömürülerek veri tabanı erişimi sağlanmıştır.

Ek olarak, **Yetki Atlatma ve Doğrudan Nesne Referansı Kontrolü (IDOR)** açıklığı da kritik açıklık olarak tespit edilmiştir. Bu açıklık, bir kullanıcının diğer kullanıcıların verilerine izinsiz erişim sağlamasına olanak tanımaktadır. Senaryo kapsamında yapılan sömürülerle, belirli kullanıcıya ait hassas verilere erişim sağlanmış, bu durum kullanıcı gizliliği ve veri bütünlüğünün ihlali olarak değerlendirilmiştir.

Yüksek seviyeli açıklık olarak da destekleği sona ermiş web sunucusu ile PHP sürüm kullanımı tespit edilmiştir.

Bunun haricinde hem yerel ağ hemde web uygulamalarında, önlem almanın faydalı olacağı ve bir saldırgan için yapabileceği **farklı tür saldırıla kaynak teşkil edebilecek** orta seviyeli açıklıklar da tespit edilmiştir.

Clickjacking zafiyeti, kullanıcıların tarayıcıları üzerinde yanıltıcı yönlendirmelere maruz kalması riskini taşırken, Eski sürüm JavaScript kütüphaneleri güncel olmayan güvenlik yamalarına sahip olabilir ve kötü niyetli saldırılara karşı savunmasız olabilir. Güncelleme ve son sürümlerin kullanılması güvenlik için çok önemlidir.

Gri kutu olarak başlayıp belirli bir süreden sonra beyaz kutu olarak icra edilen test ile CVSS Skoru baz alınarak yapılan değerlendirme neticesinde Gri kutu sızma testi ile **4** adet yüksek, 9 adet orta seviye ve Beyaz kutu sızma testi ile **2** adet kritik seviye olmak üzere toplamda **15** adet zafiyet tespit edilmiştir.

Sonuç olarak tespit edilen kritik seviyedeki zafiyetin zaman kaybedilmeden çözümlenmesi ve yüksek ve orta seviye açıklıkların da potansiyel risklerinin kaldırılması, uygulamalarınızın ve sistemlerinizin genel güvenlik seviyesinin daha da artmasını sağlayacaktır.

Tüm zafiyetlere yönelik etkilenen sistemlerin bazılarının örnek ekran görüntüleri ile birlikte detaylı anlatımı "**Teknik Bilgiler**" bölümünde verilmiştir.

1.7 .TAVSİYE ÖZETİ

Sızma testi neticesinde kritik ve yüksek seviyeli açıklık tespit edilemiştir. Bu açıklıklar için;

SQL injection zafiyetinden korunmak için kullanıcıdan alınan girdiler filtrelenerek alınması önerilmektedir. Uygulamaların ve veri tabanlarının ayrıştırılmış olarak kullanılması önerilmekle birlikte, uygulama kaynak kodlarına yönelik bir **zafiyet/kaynak kod analizi gerçekleştirilmesi** de tavsiye edilmektedir.

IDOR (Insecure Direct Object References) açıklığını önlemek için, sunucu tarafında her erişim talebi için sıkı yetkilendirme kontrolleri uygulanmalı ve kullanıcıların yalnızca kendi verilerine erişebilmesini sağlayan mekanizmalar oluşturulmalıdır. Doğrudan nesne referansları yerine, tahmin edilmesi zor rastgele erişim belirteçleri kullanılmalı ve bu belirteçler yetkilendirme ile ilişkilendirilmelidir.

Güncel versiyonu olmayan sistemler her an sorun olma potansiyeli içermektedir. Güncelleştirme uyarıları halka açık olarak yayınlandığı için art niyetli kişiler tarafından da kolaylıkla takip edilip zafiyetler kullanılabilmektedir. Güncelleştirmelerin takip edilmesini sağlayan bir politika ve prosedür kurulması ile bu konudan kaynaklanan risklerin asgari seviyeye indirgenebileceği öngörülmektedir.

Arayüze sahip ve varsayılan kullanıcı adı ve parolaları kolay bulunabilen sistemlerin gözden geçirilerek, farklı kullanıcı adı ve güçlü parola ile güncellenmesi gerekmektedir.

