Sızma Testi Raporu

Datassist Bilgi Teknolojileri A.Ş.
03/11/2025

DİKKAT GİZLİ BİLGİ!

Bu rapor yukarıda adı geçen kuruma özel olarak hazırlanmıştır. İçeriği yüksek gizlilik gerektiren bilgiler barındırmaktadır. Yüksek standartlarda şifrelenmeden Internet üzerinden veya fiziksel ortamda yetkilendirilmemiş kişilerle paylaşılamaz.

TerraMedusa Bilişim Güvenliği Çözümleri Ltd. Şti.

Metodoloji

TerraMedusa tarafından hazırlanan bu rapor, TerraMedusa Sızma Testi analiz sonuçlarını içermektedir. Zafiyetler detaylı açıklamaları, risk analizleri, çözümleri ve ekran görüntüleri ile listelenmiştir. Çalışma kapsamında gerçekleştirilen eylemlerde kurumun işleyişini etkileyecek veya aksatacak yöntemler kullanılmamıştır. Yukarıda bahsi geçen kurum bu çalışma yapılmadan önce onay vermiştir.

Sızma Testi, günümüz ekonomisinde ve bilgi alışverişi sırasında bize her türlü fırsatı sunan internet ortamında çok büyük bir rekabet avantajı sağlamaktadır. Ancak kurumlar, dışarıdan kişilere kurum içi sistem kaynaklarına yetkisiz erişim imkânı sağlayacak hatalar yaparak kaynaklarının kullanımını engellemekte veya değerli bilgilerin çalınmasına neden olmaktadır. TerraMedusa'nın kapsamlı bilgi birikimi, kuruluşların bilgi varlıklarına yetkisiz erişime karşı benzersiz bir Sızma Testi metodolojisi geliştirmiştir.

Sızma Testi, belirli güvenlik seviyelerinde ihlallerin varlığını tespit etmek, bu ihlalleri azaltmak, gerekli adımları sağlamak için mevcut güvenlik mekanizmalarını denetlemek ve daha sonra bu adımları ve mekanizmaları atlamaya çalışmaktan oluşur. TerraMedusa Sızma Testi, sektör içerisinde güvenlik açığı analizi, güvenlik taraması veya zafiyet analizi olarak adlandırılan ve otomatik araçların kullanıldığı diğer güvenlik taramalarından farklılık göstermektedir. TerraMedusa Sızma Testi'nde risklerin ve zafiyetlerin zararları, saldırganların ulaşabileceği noktalar analiz edilir ve ağ güvenliği bütünüyle ele alınır.

TerraMedusa çalışanları tarafından kullanılan araç, yöntem ve teknikler, gerçek Hacker'ların bildiği süreçlerle birlikte uygulanır ve istisnai güvenlik açıkları, teknik araç ve yöntemler ustalıkla uygulanır. Güvenlik açıkları ve konfigürasyon hataları gibi sorunlar tespit edilerek, saldırganların ağ ve ağa bağlı sistemlere verebileceği zarar en aza indirilir.

Sızma Testi çalışmalarımızda, dış ağ, iç ağ güvenlik mekanizmalarının güvenli şekilde çalışıp çalışmadığı kontrol edilerek kritik verilere izinsiz erişimin engellenmesi sağlanmaktadır. Tüm analizler saldırgan bakış açısıyla gerçekleştirilmekte olup, dışarıdan yetkisiz erişim sağlamaya yönelik tüm yöntemler incelenmektedir.

Süreç

Adım 1	Sistem Güvenliği Ana Hatları	Bu aşama, sistemler ve ağ güvenliği ortamına ilişkin kapsamlı bir anlayış kazanmayı amaçlamıştır. Ağ altyapısını, işletim sistemlerini, uygulamaları ve mevcut güvenlik önlemlerini incelenir. Bu bilgiler Sızma Testi sürecinin sonraki adımları için temel oluşturur.
Adım 2	Sistem Zayıflık İncelemesi	Bu aşamada sistemin güvenlik altyapısının kapsamlı bir incelemesi yapılır. Ekibimiz sistem konfigürasyonlarını, erişim kontrollerini, izinleri ve güvenlikle ilgili diğer ayarları inceler. Ayrıca, sistem dokümantasyonu, önceki güvenlik denetimleri ve sistem bileşenlerindeki bilinen güvenlik açıkları gözden geçirilmektedir.
Adım 3	Zayıflık Değerlendirmesi	Bu adımda kapsamlı bir güvenlik açığı değerlendirmesi yapmak için araçlar ve manuel teknikler kullanılır. Ekibimiz, güncel olmayan yazılım sürümleri, yanlış yapılandırmalar, zayıf şifreler ve yaygın güvenlik sorunları gibi güvenlik açıklarını tespit etmek için son teknoloji araç ve yöntemleri kullanır. Bu değerlendirmenin sonuçları, daha fazla analiz için belirlenen güvenlik açıklarının önceliklendirilmesine yardımcı olur.
Adım 4	Araç Analizi	Zafiyet değerlendirmesinin ardından elde edilen sonuçlar titizlikle analiz edilir. Bulgular dikkatle incelenir, önem derecesine göre kategorize edilir ve yanlış pozitifler filtrelenir. Manuel doğrulama yoluyla, tespit edilen güvenlik açıklarının doğruluğu sağlanır ve sistemin güvenliği üzerindeki potansiyel etkilerini değerlendirilir.
Adım 5	Penetrasyon Saldırıları	Ekibimiz bu aşamada belirlenen güvenlik açıklarından yararlanmak ve gerçek dünya senaryolarını simüle etmek için hedefli saldırılar gerçekleştirir. Parola kırma, ağ izleme ve yazılım açıklarından yararlanma gibi çeşitli teknikler kullanarak sistemin potansiyel tehditlere karşı direncini değerlendirmeye çalışır.
Adım 6	Zayıflık Analizi	Sızma saldırılarının ardından, başarılı ve başarısız istismar girişimleri kapsamlı bir şekilde analiz edilir. Bu analiz, güvenlik açıklarının etkisini belirlememizi ve potansiyel çözüm stratejileri hakkında fikir edinmemizi sağlar. İyileştirme çabalarını kolaylaştırmak için saldırı vektörlerinin, kullanılan yöntemlerin ve bunların sonuçlarının ayrıntılı dokümantasyonu hazırlanır.
Adım 7	Geribildirim Süreci	Son adım, bulgularımızı ve sistemin güvenliğini artırmaya yönelik önerilerimizi iletmek için kapsamlı bir rapor sunmayı içeriyor. Bu rapor sistem yöneticileri, BT ekipleri ve yönetim de dahil olmak üzere paydaşlarla paylaşılır. Belirlenen güvenlik açıkları, bunların kurum üzerindeki potansiyel etkileri ve düzeltme için önerilen önlemler hakkında ayrıntılı bilgiler içerir. Ayrıca soru veya endişeleri ele almak ve önerilen güvenlik iyileştirmelerini uygularken rehberlik sağlamak için toplantılar veya görüşmeler yapmak teklif edilir.

Sızma Testi sürecinin yinelemeli olduğunu ve belirli kurumsal gereksinimlere uyacak şekilde uyarlanabileceğini anlamak önemlidir. Bu proje boyunca amacımız güvenlik açıklarını tespit etmek, potansiyel etkilerini değerlendirmek ve sistemin güvenlik duruşunu güçlendirmek için eyleme geçirilebilir öneriler sunmaktır.

Bulgu Risk Seviyeleri

Gerçekleştirilen analizler ilgili firma tarafından iletilen bilgi varlıkları baz alınarak gerçekleştirilmiştir. Yapılan çalışmada Sızma Testi çalışmasını gerçekleştiren uzmanlar ile Bilgi İşlem ekibinin bakış açıları birbirinden farklıdır. Dolayısıyla Bilgi İşlem ekibi tarafından açık olarak değerlendirilmeyen bir konu çok kritik bir güvenlik tehditine sebep olabilir.

Ağ ve sistemlerde bulunan riskler çeşitli kategorilerde sınıflandırılır. Aşağıda bu risk sınıflandırmaları ve yol açabileceği zararları bulabilirsiniz.

