Esbilgi Teknolojileri
You Are Secured...

ESBİLGİ TEKNOLOJİLERİ SAN. TİC.LTD.ŞTİ.

Ticimax Bilişim Teknolojileri A.Ş.

Güven Damgası Testi Sonuç Raporu

Versiyon 1.0

Güven Damgası Testi Tarihi : 01.06.2024 - 07.06.2024

Esmer Bilgi Teknolojileri San. Tic. Ltd. Şti.
Saray Mah. Küçüksu Cad. No:64/A Antasya Residance Ümraniye/İstanbul
Telefon : +90 216 606 0287
Email : info@esbilgi.com

Esbilgi Teknolojileri
You Are Secured...

Döküman Künyesi		
Sızma Testine Ait Bilgiler	Proje Adı	**Ticimax Bilişim Teknolojileri A.Ş. Güven Damgası Testi**
	Faaliyet Başlangıç Tarihi	**01.06.2024**
	Faaliyet Bitiş Tarihi	**07.06.2024**
	İcra Eden Personel Kimlikleri	**Utku YILDIRIM**
	Rapor Adı	**Ticimax Bilişim Teknolojileri A.Ş. Güven Damgası Testi Sonuç Raporu**
	Rapor İlk Yayın Tarihi	**08.06.2024**
	Rapor Revizyon No	-

Testte Kullanılan Veriler
Blackbox test metodolojisi ile gerçekleştirilmiştir.

Doğrulama Testi			
Doğ.No.	**Doğrulama Tarihi**	**Doğrulamayı Yapan**	**Doğrulama Açıklaması**
-	-	-	-

İçindekiler

Tablo Listesi

1. GİRİŞ

Bu rapor, Esbilgi Teknolojileri tarafından "**TICIMAX BILIŞIM TEKNOLOJILERI A.Ş.**" kurumuna ait kapsam bölümünde verilen varlıklar üzerindeki güvenlik zafiyetlerini ortaya çıkarmak amacı ile **01.06.2024** - **07.06.2024** tarihleri arasında gerçekleştirilen güvenlik ve sızma testlerinin detaylı sonuçlarını içermektedir.

Sızma testi çalışması kapsamında "**TICIMAX BILIŞIM TEKNOLOJILERI A.Ş.**" altyapısı ve sunucularının çalışmasını olumsuz yönde etkileyecek araçlar ve yöntemler kullanılmamış, izinsiz ve yetkisiz bir şekilde hizmetin aksamasına neden olabilecek herhangi bir işlem gerçekleştirilmemiştir.

Rapor, testin yapıldığı anda kapsamda belirtilen sistemlerin bilinen güvenlik açıkları açısından durumunu göstermektedir. Testler için planlanan zaman çerçevesinde, kapsam dâhilindeki sistemlerin üzerinde bulunan açıklıkların azamisinin tespit edilerek raporlanması hedeflenmiştir. Ancak hedefe odaklanmış, yeterince donanımlı, kaynağa ve çok daha fazla zamana sahip saldırganların, bu raporda belirtilen güvenlik açıklarından belki daha fazlasını bulup, kötüye kullanması olasılığı her zaman bulunmaktadır.

2. SIZMA TESTİ HAKKINDA BİLGİLENDİRME

Proje Kapsamı

TICIMAX BILIŞIM TEKNOLOJILERI A.Ş. Güven Damgası Testi: Aşağıdaki tabloda belirtilen sızma testi kapsamına karşı saldırı ve güvenlik testleri gerçekleştirilmiştir. Bu testler esnasında, test edilen sunucu tarafından verilen hizmetlerin sekteye uğratılmaması amacıyla Denial of Service (DoS) saldırıları ve bellek taşması tipi zayıflıkları kullanan saldırılar gerçekleştirilmemiştir.