SSL Medium Strength Cipher Suites Supported (SWEET32) zafiyeti, 64-bit blok boyutuna sahip şifreleme algoritmalarının kullanılmasıyla ilgilidir. Bu zafiyeti gidermek için, sunucunuzda güçlü şifreleme algoritmalarının tercih edilmesi ve zayıf olanların devre dışı bırakılması tavsiye edilir.

Ancak **tedbir alınmasının faydalı olacağı** ve bir saldırgan için yapabileceği **farklı tür saldırıla kaynak teşkil edebilecek** orta seviye açıklıklar da tespit edilmiştir. Bu açıklıklar için; HTTP güvenlik başlıklarındaki eksiklikler, sistemin güvenlik seviyesini düşürerek potansiyel saldırılara açık hale getirmektedir. Bu durumun önüne geçmek için, uygulama katmanında HTTPS protokolünün zorunlu tutulması, yalnızca izin verilen kaynaklardan içerik yüklenmesi gibi başlıkların bir an önce eksiksiz bir şekilde yapılandırılması tavsiye edilmektedir.

Clickjacking saldırılarına karşı korunmak için web uygulamanızda X-Frame-Options başlığını kullanarak tarayıcının sayfanızı başka bir çerçevede gömülü olarak yüklemesinin engellenmesi tavsiye edilir.

SSL/TLS protokollerinde güvenli olmayan sürümlerin kullanımı tamamen engellenmeli, yalnızca TLS 1.2 ve TLS 1.3 protokolleri desteklenmelidir.

SMB, TLS, Versiyon Güncelleme gibi tüm sistemlerin birbirine bağlandığı protokoller ve durumlar için belirtilen zafiyetlerin kapatılmasının belirli bir plan dahilinde yapılması önerilmektedir. Aksi durumlarda sistemlerde kesintiler olabilmektedir.

Bunların haricinde sürekli olarak göz önünde tutulması gereken genel hususlar;

1. Form gönderme işlemlerinde otomatize araç kullanımlarının ve kaba kuvvet saldırılarının önüne geçilmesi adına tüm uygulamalar için CAPTCHA kullanılması tavsiye edilir.

2. Information Disclosure zafiyeti hassas ve gizli bilgilerin gerektiği gibi korunamamasından kaynaklanan bir zafiyettir. Kullanıcı girdileri, kullanıcı rolleri ve yetkilerinin dikkatle konfigüre edilmesi ve yetkisiz erişimlerin engellenmesi önem arz etmektedir. Server veya veri tabanından dönen hata mesajları kullanıcıya gösterilmemeli, boş bir sayfaya yönlendirilmelidir.

3. Networkte kullanılan protokollerin mümkünse şifreli olarak (HTTP yerine HTTPS, FTP yerine SFTP, TELNET yerine SSH gibi) ve güçlü kriptolama algoritmaları ile kullanılması önerilmektedir.