Acil Risk Sınıfı

Doğrudan uzaktan izinsiz erişim ve veri ihlaline sebep olabilecek, en ileri seviyede riskli bulgular için kullanılır. Bu tür zayıflıklar hem bireysel saldırganlar, hem de worm, botnet gibi hack gruplarının kullandığı kitlesel saldırılarla istismar edilebilirler.

Kritik Risk Sınıfı

Sistemin bütünlüğünü tehdit eden tarzda saldırılar bu sınıfta görülür. Bu sınıfta bulunan zayıflıklar saldırganın en çabuk şekilde sistemlere erişmesini sağlar. Niteliksiz saldırganlar dahi bu zayıflıklarla sistemlere erişim sağlayabilirler.

Yüksek Risk Sınıfı

Yüksek risk derecesindeki zayıflıklar sistemden bazı kritik bilgi edinme ile sonuçlanabilecek saldırıları tanımlar. Ayrıca yerel ağdan ya da sunucular üzerinden hak yükseltmeyle sonuçlanacak saldırılara sebep olabilirler.

Orta Risk Sınıfı

Yerel ağdan veya sunucu üzerinden gerçekleştirilebilecek, hizmet dışı bırakma, servis engelleme ile sonuçlanan saldırılara sebep olan açıklıklardır.

Düşük Risk Sınıfı

Bu sınıfta yer alan zayıflıklar tamamıyla sistem ile ilgili bilgilerin deşifre edilmesi veya sistem, ağ üzerinde çalışan riskli bir servisin haberdar edilmesi amacıyla kullanılır. Bu sınıfta yer alan sistem ve ağ ile ilgili yöneticilerin haberdar olması için belirtilir. Bu bilgiler ve öneriler ışığında sıkılaştırma (Hardening) çalışmaları yapılması gerekir.

Revizyon Geçmişi

Versiyon	Tarih	Açıklama
1	03/11/2025	Sızma Testi çalışması sonucunda rapor yayınlanmıştır.

Kapsam ve Toplam Güvenlik Açığı Özeti

Kapsam

Giriş

Kapsam bölümü Sızma Testinin sınırlarını ve hedeflerini tanımlar. Test için yetkilendirilen sistemleri, ağları ve uygulamaları ve müşteri tarafından belirtilen sınırlamaları veya istisnaları ana hatlarıyla belirtir. Kapsam, genel değerlendirmenin temelini oluşturur ve Sızma Testi görevine nelerin dahil edilip nelerin hariç tutulduğunun net bir şekilde anlaşılmasını sağlar.

Amaç

Sızma Testi'nin amacı, kurumsal ağın ve ilgili altyapının güvenlik durumunu değerlendirmektir. Değerlendirme, kötü niyetli aktörlerin yararlanabileceği güvenlik açıklarını ve zayıflıkları belirlemeyi amaçlamıştır. Test, belirlenen sistemlerin ve uygulamaların kapsamlı bir değerlendirmesini yaparak, kuruluşun güvenlik kontrollerini geliştirmesine ve potansiyel riskleri azaltmasına yardımcı olmayı amaçlamıştır.

Standartlar

Rapor hazırlanırken KVKK, TSE, BDDK, SPK, EPDK, ISO/IEC 27001/27002, PCI DSS, SoX/Cobit, NSA, NIST, CIS, SAS 70 uyumlu raporlama ve standartlar kullanılmıştır. Metodoloji olarak ise OWASP Top 10, OSSTMM standartlarını da karşılayacak biçimde en güncel tekniklerden yararlanılmıştır. Çalışma boyunca yerel ve uluslararası standartlara bağlı kalınarak analizler gerçekleştirilmiştir.

Aşağıdaki bilgi varlıkları ilgili firmadan yazılı olarak temin edilmiştir. Tüm çalışma ve analizler bu bilgi varlıkları üzerinden gerçekleştirilmiştir. Aşağıda IP, URL, uygulama ve diğer bilgi varlıkları detaylı olarak açıklanmıştır.

1. Dış ağ analizi
2. İletişim altyapısı ve aktif cihazlar
3. Firewall, IPS, Router, VPN sistemleri analizleri
4. DNS servisleri
5. Sunucu sistemleri ve sanallaştırma platformları
6. Eposta servisleri
7. Veritabanı sistemleri
8. Web uygulamaları ve Web servisleri

Kurumda yapılan detaylı incelemeler sonucunda aşağıdaki güvenlik açıkları tespit edilmiştir. Açıklamalar risk seviyeleri ile birlikte listelenmiştir. Sistem, ağ, uygulama ve bileşenlere ilişkin açık olmayan kategorilerdeki bilgiler rapora dahil edilmemiştir. Ayrıca yanlış pozitif oluşturabilecek mevcut olmayan bulgulara da yer verilmemektedir.

Güvenlik açıkları, raporun okunabilirliğini artırmak ve tekrarlı girişlerden kaçınmak için gruplandırılarak listelenir. Her bir zafiyetin altında, zafiyetin tespit edildiği bilgi varlıklarının bir listesi yer almaktadır.

İstatistik kısmında ise tekil ve toplam olarak bilgi varlıklarındaki açıklar iki ayrı şekilde verilmiştir. Tekil olarak bakıldığında bilgi varlıklardaki açıkların tamamı görülmektedir. Toplam bilgi varlıklarındaki açıklar ele alındığında ise, aynı açıklar birden fazla bilgi varlığında bulunabildiği için genel bir toplu resim elde edilebilir.

Kurumdaki riskin ciddiyetine bakıldığında; tüm bilgi varlıklarındaki açıkların miktarının göz önüne alınmasıyla daha gerçekçi bir bilgi elde edilebilir.

Rapor Detayları

Sözleşme Tarihi
23/10/2025

Rapor Tarihi
03/11/2025

Raporu Hazırlayan Firma
TerraMedusa Bilişim Güvenliği Çözümleri Ltd. Şti.
bilgi@terramedusa.com

Analizin Gerçekleştirildiği Kuruluş
Datassist Bilgi Teknolojileri A.Ş.

Yetkili Kişi
Yağmur Teke

Yetkili Kişi İletişim Bilgisi
507 821 8256

Güvenlik Açığı Çizelgesi

Güvenlik açığı tablosu bölümü, tespit edilen güvenlik açıklarına ve bunların önem derecelerine ilişkin kapsamlı bir genel bakış sağlar. Sızma Testi çalışması sırasında keşfedilen güvenlik açıklarının görsel bir temsili olarak hizmet eder.

Bu bölüm, paydaşların genel risk ortamını anlamalarına ve iyileştirme çabalarına öncelik vermelerine yardımcı olmayı amaçlamaktadır.

Kod	Zayıflık	Ağ	Risk Seviyesi	Durum
ENF473826	Tomcat Java Stack Trace Bilgi Edinme Zayıflığı	Dış Ağ	Düşük	Kapatılmadı
ENF168641	Eksik X-Content-Type-Options Header Zayıflığı	Dış Ağ	Orta	Kapatılmadı
ENF603251	Web Uygulaması HttpOnly Zayıflığı	Dış Ağ	Düşük	Kapatılmadı
ENF016619	JQuery Çoklu Zayıflıklar	Dış Ağ	Orta	Kapatılmadı
ENF585303	Eksik Content Security Policy (CSP) Zayıflığı	Dış Ağ	Orta	Kapatılmadı

İstatistikler

Mevcut Rapor - 03/11/2025

Tekil Güvenlik Açığı Sayısı

Tekil güvenlik açıklarının sayısı, Sızma Testi görevi sırasında keşfedilen farklı güvenlik açıklarının toplam sayısını ifade eder. Her bir güvenlik açığı, kuruluşun sistemlerinde, uygulamalarında veya altyapısında saldırganların yararlanabileceği belirli bir kusuru veya yanlış yapılandırmayı temsil eder. Bu metriğin dahil edilmesi, güvenlik açıklarının kapsamının ölçülmesine yardımcı olur ve risk değerlendirmesi için önemli bir veri noktası sağlar.