Güvenlik Testinin Yapıldığı Kapsam Bilgisi
guvendamgasi.ticimaxtest.com

Tablo 1 : Güvenlik Testinin Yapıldığı Kapsam Bilgisi

Test Yöntemi

Saldırı ve güvenlik testleri, kullanılan sunucu, uygulama yapısı veya teknolojisi hakkında sorumlulardan bilgi edinilmeden gerçekleştirilmiş olup “siyah kutu” (black box) olarak nitelendirilmektedir. Bu sebeple test sonucunda mantıksal güvenlik açıklıkları, olası güvenlik açıkları, yanlış yapılandırmalar, savunma önlemlerinin eksikliklerinin tespiti için saldırgan bakış açısıyla yapılmış bir çalışma ortamı olarak düşünülebilir.

Testler, Esbilgi Teknolojileri sızma testi ekibi tarafından gerçekleştirilmiştir. Testler sırasında çeşitli ticari tarama ürünleri, herkes tarafından temin edilebilecek açık kaynak kodlu programlar ve ekip tarafından geliştirilmiş yardımcı program ve araçlar kullanılmıştır.

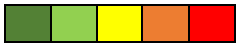
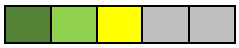
Bulunan her güvenlik açığı veya sistemler hakkında bilgi toplamaya yarayan her türlü bilgi sızıntısı, kurumun bilgi sistemlerinin güvenliği için oluşturduğu tehdit açısından önem sırasına göre değerlendirilmelidir. Her kurumun kaynakları sınırlı olduğu göz önünde tutulduğunda, bulunan güvenlik açıklarını kapatmak için harcanacak olan kaynakların bu önem sırasına göre ayrılması önerilmektedir. Yapılan çalışma sonucunda ortaya çıkarılan güvenlik açıkları, aşağıda anlatılan risk değerlendirmesi yöntem ve kıstaslarına göre sınıflandırılmıştır.

Bulguların Önem Derecesi Sınıflandırması

Bulunan her güvenlik açığı veya sistemler hakkında bilgi toplamaya yarayan her türlü bilgi sızıntısı, kurumun bilgi sistemlerinin güvenliği için oluşturduğu tehdit açısından önem sırasına göre değerlendirilmelidir. Her kurumun kaynakları sınırlı olduğuna göre, bulunan güvenlik açıklarını kapatmak için harcanacak olan kaynakların bu önem sırasına göre ayrılması gerekir. Yapılan çalışma sonucunda ortaya çıkarılan güvenlik açıkları, aşağıda anlatılan yöntem ve kıstaslarına göre sınıflandırılmıştır.

Bulunan güvenlik açıkları, önem seviyesi Acil, Kritik, Yüksek, Orta, Düşük olmak üzere belirlenmiştir. Acil ya da Kritik öneme sahip açıklıklar sonuç raporu beklenmeden hemen standart bir form aracılığıyla sorumlular ile paylaşılır.

Raporda yer alan her bir güvenlik açığına, yukarıda anlatılan önem derecelerinden biri atanır. Önem derecelerinin açıklamaları aşağıdaki tablolardan incelenebilir.

Bulgu Önem Dereceleri		
Acil		Bir sistemin veya uygulamanın güvenlik açığı, çok yetenekli olmayan kötü niyetli bir saldırgan tarafından her an sömürülebilir olan bulgulardır. Bu tür bir bulgu, sistemin genel güvenliğini ciddi şekilde tehlikeye atabilir ve derhal düzeltilmesi gereken açıklıklardır.
Kritik		Kritik bulgular, genellikle saldırganların sistemi kolayca ele geçirmelerine veya önemli bir zarar vermelerine olanak tanıyan yüksek riskli açıklardır. Genellikle sömürmek için yetenek gereksinimi bulunur.
Yüksek		Önemli bir güvenlik zafiyeti içeren, ancak doğrudan bir saldırıya yol açma potansiyeli daha düşük olan açıklıklardır. Yine de, bu tür açıklar ciddi bir şekilde ele alınmalı ve mümkün olan en kısa sürede düzeltilmelidir.
Orta		Orta seviye, belirli bir risk taşıyan ancak acil müdahale gerektirmeyen güvenlik açıklarını ifade eder. Bir uygulamanın orta seviye bulgu ile canlıya alınması uygun değildir.
Düşük		Düşük öneme sahip açıklıklar ise etkilerinin tam olarak belirlenemediği ve literatürdeki en iyi sıkılaştırma yöntemlerinin izlenmemesinden kaynaklanan eksikliklerdir.