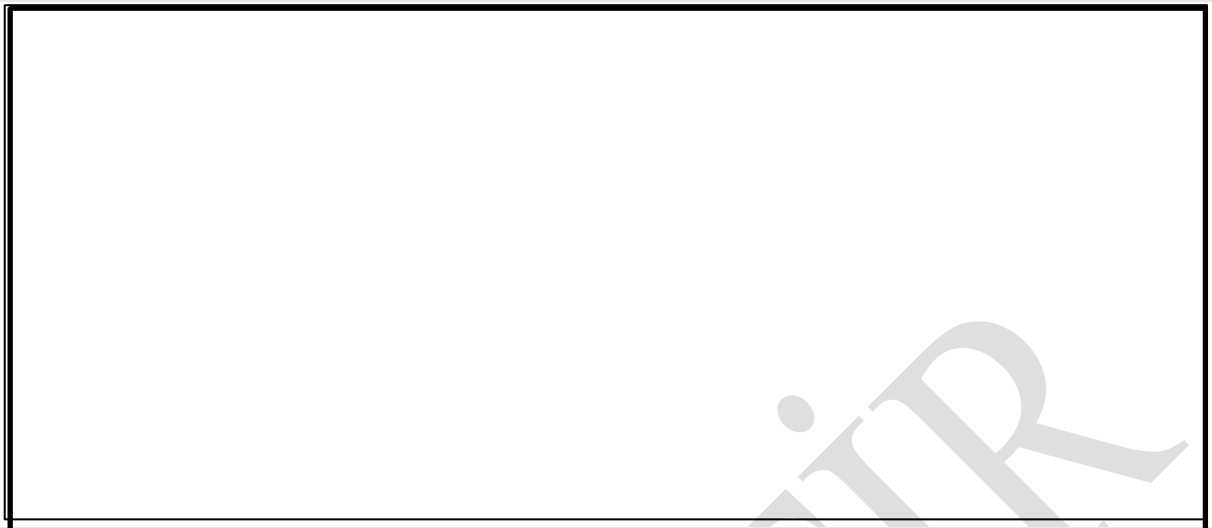
2. TEKNİK BİLGİLER

2.1 SQL Enjeksiyonu (SQLi)

CVSS SEVİYESİ	KRİTİK	CVSSv3.1 SKORU	10.0
CVSS VEKTÖRÜ	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H		
ETKİLENEN SİSTEMLER	https://örnek.***.com/		
AÇIKLAMA	SQL Injection (SQLi), bir saldırganın, uygulamanın veritabanıyla olan etkileşimini manipüle etmek için SQL sorgularını kötüye kullandığı bir güvenlik açığıdır. Bu tür saldırılar, kullanıcı girdilerinin yeterince doğrulanmaması veya filtrelenmemesi durumunda ortaya çıkar. Bir saldırgan, özel hazırlanmış SQL ifadelerini bir uygulamanın girdi alanlarına veya URL parametrelerine enjekte ederek şu gibi zararlı işlemler gerçekleştirebilir: 1. Yetkisiz erişim elde etmek, 2. Veritabanında saklanan hassas verileri çalmak, 3. Veritabanını değiştirmek, silmek veya sistemde bozulmaya neden olmak, 4. Yönetici ayrıcalıklarıyla işlemler yapmak. **Örnek:** ***SELECT * FROM users WHERE username = 'admin' AND password = 'password';*** Bu sorguda, saldırgan aşağıdaki girdiyle sistemin kontrolünü ele geçirebilir: **Input:** ' OR '1'='1 **Sonuçta oluşan sorgu:** ***SELECT * FROM users WHERE username = '' OR '1'='1' AND password = 'password';*** Bu sorgu, her zaman doğru döneceği için saldırgan yetkisiz erişim elde eder. SQL Injection, bir uygulamanın veri bütünlüğünü, sistem güvenliğini ve kullanıcı gizliliğini tehlikeye atar.		

TEST DETAYLARI

İlgili açıklık "***https://örnek.****.com/örnek /tr***" sayfası üzerinden iletilen istek üzerindeki "**kind**" parametresinde tespit edilmiştir. Açıklık test için verilen kullanıcı bilgileri ile sisteme girildikten sonra tespit edilmiştir.