Tekil güvenlik açıkları sayısı, hem kritik hem de daha az ciddi sorunları kapsayan tanımlanmış güvenlik açığı türlerini yansıtır. Daha yüksek sayıda tekil güvenlik açığının daha yüksek bir genel risk seviyesine işaret etmediğini belirtmek çok önemlidir. Her bir güvenlik açığının ciddiyeti ve istismar edilebilirliği, kurumun güvenlik duruşu üzerindeki etkisini değerlendirmek için ayrı ayrı değerlendirilmelidir.

Bilgi Varlıklarındaki Toplam Güvenlik Açıkları

Bilgi varlıklarındaki toplam güvenlik açıkları, Sızma Testi çalışması sırasında kuruluşun sistemleri, uygulamaları ve altyapısı genelinde tespit edilen güvenlik açıklarının kümülatif sayısını temsil eder. Bu metrik, mevcut güvenlik açıklarının nicel bir değerlendirmesini sağlar ve ele alınması gereken güvenlik açıklarının ölçeğini ve kapsamını anlamaya yardımcı olur.

Toplam güvenlik açığı sayısı, kritikten daha az ciddi olana kadar çeşitli güvenlik açıklarını kapsar. Her bir güvenlik açığının ciddiyeti, istismar edilebilirliği ve potansiyel etkisi ayrı ayrı değerlendirilmesi gerektiğinden, daha yüksek bir sayının mutlaka daha yüksek bir risk seviyesi anlamına gelmediğini belirtmek önemlidir.

Genel Kurumsal Risk Seviyesi

Genel kurumsal risk seviyesi, tespit edilen güvenlik açıklarının ciddiyeti ve istismar edilebilirliği ile bunların kurumun genel güvenlik duruşu üzerindeki potansiyel etkisi dikkate alınarak belirlenir. Kurumun güvenlik tehditlerine karşı savunmasızlığını gösterir ve risk azaltma çabalarının önceliklendirilmesine yardımcı olur.

Tekil Güvenlik Açığı Adeti

5

Bilgi Varlıklarında Bulunan Toplam Açık

8

Kritik

0

Yüksek

0

Orta

3

Düşük

2

Bilgi

0

Genel Risk Seviyesi

Düşük

Geçmiş Sızma Testi Sonuçları

03/11/2025 Tarihli Rapor

Tekil Açık	Toplam Açık	Kritik	Yüksek	Orta	Düşük	Bilgi	Risk Seviyesi
5	8	0	0	3	2	0	Düşük

12/10/2024 Tarihli Rapor

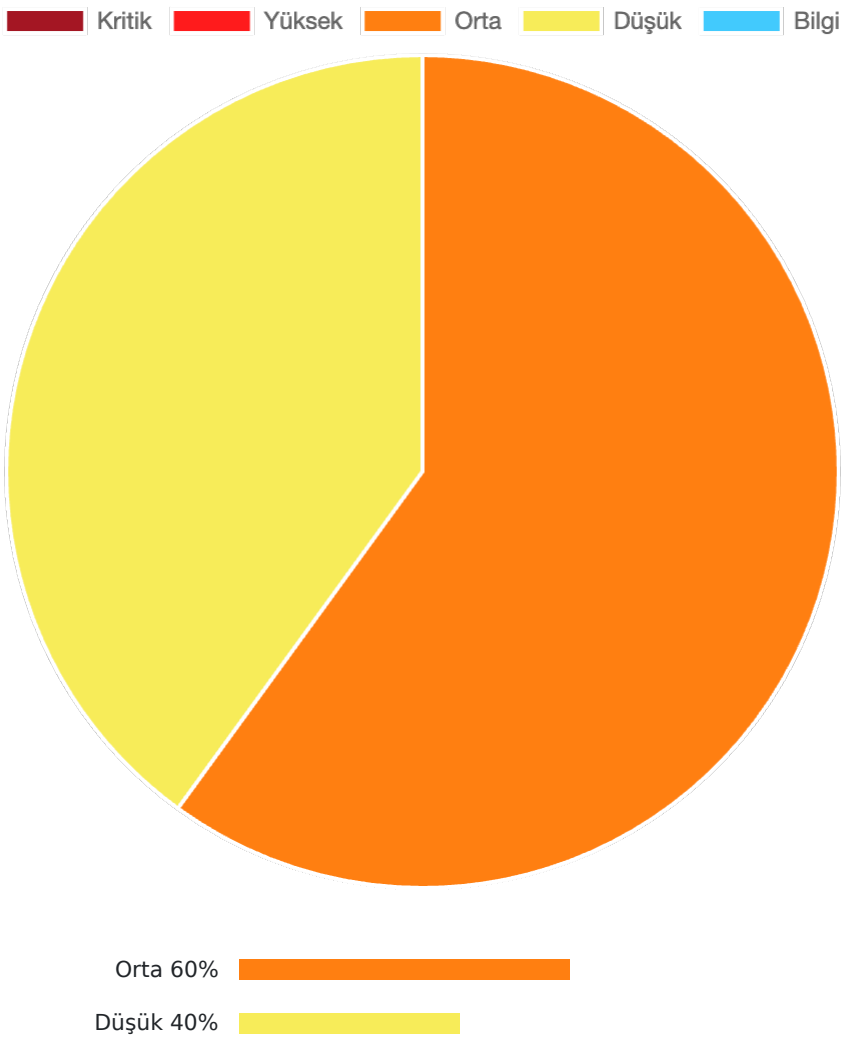
Tekil Açık	Toplam Açık	Kritik	Yüksek	Orta	Düşük	Bilgi	Risk Seviyesi
3	8	0	2	0	1	0	Orta

Güvenlik Açığı Risk Seviyesine Göre Dağılım

Mevcut Rapor - 03/11/2025

Güvenlik açığı risk derecesine göre dağılım, belirlenen güvenlik açıklarını ciddiyetlerine, istismar edilebilirliklerine ve potansiyel etkilerine göre farklı risk seviyelerine ayırır.

Bu analiz, paydaşların genel risk ortamını anlamalarına yardımcı olur ve acil dikkat ve düzeltme gerektiren alanlara ilişkin içgörüler sağlar.

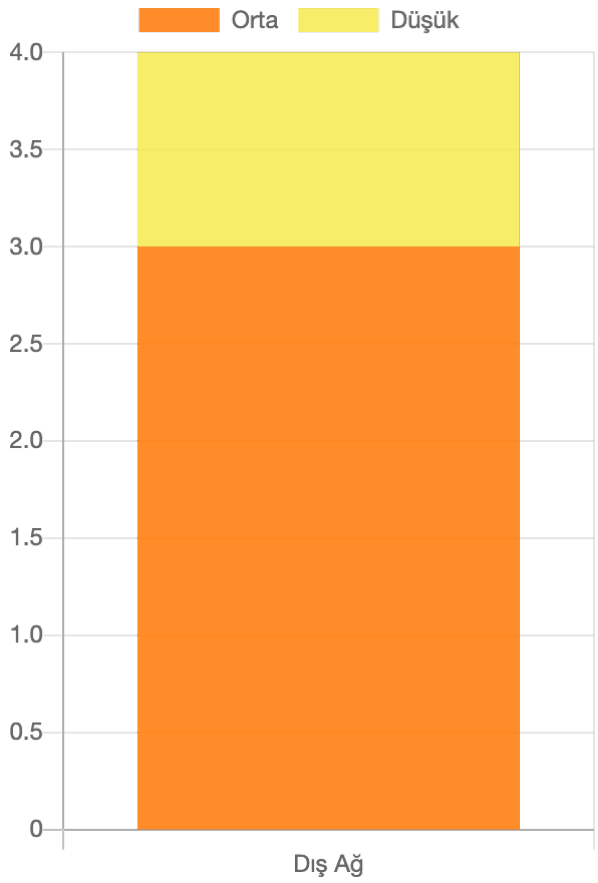


Açıkların Kategorilere Göre Dağılımı

Güvenlik açıklarının kategorilere göre dağılımı bölümü, sızma testi çalışması sırasında tespit edilen güvenlik açıklarını ilgili alanlarına veya türlerine göre kategorize edilmiş şekilde görsel olarak temsil eder.