Tablo 2 : Bulgu Önem Dereceleri

3. YÖNETİCİ ÖZETİ

Esbilgi Teknolojileri sızma testi ekibi tarafından **TICIMAX BILIŞIM TEKNOLOJILERI A.Ş.** sistemleri üzerine yetkisiz erişim elde edilmesine veya hassas bilgilere ulaşılmasına neden olabilecek güvenlik açıklarının istismar edilmeden önce tespit edilerek düzeltilmesi maksadıyla **01.06.2024** – **07.06.2024** tarihleri arasında güvenlik testleri icra edilmiştir.

Testlerin sonuçları bu bölümde özetlenmiştir. Denetlenen sistemlerde tespit edilen bulguların detaylı açıklamaları raporun ilgili bölümlerinde yer almaktadır. Güvenlik testleri gerçekleştirilirken, kurum faaliyetlerinin aksamasına ve hizmet kesintisine yol açmayacak yöntemler kullanılmasına dikkat edilmiştir. Hizmet kesintisine yol açabilecek tüm testler kurum ile koordineli bir şekilde planlanarak gerçekleştirilmiştir.

En Yüksek Bulgu Önem Dereceleri	
Güven Damgası Testi	**Orta**

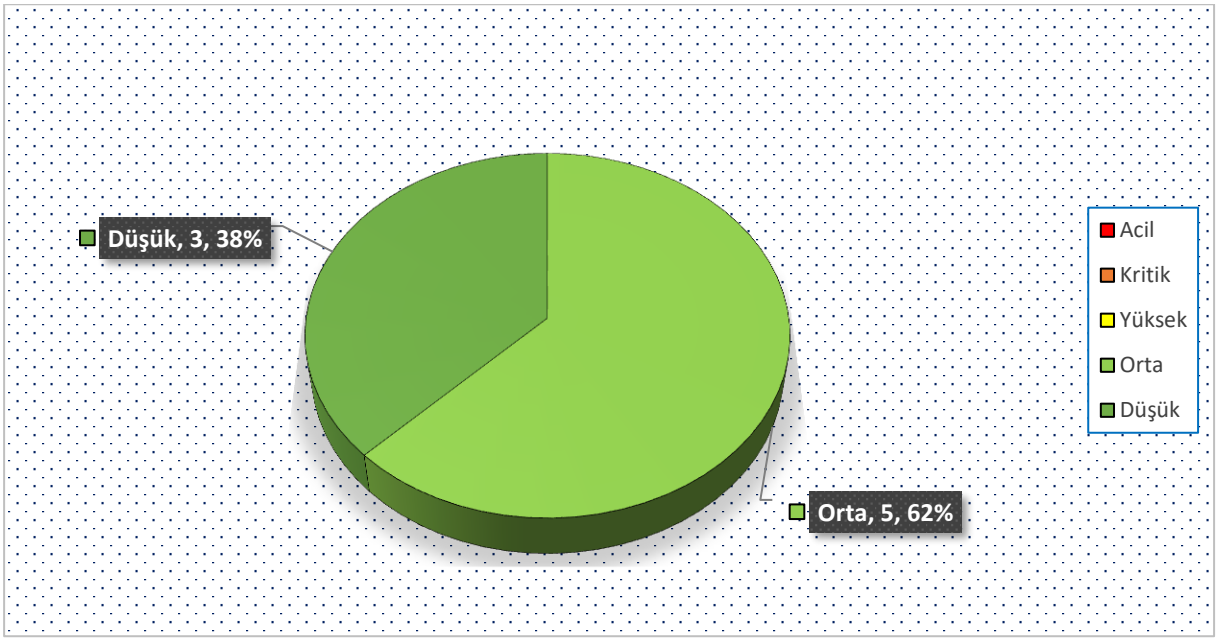
Tablo 3 : Güvenlik Testi En Yüksek Bulgu Önem Dereceleri

Gerçekleştirilen her bir test kapsamında tespit edilen bulgular içerisinde bulunan en yüksek bulgu önem derecesi ilgili testin karşısında Tablo 4'te belirtilmiştir. Söz konusu testler süresince bulgu önem dereceleri belirlenirken varlığın değeri dikkate alınmamıştır. Varlık değerlendirmesi yapma ve varlıkların öncelik derecelerine göre düzeltmeleri yapma işlemleri uygulamadan sorumlu birime bırakılmıştır.