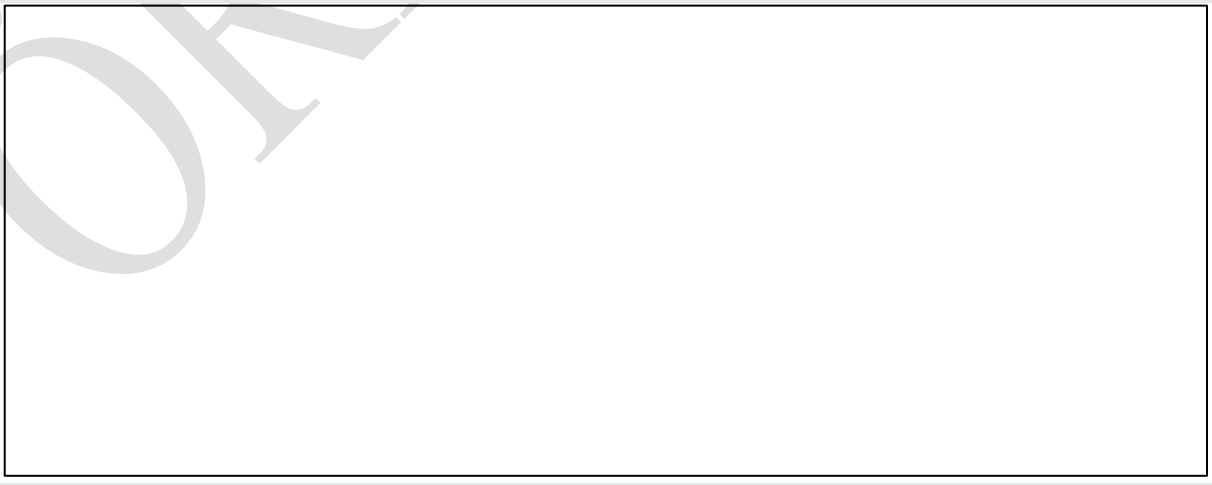
Resim 1 _

Resim 2 _

Burp suite aracıyla istek kesilerek kopyalanmış ve sqlmap aracına girdi olarak verilmiştir.

Resim 3 _

Veritabanlarının tespitine yönelik ekran görüntüsü aşağıda sunulmuştur.



Resim 4 _

“**” veritabanındaki 243 adet tablonun erişimine yönelik ekran görüntüsü aşağıda sunulmuştur.

Resim 9 _

Veritabanlarının tespitine yönelik ekran görüntüsü aşağıda sunulmuştur.

Resim 10 _

ÇÖZÜM ÖNERİLERİ	SQL Injection saldırılarına karşı alınabilecek önlemler: **Prepared Statements (Hazır Beyanlar) Kullanımı:** SQL sorgularını parametrelenmiş şekilde yazarak kullanıcı girdilerini otomatik olarak filtreleyin. **Örnek (PHP):** ***$stmt = $conn->prepare("SELECT * FROM users WHERE username = ? AND password = ?");*** ***$stmt->bind_p**("ss", $username, $password);*** ***$stmt->execute();*** **ORM (Object Relational Mapping) Kullanımı:** SQL sorgularını otomatik olarak oluşturmak ve kullanıcı girdilerini güvence altına almak için ORM araçlarını kullanın (örn: SQLAlchemy, Entity Framework). **Girdi Doğrulama ve Temizleme:** Kullanıcı girdilerini belirli bir şablona uygun olacak şekilde doğrulayın. Beklenmeyen karakterleri (örneğin tek tırnak ', çift tırnak ", noktalı virgül ;) temizleyin. **Minimum Yetkilerle Çalışma:** Veritabanı kullanıcılarına yalnızca gerekli izinleri tanımlayın. Yönetici (admin) haklarıyla uygulama çalıştırmaktan kaçının. **Web Uygulama Güvenlik Duvarı (WAF):** SQL Injection saldırılarını tespit etmek ve engellemek için bir WAF yapılandırın. **Detaylı Günlükleme:** Anormal sorguları ve hataları kaydedin. Saldırı girişimlerini izlemek için log dosyalarını düzenli olarak kontrol edin.
REFERANSLAR	https://www.acunetix.com/vulnerabilities/web/sql-injection/ https://www.acunetix.com/websitesecurity/sql-injection/ https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/sql-injection/ https://www.invicti.com/learn/sql-injection-sqli/ https://www.invicti.com/blog/web-security/sql-injection-cheat-sheet/ https://www.tenable.com/plugins/was/98115 https://portswigger.net/web-security/sql-injection https://portswigger.net/kb/issues/00100200_sql-injection https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html https://www.sqltattoo.com/blog/2022/06/microsoft-sql-server-remote-code-executionvulnerability-jun-202201/