Bu grafiksel gösterim, paydaşlara güvenlik açıklarının farklı alanlara dağılımına ilişkin açık ve özlü bir genel bakış sunarak eğilimleri belirlemelerine ve iyileştirme çabalarını etkili bir şekilde önceliklendirmelerine olanak sağlamayı amaçlamaktadır.

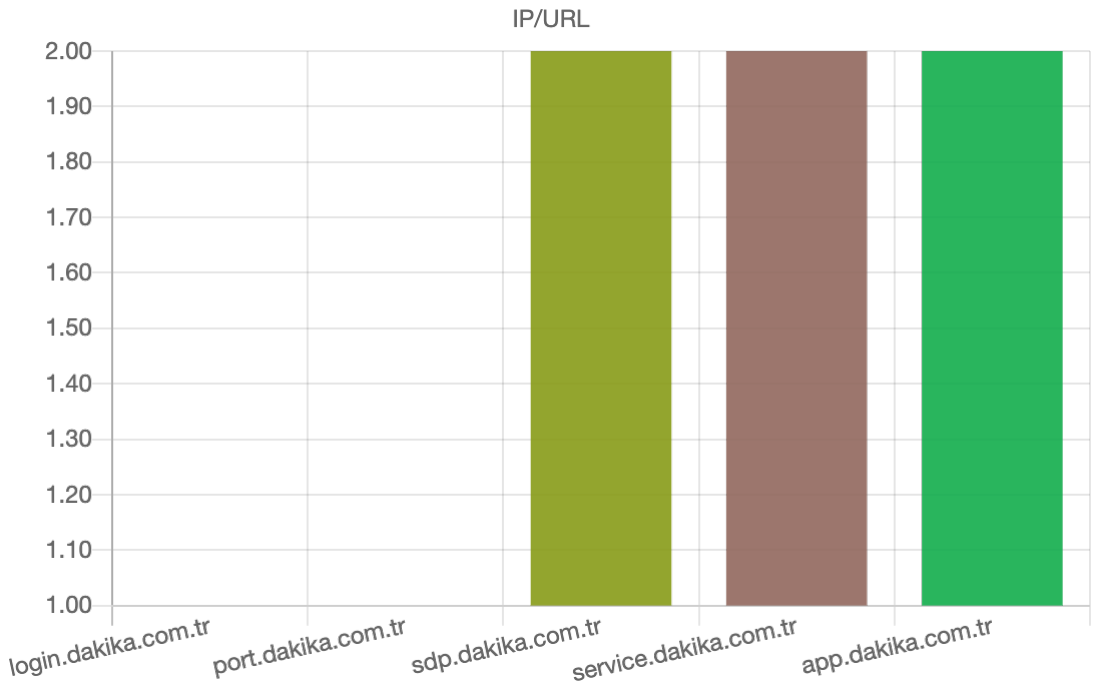
Güvenlik açıkları, etkiledikleri güvenlik açığı, sistem veya teknoloji türüne göre ilgili kategoriler halinde gruplandırılmıştır.

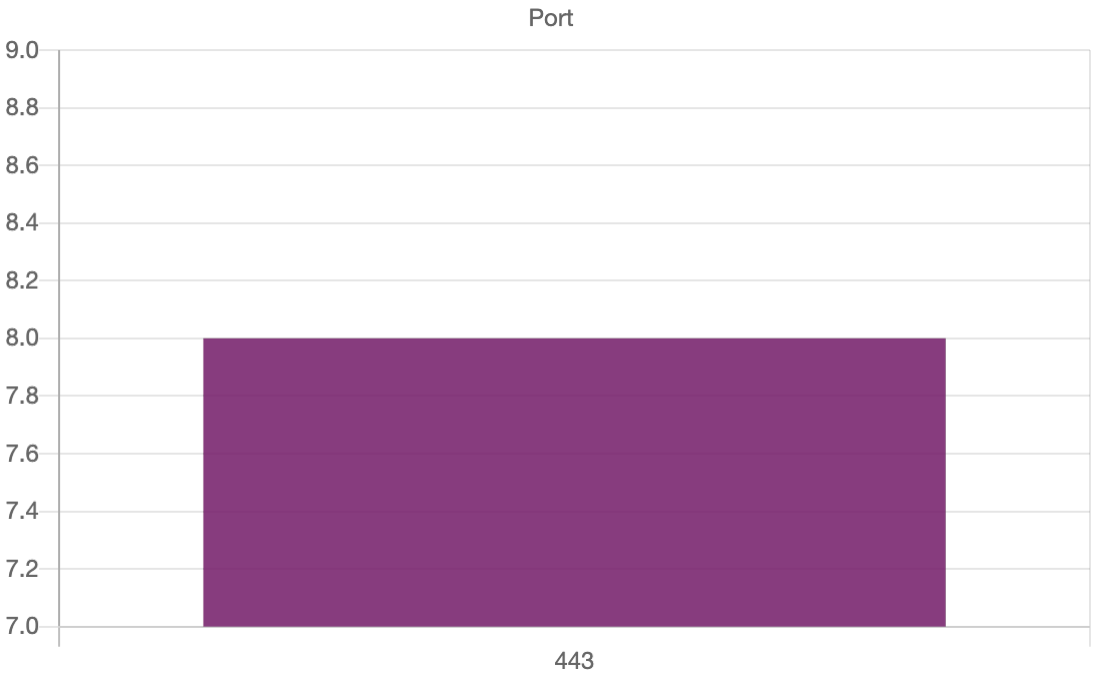


En Çok Açık Görülen Bilgi Varlıkları

En savunmasız bilgi varlıkları, Sızma Testi görevi sırasında en yüksek güvenlik açığı yoğunluğunu gösteren, kuruluşun altyapısındaki belirli IP, URL ve Bağlantı Noktasıdır. Bu varlıklar daha önemli sayıda güvenlik açığına sahip olabilir veya kuruluşun güvenlik duruşu için önemli bir risk oluşturan kritik güvenlik açıkları içerebilir.

En savunmasız bilgi varlıklarının belirlenmesi, paydaşların dikkatlerini ve kaynaklarını bu kritik alanların güvenliğini sağlamaya odaklamalarına yardımcı olur. Kuruluş, bu varlıklardaki güvenlik açıklarını ele alarak genel risk maruziyetini önemli ölçüde azaltabilir ve güvenlik savunmasını geliştirebilir.





Hedef Listesi

Hedef listesi bölümü, Sızma Testi görevi sırasında hedef olarak dahil edilen belirli sistemlere, uygulamalara ve altyapıya genel bir bakış sağlar. Değerlendirmenin kapsamını ve güvenlik açıkları için değerlendirilen varlıkları ana hatlarıyla belirtmeyi amaçlamaktadır.

Bu bölüm, paydaşların Sızma Testinin kapsamını ve kuruluşun genel güvenlik duruşuyla ilgisini anlamaları için çok önemlidir.

195.87.95.57
login.dakika.com.tr
service.dakika.com.tr
sdp.dakika.com.tr

195.87.95.53
port.dakika.com.tr
app.dakika.com.tr

DDoS/DoS Analizi

Datassist Bilgi Teknolojileri A.Ş. için raporda belirtilen hedefler üzerinde detaylı bir analiz yapılmıştır. Bu analizler sonucunda belirli güvenlik açıkları ve riskler tespit edilmiştir. Aşağıda yönetici özeti yer almakta olup, diğer bölümlerde teknik detaylar ve çözüm önerileri açısından risk faktörleri tartışılmaktadır.

Uygulamada etkili bir Content-Security-Policy bulunmadığı tespit edilmiştir. “Content-Security-Policy” başlığının gönderilmemesi veya “unsafe-inline/unsafe-eval” izinleriyle fiilen etkisiz bırakılması nedeniyle inline script engellemesi, kaynak whitelist listesi (script-src, connect-src, img-src) ve frame-ancestors tabanlı clickjacking önlemleri uygulanamamıştır. Bu durum, reflected/stored/DOM-based XSS vektörlerinin gerçek kullanıcı tarayıcılarında alan adı altında çalıştırılmasını mümkün kılmış ve Subresource Integrity (SRI) ile strict-dynamic gibi modern hardening yaklaşımlarının da devreye alınamaması sebebiyle supply-chain kaynaklı kötü niyetli script enjeksiyonlarına açık kapı bırakmıştır. Sonuç olarak, tarayıcı tarafında kod çalıştırma engellenememiş, veri exfiltration istekleri (Fetch/XHR, beacon) aynı origin görünümüyle tespit edilmeden gerçekleştirilebilir hâle gelmiştir; bu zemin, aşağıda açıklanan cookie koruma eksikleri ile birleştirildiğinde session takeover etkisi belirgin biçimde yükselmiştir.

Web uygulaması oturum çerezlerinde “HttpOnly” flaginin tutarlı biçimde uygulanmadığı doğrulanmıştır. HttpOnly eksikliği nedeniyle session cookie değerlerine document.cookie üzerinden script erişimi mümkün olmuş, bu da XSS tetiklenmesi hâlinde session hijacking, CSRF korumalarının atlatılması ve yetkisiz işlem başlatılması gibi sonuçların doğrudan gerçekleşmesine imkan tanımıştır. Ek olarak, aynı oturum çerezlerinde “Secure” flagi kullanımının da tutarsız olduğu gözlemlenmiş ve TLS dışı aktarım senaryolarında (özellikle captive portal veya hatalı yönlendirme anlarında) cookie sızıntısı riski artmıştır. Bu tablo, CSP’nin bulunmaması ile doğrudan ilişkilendirildiğinde, saldırganın tarayıcıda kod çalıştırmasının sadece bilgi sızıntısı ile sınırlı kalmadığı, oturum ele geçirme ve persistence elde etme başarısına dönüştüğü netleşmiştir.

İstemci tarafında kullanılan jQuery kütüphanesinin güncel olmadığı ve bilinen birden fazla zafiyeti içerdiği saptanmıştır. Eski jQuery sürümlerine özgü XSS, prototype pollution ve selector-based injection sınıflarındaki açıklar, dynamic DOM manipulation akışlarında user-controlled input ile doğrudan kesişmekte ve exploit edilmesi pratikte mümkün olmaktadır. Üçüncü taraf jQuery eklentileriyle birleşen bu durum, event handler zincirlerinde güvenilmeyen veri kullanımını artırmış; output encoding ve context isolation uygulanmadığı için script execution bariyerleri etkinleştirilememiştir. Bu koşullar altında, yukarıda belirtilen HttpOnly eksikliği ile birleştiğinde saldırı, tarayıcıdaki kod yürütmeden oturum devralmaya; CSP yokluğuyla birlikte ise kalıcı script yerleşimine ve sessiz veri exfiltration akışlarına evrilmiştir.

HTTP katmanında “X-Content-Type-Options: nosniff” başlığının gönderilmediği doğrulanmıştır. Tarayıcıların MIME sniffing yapabilmesi sonucunda “application/json” veya “text/plain” olarak sunulması gereken içeriklerin belirli koşullarda “text/html” olarak işlenebildiği; JSON/CSV gibi formatların “polyglot” içeriklerle script olarak yürütülebilir hâle geldiği görülmüştür. Özellikle dosya indirme ve JSON API uçlarında content-type zorlamasının bulunmaması, script-gadgets üzerinden XSS tetiklenmesini kolaylaştırmış; bu açık, jQuery kaynaklı DOM bağlamı zafiyetleriyle birleştirildiğinde istismar eşiğini daha da düşürmüştür. Sonuçta, içerik tipinin katı doğrulanmaması sadece istemci tarafında kod çalıştırmayı mümkün kılmakla kalmamış, güvenlik kontrollerinin (ör. CSP yokluğu) zaten zayıf olduğu bir ortamda zincirleme istismar senaryolarına doğrudan hizmet etmiştir.

Sunucu tarafında hata yönetimi kapsamında Tomcat istisna stack izlerinin (Java stack trace) son kullanıcıya sızdığı doğrulanmıştır. Ayrıntılı stack trace çıktıları üzerinden sınıf/ad paket isimleri, çerçeve versiyon bilgileri, uygulama iç dosya/dizin yolları ve belirli kod yolları açığa çıkarılmış; bu bilgiler teknoloji parmak izi çıkarma (fingerprinting), hedefe yönelik exploit seçimi ve güvenlik kontrol atlatma (ör. belirli framework sürümü için bilinen bypass) amaçlarıyla kullanılabilir nitelikte bulunmuştur. Bilgi ifşasının, yukarıda açıklanan client-side zafiyetlerle birleştirildiğinde saldırgana hem doğru payload seçimi hem de lateral hareket planlaması için düşük maliyetli keşif (reconnaissance) sağladığı netleştirilmiştir. Sonuç olarak, eksik CSP ve çerez sertleştirmesi ile başlatılan tarayıcı içi kod çalıştırma, jQuery zafiyetleri ve nosniff eksikliğiyle genişletilmiş; Tomcat stack trace ifşası ile hedefe özgü exploit zincirleri oluşturularak güvenilirlik, bütünlük ve gizlilik üzerinde yüksek etkili, uçtan uca bir risk profili somutlaştırılmıştır.

Yapılan analizler, genel kurumsal risk seviyesinin **DÜŞÜK** düzeyde olduğunu göstermiştir. Raporda belirtilen zafiyetlerin sistematik olarak ele alınması ve gerekli iyileştirmelerin yapılması tavsiye edilmektedir.

Dış Ağ, Sistem ve Web Uygulamaları

ENF473826 - Tomcat Java Stack Trace Bilgi Edinme Zayıflığı

Kullanıcı Profili	Erişim Noktası	CVSS Skoru	Risk Seviyesi
Anonim	Internet	0.1-3.9	Düşük

Etki

Sistem, ağ ve uygulama hakkında bilgi edinme.

Açıklama

Saldırgan Tomcat üzerinden elde ettiği exception dökümünden çeşitli bilgi edinme kategorisinde verileri elde edebilmektedir.

Bu veriler Tomcat dosyalarının fiziksel olarak bulunduğu dizin, detaylı Tomcat versiyonu, exception mesajının neden oluştuğuna dair detaylı döküm gibi bilgilerdir.

Bu bilgiler tek başına tehlikeli olmasa da başka açıklarla birleştiğinde tehlikeli bir durum oluşturabilmektedir.

Çözüm

Sunucudaki web.xml dosyası içerisine aşağıdaki satırların girilmesi gereklidir:

```
<error-page>
   <error-code>500</error-code>
   <location>/server_error.html</location>
</error-page>
```

Bulgunun Tespit Edildiği Bileşenler

IP/URL: login.dakika.com.tr
Port: 443/TCP

Detaylar

Gönderilen istek.

```
POST /recover/password HTTP/1.1
Host: login.dakika.com.tr
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Cookie: SESSION=ZjYwM2RkZTktMDhiMi00YWIzLWI5NTktNWQ1Y2JiYmFkMzc2
Referer: https://login.dakika.com.tr/recover/password
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.140 Safari/537.36

method=3&type=EMAIL&g-recaptcha-response=10000000146&_csrf=ef449935-3cf3-4c73-9946-cf415538876d&identifier=3
```