2.2 Güvensiz Doğrudan Nesne Referansı Kullanımı (IDOR)

CVSS SEVİYESİ	KRİTİK	CVSSv3.1 SKORU	9.1
CVSS VEKTÖRÜ	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N		
ETKİLENEN SİSTEMLER	https://********.com:8001/		
AÇIKLAMA	**Insecure Direct Object Reference (IDOR)**, web uygulamalarında, kullanıcının doğrulanmamış ve güvenlik önlemleri alınmamış bir şekilde doğrudan erişim sağladığı bir güvenlik açığıdır. Bu tür zafiyet, genellikle bir URL veya API parametresi aracılığıyla sistemdeki bir nesneye (örneğin, dosya, veri kaydı, kullanıcı bilgisi) erişim sağlanabilir. Eğer uygulama, kullanıcıların yalnızca kendilerine ait nesnelere erişimine izin vermek yerine, kimlik doğrulama veya yetkilendirme kontrolleri yapılmadan kullanıcıya farklı nesnelere de erişim izni verir, bu IDOR açığına yol açar. Saldırgan, genellikle URL'deki parametreleri manipüle ederek, başka kullanıcıların verilerine ulaşabilir veya yetkisiz işlemler yapabilir. Örneğin, bir URL'deki kullanıcı ID parametresini değiştirerek başka bir kullanıcının hesabına veya verilerine erişebilir. Bu durum, kişisel bilgilerin çalınmasına, verilerin değiştirilmesine veya uygulama içerisinde başka kötü niyetli işlemlerin yapılmasına sebep olabilir.		

TEST DETAYLARI

Resim 1 –

Yukarıda ekran görüntüsü verilen kullanıcı profili bölümünün istek bilgisi aşağıda sunulmuştur.

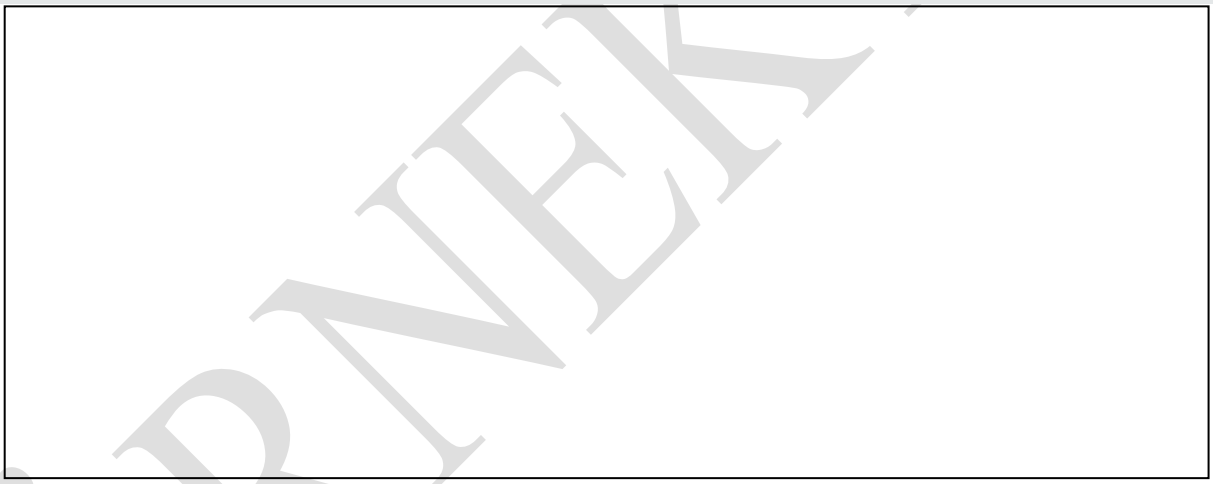
Resim 1 –

Bu istek bölümündeki id değeri değiştirilip doğru bir kullanıcı id değeri girildiğinde kullanıcı bilgileri görünmektedir. Bu zafiyet kullanılarak uygulama üzerinde yer alan tüm kullanıcılara ait kişisel verilere erişilebildiği tespit edilmiştir. Örnek ekran görüntüleri aşağıda sunulmuştur.

Resim 1 –

Resim 1 –

İd bilgisi dahil bazı bilgilerin aşağıda ekran görüntüsü verilen "chat/sohbet" bölümünden alınabileceği tespit edilmiştir.



Resim 1 –

Yukarıdaki sayfa açılmadığından dolayı ilgili sayfa ve isteği "https:// ***.com:8105/chat" üzerinden incelenmiş ve buradaki istek oluşturulmuştur. "https://****:8105 /chat" isteği ile aynı isteğin "https://****:8001/chat" adresine uygulanması ile ilgili ekran görüntüleri aşağıda sunulmuştur.