Alınan cevabın bir kısmına yer verilmiştir.


```
{"violations":[{"field":"method","message":"Failed to convert property value of type 'java.lang.String' to required type 'com.datassist.sso.dto.RecoverPasswordMethod' f
r property 'method'; nested exception is org.springframework.core.convert.ConversionFailedException: Failed to convert from type [java.lang.String] to type [@com.faster
ml.jackson.annotation.JsonProperty com.datassist.sso.dto.RecoverPasswordMethod] for value [3]; nested exception is java.lang.IllegalArgumentException: No enum constant
om.datassist.sso.dto.RecoverPasswordMethod.3"}],"stacktrace":["org.zalando.problem.spring.web.advice.validation.BaseValidationAdviceTrait.newConstraintViolationProblem(
aseValidationAdviceTrait.java:50)","org.zalando.problem.spring.web.advice.validation.BindAdviceTrait.handleBindingResult(BindAdviceTrait.java:30)","java.base/jdk.intern
l.reflect.NativeMethodAccessorImpl.invoke0(Native Method)","java.base/jdk.internal.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:77)","java.base
jdk.internal.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)","java.base/java.lang.reflect.Method.invoke(Method.java:568)","org.spring
ramework.web.method.support.InvocableHandlerMethod.doInvoke(InvocableHandlerMethod.java:205)","org.springframework.web.method.support.InvocableHandlerMethod.invokeForRe
uest(InvocableHandlerMethod.java:150)","org.springframework.web.servlet.mvc.method.annotation.ServletInvocableHandlerMethod.invokeAndHandle(ServletInvocableHandlerMetho
.java:117)","org.springframework.web.servlet.mvc.method.annotation.ExceptionHandlerExceptionResolver.doResolveHandlerMethodException(ExceptionHandlerExceptionResolver.
va:428)","org.springframework.web.servlet.handler.AbstractHandlerMethodExceptionResolver.doResolveException(AbstractHandlerMethodExceptionResolver.java:75)","org.spring
ramework.web.servlet.handler.AbstractHandlerExceptionResolver.resolveException(AbstractHandlerExceptionResolver.java:142)","org.springframework.web.servlet.handler.Hand
erExceptionResolverComposite.resolveException(HandlerExceptionResolverComposite.java:80)","org.springframework.web.servlet.DispatcherServlet.processHandlerException(Dis
atcherServlet.java:1332)","org.springframework.web.servlet.DispatcherServlet.processDispatchResult(DispatcherServlet.java:1143)","org.springframework.web.servlet.Dispat
herServlet.doDispatch(DispatcherServlet.java:1089)","org.springframework.web.servlet.DispatcherServlet.doService(DispatcherServlet.java:965)","org.springframework.web.s
rvlet.FrameworkServlet.processRequest(FrameworkServlet.java:1006)","org.springframework.web.servlet.FrameworkServlet.doPost(FrameworkServlet.java:909)","javax.servlet.h
ttp.HttpServlet.service(HttpServlet.java:555)","org.springframework.web.servlet.FrameworkServlet.service(FrameworkServlet.java:883)","javax.servlet.http.HttpServlet.serv
ce(HttpServlet.java:623)","org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:209)","org.apache.catalina.core.ApplicationFilte
Chain.doFilter(ApplicationFilterChain.java:153)","org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:51)","org.apache.catalina.core.ApplicationFilterCha
n.internalDoFilter(ApplicationFilterChain.java:178)","org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:153)","org.springframework.se
urity.web.FilterChainProxy.doFilterInternal(FilterChainProxy.java:214)","org.springframework.security.web.FilterChainProxy.doFilter(FilterChainProxy.java:181)","org.apa
he.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:178)","org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterCh
in.java:153)","org.springframework.security.saml.SAMLLogoutFilter.processLogout(SAMLLogoutFilter.java:168)","org.springframework.security.saml.SAMLLogoutFilter.doFilte
SAMLLogoutFilter.java:110)","org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:178)","org.apache.catalina.core.ApplicationFil
erChain.doFilter(ApplicationFilterChain.java:153)","org.springframework.security.saml.SAMLLogoutProcessingFilter.processLogout(SAMLLogoutProcessingFilter.java:209)","o
.springframework.security.saml.SAMLLogoutProcessingFilter.doFilter(SAMLLogoutProcessingFilter.java:107)","org.apache.catalina.core.ApplicationFilterChain.internalDoFilt
r(ApplicationFilterChain.java:178)","org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:153)","org.springframework.security.saml.metad
ta.MetadataGeneratorFilter.doFilter(MetadataGeneratorFilter.java:87)","org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:178)
,"org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:153)","org.springframework.security.web.authentication.AbstractAuthenticationProc
ssingFilter.doFilter(AbstractAuthenticationProcessingFilter.java:223)","org.springframework.security.web.authentication.AbstractAuthenticationProcessingFilter.doFilter(
bstractAuthenticationProcessingFilter.java:217)","org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:178)","org.apache.catalin
.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:153)","org.springframework.security.web.authentication.AbstractAuthenticationProcessingFilter.doFilter
AbstractAuthenticationProcessingFilter.java:223)","org.springframework.security.web.authentication.AbstractAuthenticationProcessingFilter.doFilter(AbstractAuthenticatio
ProcessingFilter.java:217)","org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:178)","org.apache.catalina.core.ApplicationFil
erChain.doFilter(ApplicationFilterChain.java:153)","org.springframework.security.saml.metadata.MetadataDisplayFilter.doFilter(MetadataDisplayFilter.java:84)","org.apach
.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:178)","org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChai
.java:153)","org.springframework.security.saml.SAMLDiscovery.doFilter(SAMLDiscovery.java:137)","org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(Applica
ionFilterChain.java:178)","org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:153)","org.springframework.security.saml.SAMLEntryPoint.
oFilter(SAMLEntryPoint.java:102)","org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:178)","org.apache.catalina.core.Applicat
onFilterChain.doFilter(ApplicationFilterChain.java:153)","org.springframework.security.web.FilterChainProxy$VirtualFilterChain.doFilter(FilterChainProxy.java:337)","org
springframework.security.web.access.intercept.FilterSecurityInterceptor.invoke(FilterSecurityInterceptor.java:115)","org.springframework.security.web.access.intercept.F
lterSecurityInterceptor.doFilter(FilterSecurityInterceptor.java:81)","org.springframework.security.web.FilterChainProxy$VirtualFilterChain.doFilter(FilterChainProxy.jav
:346)","org.springframework.security.web.access.ExceptionTranslationFilter.doFilter(ExceptionTranslationFilter.java:122)","org.springframework.security.web.access.Excep
ionTranslationFilter.doFilter(ExceptionTranslationFilter.java:116)","org.springframework.security.web.FilterChainProxy$VirtualFilterChain.doFilter(FilterChainProxy.java
346)","org.springframework.security.web.session.SessionManagementFilter.doFilter(SessionManagementFilter.java:126)","org.springframework.security.web.session.SessionMan
gementFilter.doFilter(SessionManagementFilter.java:81)","org.springframework.security.web.FilterChainProxy$VirtualFilterChain.doFilter(FilterChainProxy.java:346)","org.
springframework.security.web.authentication.AnonymousAuthenticationFilter.doFilter(AnonymousAuthenticationFilter.java:109)","org.springframework.security.web.FilterChain
roxy$VirtualFilterChain.doFilter(FilterChainProxy.java:346)","org.springframework.security.web.servletapi.SecurityContextHolderAwareRequestFilter.doFilter(SecurityConte
tHolderAwareRequestFilter.java:149)","org.springframework.security.web.FilterChainProxy$VirtualFilterChain.doFilter(FilterChainProxy.java:346)","org.springframework.sec
rity.web.savedrequest.RequestCacheAwareFilter.doFilter(RequestCacheAwareFilter.java:63)","org.springframework.security.web.FilterChainProxy$VirtualFilterChain.doFilter(
ilterChainProxy.java:346)","org.springframework.security.web.FilterChainProxy.doFilterInternal(FilterChainProxy.java:214)","org.springframework.security.web.FilterChain
roxy.doFilter(FilterChainProxy.java:181)","org.springframework.security.web.FilterChainProxy$VirtualFilterChain.doFilter(FilterChainProxy.java:346)","org.springframewor
.security.web.authentication.www.BasicAuthenticationFilter.doFilterInternal(BasicAuthenticationFilter.java:164)","org.springframework.web.filter.OncePerRequestFilter.do
ilter(OncePerRequestFilter.java:117)","org.springframework.security.web.FilterChainProxy$VirtualFilterChain.doFilter(FilterChainProxy.java:346)","org.springframework.se
urity.web.authentication.AbstractAuthenticationProcessingFilter.doFilter(AbstractAuthenticationProcessingFilter.java:223)","org.springframework.security.web.authenticat
on.AbstractAuthenticationProcessingFilter.doFilter(AbstractAuthenticationProcessingFilter.java:217)","org.springframework.security.web.FilterChainProxy$VirtualFilterCha
n.doFilter(FilterChainProxy.java:346)","org.springframework.security.web.authentication.AbstractAuthenticationProcessingFilter.doFilter(AbstractAuthenticationProcessing
```

ENF168641 - Eksik X-Content-Type-Options Header Zayıflığı

Kullanıcı Profili	Erişim Noktası	CVSS Skoru	Risk Seviyesi
Anonim	Internet	4.0-6.9	Orta

Etki

Tarayıcılar yanıt türünü MIME-sniffing ile yanlış yorumlayabilir; özellikle dosya yükleme akışlarında script olarak yürütülme riski doğar. Bu, XSS, içerik enjeksiyonu ve kullanıcı verisinin ifşası ile hesap ele geçirmeye yol açabilir.

Açıklama

Hedef uygulamanın HTTP yanıtlarında X-Content-Type-Options başlığının bulunmaması, tarayıcıların içerik tipini yanıt gövdesinden “tahmin ederek” farklı bir MIME türü gibi işlemesine izin verir. Özellikle kullanıcı tarafından yüklenen dosyaların (örneğin “image/png” veya “text/plain” olarak sunulan fakat içine HTML/JS gömülmüş içerikler) yayınlandığı akışlarda, bu gevşek davranış tarayıcıya içeriği betik gibi yorumlatabilir ve istemci tarafında code execution’a zemin hazırlar.

Modern tarayıcılar nosniff olmadan yanlış/eksik Content-Type ile servis edilen CSS/JS kaynaklarını daha toleranslı biçimde işler; bu da supply-chain sorunları veya dosya barındırma modülleriyle birleştiğinde XSS etkisini büyütür.

Çözüm

Tüm yanıtlar için X-Content-Type-Options: nosniff başlığını etkinleştirin ve her kaynağı doğru Content-Type ile tutarlı şekilde servis edin (ör. application/javascript, text/css, image/png). Kullanıcı yüklemeleri için sıkı sunucu-tarafı doğrulama ve tip tespiti yapın, tehlikeli içerikleri reddedin ya da güvenli depoda izole edin; görüntüleme gerekiyorsa yalnızca güvenli tiplerle sunun, mümkün olduğunda Content-Disposition: attachment kullanarak tarayıcıda yürütülmesini engelleyin.

Statik dosya/CDN veya reverse proxy katmanında tutarlı MIME eşlemesi uygulayın ve otomatik tip “sniffing”/eşleştirme özelliklerini kapatın. Değişiklik sonrası uygulamayı yeniden tarayıcı ve güvenlik taramalarıyla doğrulayın.

Referanslar/CWE ID

CWE-693: https://cwe.mitre.org/data/definitions/693.html

CWE-79: https://cwe.mitre.org/data/definitions/79.html

Bulgunun Tespit Edildiği Bileşenler

IP/URL: port.dakika.com.tr
Port: 443/TCP

IP/URL: sdp.dakika.com.tr
Port: 443/TCP

ENF603251 - Web Uygulaması HttpOnly Zayıflığı

Kullanıcı Profili	Erişim Noktası	Risk Seviyesi
Anonim	Internet	Düşük

Etki

Olası zararlı Script çalıştırma, kullanıcı veri gizliliğinin ihlali.

Açıklama

Web uygulamasında yapılan analizlerde kullanılan Cookie'lerin HttpOnly olarak işaretlenmediği tespit edilmiştir. Bugünün Web dünyasında, kullanıcıya ait pek çok değerin, daha zengin bir etkileşim için saklanıp, Javascript kütüphaneleri tarafından okunabilmesinin sayısız faydaları olsa da, bazı Cookie'lerin, örneğin Javascript'i hiç ilgilendirmeyen, sadece kullanıcının yetkili bir kişi olduğunu server'a bildirmek için set edilmiş Session Cookie'lerini okuyabilmesinin gereği yoktur. Gerek olmadığı gibi böyle bir durum, XSS zafiyeti gibi diğer parametrelerle bir arada düşünüldüğünde oldukça tehlikeli bir hâl alabilir.

Bu sebepten ötürü 2002 yılında Microsoft tarafından geliştirilen ve sonrasında Cookie spesifikasyonuna da eklenip, bugün tüm modern browserlar tarafından desteklenen httpOnly flag'ı kullanıma sunulmuştur.

Sunucu tarafından browser belleğine kaydedilen Cookie eğer bir httpOnly belirteci içeriyor ise, bu Cookie yalnızca HTTP isteklerine eklenir ve Javascript tarafından okunup, manipüle edilemez. HttpOnly belirteci ile bir Cookie tanımlamak için, Cookie tanımına httpOnly ifadesini eklemek yeterlidir.

Cookie'lerin bu şekilde işaretlenmediği durumlarda, kullanıcı taraflı bazı zararlı JavaScript kodları Cookie'leri okuyabilmektedir. Bu bağlamda HttpOnly işareti Cross Site Scripting saldırılarına karşı etkin bir ek koruma sunmaktadır.

Cookie adı: JSESSIONID

Çözüm

Oturumda kullanılan tüm Cookie'lere HttpOnly etiketi eklenmelidir.

Bulgunun Tespit Edildiği Bileşenler

IP/URL: service.dakika.com.tr
Port: 443/TCP

IP/URL: app.dakika.com.tr
Port: 443/TCP

ENF016619 - JQuery Çoklu Zayıflıklar

Kullanıcı Profili	Erişim Noktası	CVSS Skoru	Risk Seviyesi
Anonim	Internet	4.0-6.9	Orta

Etki

XSS ve prototype pollution üzerinden client-side arbitrary JS execution mümkün; bu da hesap ele geçirme, yetkisiz işlem, veri sızıntısı ve içerik/işlev manipülasyonu risklerini doğurur, uygulama genelinde geniş saldırı yüzeyi yaratır.

CVE ID

CVE-2012-6708	CVE-2015-9251	CVE-2019-11358
CVE-2020-7656	CVE-2020-11022	CVE-2020-11023

Açıklama

Hedef uygulamada jQuery 1.7.2 kullanımı tespit edilmiştir. Bu sürüm, birden fazla bilinen zafiyetin etki aralığındadır (CVE-2012-6708, CVE-2015-9251, CVE-2019-11358, CVE-2020-7656, CVE-2020-11022, CVE-2020-11023) ve bunların ortak paydası, untrusted input'un DOM'a güvensiz işlenmesi veya obje prototiplerinin manipülasyonu yoluyla istemci tarafında keyfi kod çalıştırma ya da uygulama davranışını saldırgan lehine değiştirme imkânıdır.

Bu, authentication/authorization katmanları aşılmış olsa dahi kullanıcı bağlamında yüksek ayrıcalıklı işlemlerin kötüye kullanılabilmesi anlamına gelir.

Mevcut jQuery versiyonu 1.3.2. Son yayınlanan jQuery versiyonu 3.7.1

https://service.dakika.com.tr/payroll/a4j/g/3_3_3.Final/org/ajax4jsf/framework.pack.js

https://app.dakika.com.tr/payroll/a4j/g/3_3_3.Final/org/ajax4jsf/framework.pack.js

Çözüm

jQuery bağımlılığını öncelikli olarak en az 3.7.1'e (veya kurum standardına uygun en güncel 3.x'e) yükseltin; XSS ile ilgili kritik düzeltmeler 3.5+ sürümlerinde yer aldığı için geçiş testlerini bu kırılım esas alınarak gerçekleştirin.

Kod tarafında .html()/append() gibi DOM manipulation çağrılarına untrusted input vermekten kaçının; mümkün olduğunda .text() veya güvenli templating kullanın, $.ajax için dataType'ı açıkça tanımlayın ve .load() kullanımını gözden geçirip kaldırın ya da güvenli alternatiflerle değiştirin. Defense-in-depth kapsamında katı bir CSP uygulayın, CDN bağımlılıkları için SRI kullanın ve uygulamayı tek, güncel bir jQuery kopyasına standardize ederek eski kütüphane sürümlerini tamamen temizleyin.