Resim 1 –

Her ne kadar ID bilgisi karmaşık bir yapı gösterse bile, ilgili isteğin yapıldığı session doğrulaması yapılmadığından dolayı yetkilendirme zafiyeti oluşmaktadır. Bu durum, herhangi bir kullanıcının farklı ID'ler ile erişim sağlayarak yetkisi olmayan verilere ulaşmasına olanak tanımaktadır. Güvenlik açısından, sunucu tarafında doğru bir şekilde oturum ve yetki doğrulaması yapılması kritik önem taşır.

ÇÖZÜM ÖNERİLERİ	**Yetkilendirme Kontrollerini Güçlendirme:** Uygulamanın her bir nesneye erişimi, doğru yetkilendirme kontrolleriyle güvence altına alınmalıdır. Kullanıcılar yalnızca kendilerine ait verilere erişebilmeli ve başkalarına ait verilere erişim engellenmelidir. **ID ve Parametreleri Güçlü Şekilde Şifreleme:** Kullanıcıya atanan benzersiz ID'ler ve parametreler, saldırganların tahmin edemeyeceği şekilde şifrelenmeli veya karma (hash) yapılmalıdır. Bu sayede, URL parametreleri değiştirilse bile erişim sağlanamayacaktır. **Gizli Verilerin Erişim Denetimini Yapma:** URL'lerde hassas verileri doğrudan göstermekten kaçınılmalıdır. Veriler, her zaman doğru kimlik doğrulama ve yetkilendirme adımlarını geçtikten sonra erişilebilir olmalıdır. **Erişim Kısıtlamaları ve Denetimi:** Kullanıcıların sadece kendi verilerine erişmesini sağlamak için ek sınırlamalar getirilmelidir. Erişim logları düzenli olarak izlenmeli ve kötü niyetli erişimler tespit edilmelidir.
REFERANSLAR	https://www.object-references-idor/ https://portswigger.net/web-security/access-control/idor https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html https://owasp.org/www-project-web-security-testing-guide/latest/4Web_Application_Security_Testing/05-Authorization_Testing/04Testing_for_Insecure_Direct_Object_References

2.3 Varsayılan Kimlik Bilgileri

CVSS SEVİYESİ	YÜKSEK	CVSSv3.1 SKORU	8.2
CVSS VEKTÖRÜ	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N		
ETKİLENEN SİSTEMLER	**IP Santral:** 192.168.4.6, 192.168.40.8 **Yazıcı ve Tarayıcı:** 192.168.4.18, 192.168.4.19		
AÇIKLAMA	Varsayılan Kimlik Bilgisi güvenlik açığı, tüm yapılandırma ayarlarına erişmek için bazı önceden ayarlanmış (varsayılan) yönetici kimlik bilgilerine sahip cihazları (router, switch, yazıcı, kamera vs.) en yaygın şekilde etkileyen güvenlik açığıdır. Bu tür cihazların satıcısı veya üreticisi, cihaz yapılandırmalarına erişmek için önceden tanımlanmış tek bir yönetici kimlik bilgisi seti kullanır ve herhangi bir potansiyel bilgisayar korsanı, bu kimlik bilgileri tüketiciler tarafından değiştirilmezse, bu tür cihazları hacklemek için bu gerçeği kötüye kullanabilir.		

TEST DETAYLARI

Aşağıda verilen ekran görüntülerinde yer alan IP ler üzerinde çalışan sistemlere varsayılan kullanıcı adı ve şifre ile giriş yapılabilmektedir.

IP Santral ile ilgili örnek ekran görüntüleri;

Resim 11 –

Resim 14 –

ÇÖZÜM ÖNERİLERİ	Yönetim panellerinin şifrelerinin değiştirilerek yerine güçlü şifreler atanması gerekmektedir. Yeni parolaların kullanıldığından ve bu parolaların benzersiz, uzun olduğundan ve farklı sayı, harf ve sembollerden oluşan bir kombinasyon içerdiğinden emin olun. Eski şifreleri kullanmayınız.
REFERANSLAR	https://owasp.org/www-project-web-security-testing-guide/latest/4Web_Application_Security_Testing/04-Authentication_Testing/02Testing_for_Default_Credentials https://www.thehacker.recipes/web/config/default-credentials