Referanslar/CWE ID

CWE-79: https://cwe.mitre.org/data/definitions/79.html

CWE-1321: https://cwe.mitre.org/data/definitions/1321.html

Bulgunun Tespit Edildiği Bileşenler

IP/URL: service.dakika.com.tr
Port: 443/TCP

IP/URL: app.dakika.com.tr
Port: 443/TCP

ENF585303 - Eksik Content Security Policy (CSP) Zayıflığı

Kullanıcı Profili	Erişim Noktası	CVSS Skoru	Risk Seviyesi
Anonim	Internet	4.0-6.9	Orta

Etki

Etkin bir CSP olmadığında XSS ve benzeri client-side injection'ların başarı olasılığı ve etkisi artar; inline script yürütme, veri sızdırma, session hijacking ve kötü amaçlı üçüncü taraf script/CDN üzerinden keyfi kod çalıştırma riski büyür.

Açıklama

Hedef uygulama HTTP yanıtlarında Content-Security-Policy başlığı göndermediği için tarayıcı, script, style, img ve connect gibi kaynakların nereden ve nasıl yüklenebileceğine dair kısıtlar uygulamaz. Bu durum, mevcut veya gelecekte ortaya çıkabilecek XSS/HTML injection açıklarının istismar edilmesini kolaylaştırır; inline event handler'lar, eval() benzeri evaluation fonksiyonları ve kontrolsüz üçüncü taraf script'ler aracılığıyla istemci tarafında code execution, veri sızdırma ve oturum istismarı senaryolarının önünü açar.

CSP bulunmaması katmanlı savunmayı ortadan kaldırır ve supply-chain risklerini (kompromize CDN/analytics tag'leri vb.) büyütür.

Çözüm

HTTP yanıtlarına kurumsal ihtiyaçlara göre kısıtlayıcı bir CSP ekleyin ve aşamalı geçiş için önce Report-Only modda ihlal kayıtlarını toplayın. Üretimde default-src 'self' gibi bir taban kural tanımlayıp script-src 'self' 'nonce-<random>' 'strict-dynamic' veya hash-tabanlı (sha256-...) kontrol kullanın; inline script'leri mümkünse kaldırın, unsafe-inline ve unsafe-eval'den kaçının.

Potansiyel saldırı yüzeylerini kapatmak için object-src 'none', base-uri 'self' ve clickjacking'e karşı frame-ancestors 'none' (veya izinli origin listesi) uygulayın; yalnız gerekli üçüncü taraf alan adlarını açıkça allow-list'e ekleyin, karışık içerikleri engellemek için upgrade-insecure-requests/block-all-mixed-content kullanın ve dış bağımlılıklarda Subresource Integrity (SRI) etkinleştirin. Politika devredeyken uygulamayı tarayıcı konsolu ve raporlama uç noktaları üzerinden izleyip gereksiz izinleri kaldırarak politikayı sıkılaştırın.

Referanslar/CWE ID

CWE-79: https://cwe.mitre.org/data/definitions/79.html

CWE-693: https://cwe.mitre.org/data/definitions/693.html

Bulgunun Tespit Edildiği Bileşenler

IP/URL: sdp.dakika.com.tr
Port: 443/TCP

Sonuç

TerraMedusa ile çalıştığınız için teşekkür ederiz. Sadece en üst düzeyde servis hizmetinden değil aynı zamanda TerraMedusa tarafından sunulan benzersiz avantajlardan da yararlanmış bulunmaktasınız. Lütfen bu raporla ilgili her türlü destek için bilgi@terramedusa.com adresinden bize ulaşın.

Deneyim

TerraMedusa olarak bilgi güvenliği pazarında dünya çapındaki çoğu büyük firma için bu konuda en güvenilir danışman durumundayız. Üst yönetim ile direkt olarak çalışmamızın yanı sıra, bazı durumlarda gün bazında danışmanlık ve veri aktarımı sağlanması da sunduğumuz servisler arasında yer almakta. Bizden en çok talep edilen hizmet ise; bilgi güvenliği konusunda yardım alınan diğer danışmanların işlerinin kontrol edilerek, yönetime nihai tavsiyelerimizin sunulması şeklinde.

Güvenlik hizmeti sunduğumuz uzun müşteri listemiz, büyük ölçekli firmalar yanında küçük ölçekli firmalar olmak üzere hükümet, askeri, adli ve kamu vs. gibi çeşitli birçok sektörden gelen firmalardan oluşmakta. Özel sektör müşterilerimiz ise ulaştırma ve enerjiden haberleşmeye, sigorta ve finansal olmak üzere geniş bir alana yayılmış durumda.

Bilgisayar güvenliği konusunda alanımızda günden güne artan bir üne sahip olmak ve müşterilerimizin olumlu yöndeki övücü referanslarını toplamak bizim için gurur verici. Öyleki işimizin ciddi bir kısmını tekrar hizmet almak isteyen eski müşterilerimiz oluşturmakta.

Uzmanlık

Deneyimlerimiz profesyonelce yönetilen web sitelerinde dahi tespit edilememiş güvenlik sorunlarının ortaya çıktığını göstermiştir. TerraMedusa'nın büyük muhasebe ve denetim firmaları gibi güçlü rakiplerinin ardından gerçekleştirdiği Sızma Testleri, birçok durumda rakipleri tarafından kullanılan otomatik test sistemlerinin açığa çıkaramadığı problemler bulmuştur.

TerraMedusa olarak bilgi güvenliği denetiminde proaktif yaklaşım ile sızma testlerinde öncü durumdayız. Diğer herkes gibi ticari test paketlerine güvenmek yerine işlerimizi yürütürken beyin gücünden yararlanmayı tercih ediyoruz; aynı hackerların, ağınızı ele geçirmek için pahalı test araçlarını kullanmadıkları gibi. Her ağı yeni ve benzersiz güvenlik açıkları için analiz ederek, size özel araçlar geliştiriyoruz. Kendi araştırmamızı yapıp, araçlarımızı kendimiz yazıyoruz.

Çalışma prensibimiz hem firmanızın hem de ağınızın ihtiyacını karşılamak üzere tasarlanmıştır. Sonuçta hiç bir iki firma aynı olmadığı gibi hiçbir iki ağ da birbiriyle aynı değil. Jenerik ağları incelemek için yazılan araçlar firmanızın sürekli olarak değişen güvenlik ortamını dikkate almazlar.

Otomatik bir yazılı sürece dayanan yaklaşım potansiyel herhangi bir problemin efektif olarak test edilmesini imkânsız kılacaktır. Otomatik araçların bizim için iş yapmasına güvenmediğimizden, size rakiplerimizden alacağınızdan daha kapsamlı olarak gerçekleştirilecek değerlendirmeler sunuyoruz.

Daha iyi bir işbirliği

Tavsiyelerimiz çok nadir olarak müşterilerimizin yeni ekipman satın almasına yöneliktir. Çalışma hayatımız boyunca elde ettiğimiz deneyimler, çoğu güvenlik probleminin hiç para harcamadan düzeltilebileceğini göstermiştir. Rakiplerimizin aksine, size ihtiyacınız olmayacak pahalı donanım ve yazılım araçlarını satın almanızı önermiyoruz.

TerraMedusa'nın benzersiz yaklaşımı, bize her müşteri bazında öneriler sunmamızı sağlıyor. Ek ürünlerin satın alınması gereken durumlarda ise ağınıza özgü değişen fiyatlarda farklı birçok yaklaşım öneriyoruz.

Teknik deneyimimiz, seçkin ünümüz ve özel ilgimiz ile size piyasadaki başka hiçbir güvenlik firması tarafından sağlanamayacak seviyede bir servis hizmetini garanti ediyoruz. Bir TerraMedusa müşterisi olarak, ağınızın güvenliğini geliştirmek amacıyla aldığınız karardan dolayı kendinizi güvende hissedebilirsiniz.

TerraMedusa Bilişim Güvenliği Çözümleri Ltd. Şti.

Mall of İstanbul The Office No:7/E Kat:17 Daire:136 34490 Başakşehir İstanbul
+90 212 671 84 44

https://terramedusa.com
bilgi@terramedusa.com