2.4 Open Relay'e Açık SMTP Sunucusu

CVSS SEVİYESİ	YÜKSEK	CVSSv3.1 SKORU	7.5
CVSS VEKTÖRÜ	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		
ETKİLENEN SİSTEMLER	**PORT 25 / TCP :** 192.168.4.95		
AÇIKLAMA	MTA (Mail Transfer Agent) üzerinde açık mail rölelerinin (open mail relays) etkin durumda olması, sunucunun kimlik doğrulama gerektirmeden herhangi bir kaynak üzerinden e-posta göndermesine olanak sağladığını gösterir. Bu durum, saldırganların sunucuyu kötüye kullanmasına yol açarak şu gibi sorunlara neden olabilir: **Spam Gönderimi:** Saldırganlar, sunucuyu spam e-posta göndermek için kullanabilir. Bu, IP adresinizin kara listeye alınmasına yol açabilir ve meşru e-postaların teslimat oranını etkileyebilir. **Kimlik Avı Saldırıları:** Dolandırıcılar, kullanıcıları kandırmak için sahte e-postalar gönderebilir ve hassas bilgileri ele geçirebilir. **Kötü Amaçlı Yazılım Yayılımı:** Sunucu, zararlı yazılımları yaymak için bir araç haline gelebilir. **İtibar Kaybı:** Sunucunun kötüye kullanımı, işletmenizin güvenilirliğine zarar verebilir ve müşteri ilişkilerini zedeleyebilir. Açık mail röleleri genellikle güvenlik politikalarının eksik olduğu, yanlış yapılandırılmış veya güncellenmemiş MTA'larda görülür.		
TEST DETAYLARI 192.168.4.94 IP adresli Zimbra E-Posta sunucusunu mail relaying'e izin verdiği belirlenmiştir.			

BU BÖLÜMÜN DEVAMINDA ;

TÜM ZAFİYET BULGULARI BU BÖLÜMDE DETAYLI AÇIKLAMALARI VE KANITLARIYLA SUNULMAKTADIR.

3. RAPORDA GEÇEN TEKNİK TERİM VE KISALTMALAR

A

ASP : Active Server Pages
ADFS : Active Directory Federation Services
ADC : Additional Domain Controller
ACL : Access Control List
API : Application Programming Interface
AD : Active Directory

B

BIOS : Basic Input/Output System
BSSID : Basic Service Set Identifier

C

CPU : Central Processing Unit
CVE : Common Vulnerabilities and Exposures)
CVSS : Common Vulnerability Scoring System)
CWE : Common Weakness Enumeration)

D

DoS : Denial of Service
DAG : Database Availability Group
DC : Domain Controller
DCBQOS : Data Center Bridging Quality of Service
DISM : Deployment Imaging Servicing Menagement

E

EAC : Exchange Administration Center
EAP : Extensible Authentication Protocol

F

FTP : File Transfer Protocol
FC : Fiber Channel

G

GPO : Group Policy Object
GPU : Graphics Processing Unit

H

HA : High Availability
HTTP : Hypertext Transfer Protocol
HTTPS : Hypertext Transfer Protocol Secure
HTML : Hyper Text Markup Language

I

ISCSI : Internet Small Computer System Interface
IIS : Internet Information Server

J

N

NIST : National Institute of Standards and Technology)
NAT : Network address translation
NTP : Network Time Protokol
NFS : Network File System
NPS : Network Policy Server
NMAP : Network Mapper

O

OSI : Open Systems Interconnection
ODX : Offloaded Data Transfer
OU : Organization Unit
OWASP: Open Web Application Security Project

P

PPTP : Point To Point Tuneling Protocol
PKI : Publik Key Infrastructure
PII : Personally Identifiable Information

Q

QoS : Quality of Services

R

RIP : Routing Information Protocol
RDP : Remote Desktop Protokol
RCE : Remote Code Execution

S

SSL : Secure Sockets Layer
SD : Secure Digital (Secure Digital Memory Card)
SAN : Storage Area Network
SMB : Server Message Block

T

TCP : Transmission Control Protocol
TLS : Transport Layer Security

U

UDP : User Datagram Protokol

V

VPN : Virtual Private Network
VM : Virtual Machine
VAMT : Volume Activation Management Toolkit

W

WDAC : Windows Data Access Components
WDS : Windows Deployment Services

4.TEST ESNASINDA KULLANILAN ARAÇLAR

Raporda detayları sunulan sunuculara doğru gerçekleştirilen testlerde aşağıdaki listelenen ticari ve açık kaynak kodlu araçlar kullanılmıştır.

Nessus : Nessus, Ağ düzeyindeki IP'lere port taraması yaparak üzerinde çalışan servislerin zafiyetlerini gösteren araçtır. (https://www.tenable.com/)

Nmap (Network-Mapper) : Ağ haritasının çıkarılmasında ve çalışan servislerin versiyon güvenliği denetiminde kullanılan açık kaynak kodlu bir araçtır. (https://nmap.org/)

OpenVAS (Open Vulnerability Assessment System): OpenVAS, açık kaynaklı bir güvenlik tarayıcı aracıdır ve kapsamlı zafiyet değerlendirmeleri yapmak için kullanılır. Bilinen güvenlik açıklarını ve yapılandırma hatalarını tespit ederek sistemlerin ve ağların güvenliğini artırmaya yönelik ayrıntılı raporlar sunar. (https://www.greenbone.net/en/)

Acunetix : Web uygulamalarını ve web sitelerini güvenlik açıklıklarına karşı ootomatik olarak tarayabilen ve zafiyet analizi yapabilen kapsamlı bir güvenlik tarama aracıdır. (https://www.acunetix.com/)

Burp Suite : Web uygulamalarının güvenlik zafiyetlerini manuel ve otomatik olarak test etmek için kullanılan, güvenlik araştırma ve pentesting araç setidir. (https://portswigger.net/burp)

Wireshark : Ağ trafiğini yakalayıp detaylı bir şekilde analiz etmeye yarayan popüler bir ağ protokol analizörüdür. (https://www.wireshark.org/)

Savvius Omnipeek : Ağ sorunlarının teşhisi ve onarımı için binlerce protokolün kodunu çözebilen yüksek performanslı bir ağ protokolü analiz aracıdır

Cain and Abel : Ağ paket kkoklama (netwok packet sniffing), kaba kuvvet saldırıları gibi birçok özelliği bulunan ve Windows için şifre kırma/kurtarmaya yarayan ücretsiz bir araçtır. (https://sectools.org/tool/cain/)

Crackmapexec : Python ile yazılmış açık kaynak kodlu geniş ölçekli Active Directory ortamlarında kullanılmak için tasarlanmış bir post-exploitation aracıdır. (https://github.com/Porchetta-Industries/CrackMapEx)

Impacket : İçinde yerel ağda buluna konfigürasyon hatalarını, AD üzerinde zafiyet sömürmesi için gerekli araçları barındıran tool setidir. (https://github.com/fortra/impacket)

Responder : Ağ içindeki LLMNR, NBT-NS ve MDNS protokollerini dinleyerek, kimlik avı saldırıları ve kimlik doğrulama bilgilerinin ele geçirilmesi için kullanılan bir penetrasyon testi aracıdır. (https://www.kali.org/tools/responder/)

Metasploit : Güvenlik açıklıklarını keşfetmek, test etmek ve bunları istismar etmek için kullanılan açık kaynaklı bir penetrasyon testi frameworküdür. (https://www.metasploit.com/)

SQLmap: SQL enjeksiyon kusurlarını tespit etme ve bunlardan yararlanma ve veritabanı sunucularını devralma sürecini otomatikleştiren açık kaynaklı bir sızma testi aracıdır. (https://sqlmap.org/)

Advanced Ip Scanner : Yerel ağlarda cihazları hızla bulmak, taramak ve yönetmek için tasarlanmış bir ağ tarama aracıdır. (https://www.advanced-ip-scanner.com/tr/download/)

rpcclient : Rpcclient, Microsoft Windows işletim sistemlerinde çalışan sunuculara ve hizmetlere uzaktan prosedür çağrıları yapmak için kullanılan bir komut satırı aracıdır. (https://www.samba.org/samba/docs/current/man-html/rpcclient.1.html)
smbclient: SMB/CIFS protokolünü kullanarak Windows paylaşımlarına bağlanmayı ve bu paylaşımları yönetmeyi sağlayan araç