Gerçekleştirilen güvenlik testlerin genelinde bulunan bulguların önem derecelerinin dağılım oranları Şekil-1'de belirtilmiştir. Özetle; test genelinde toplam **8** adet bulgu tespit edilmiştir. Bu bulguların %62'si **Orta (5 Adet)** ve %38'i **Düşük (3 Adet)** önem derecesindedir.

Bulgu Önem Dereceleri Dağılım Grafiği

Aşağıdaki pasta grafiğinde test edilen varlıklar üzerinde tespit edilmiş olan zafiyetlerin önem derecelerine göre dağılımı bulunmaktadır.



Şekil 1 : Bulgu Önem Dereceleri Dağılım Grafiği

Bulgu Önem Derecelerinin Test Türlerine Göre Dağılımı

	ACİL	KRİTİK	YÜKSEK	ORTA	DÜŞÜK	TOPLAM
Güven Damgası Testi	-	-	-	5	3	8
TOPLAM	-	-	-	5	3	8

Tablo 4 : Bulgu Önem Derecelerinin Test Türlerine Göre Dağılımı

Güven Damgası Testleri'nde kapsamdaki tüm varlıklar blackbox sızma testi metodolojisi ile sızma testine tabi tutulmuştur. Yapılan incelemeler sonucunda, sistemde girdi validasyonu eksikliği, etkisiz oturum sonlandırma fonksiyonu ve açık yönlendirme zafiyeti gibi önemli güvenlik açıkları tespit edilmiştir. Ayrıca, yönetim arayüzlerinin dışarıdan erişime açık olması, eksik HTTP güvenlik başlıkları bulunması, çerezlerde http only ve secure bayrakları bulunmaması, zafiyetli javascript kütüphaneleri kullanımı gibi bulgulara ulaşılmıştır.

Raporun ilerleyen bölümleri, burada özetlenen güvenlik açıklarını detaylandırarak, tespit edilen her bir bulgunun;

- Bulgu Referans Numarasını,
- Bulgu Adını,
- Önem Derecesini,
- Etkisini,
- Kullanıcı Profilini,
- Bulgunun Tespit Edildiği Bileşen/Bileşenler
- Durumu,
- Bulgu Açıklaması,
- Çözüm önerilerini içermektedir.

Hedefe odaklanmış, yeterince donanımlı, kaynağa ve zamana sahip saldırganların, bu raporda belirtilen güvenlik daha fazlasını bulup, kötüye kullanması azımsanamayacak bir olasılıktır. Bu nedenle, raporlanan açıkların oluşturduğu risklerin ivedilikle değerlendirip, risk eylem planının oluşturulması önemlidir.

4. TEKNİK DETAYLAR

Güven Damgası Testlerinde, yapılan kontroller sonucunda 147 madde içerisinde 8 maddeyi karşılamadığı tespit edilmiştir. Gereksinimleri karşılamayan maddeler;

- Girdi doğrulama rutinlerinin sunucu tarafında uygulandığını doğrulayın.
- Uygulamanın saldırgana yardımcı olabilecek şekilde oturum anahtarı, yazılım/çerçeve versiyonu ve kişisel bilgileri sızdıran hata mesajları veya yığın dökümü oluşturmadığını doğrulayın.
- İçeriğin 3. taraf X-Frame içerisinde görüntülenmemesi gereken siteler için Content Security Policy V2 (CSP) kullanıldığını doğrulayın.
- URL yönlendirmenin yalnızca beyaz listedeki hedeflere izin verdiğini veya potansiyel olarak güvenilmeyen içeriklere yönlendirilirken uyarı gösterildiğini doğrulayın.
- Yönetimsel ara yüzlerin güvensiz taraflarca erişilemediğini doğrulayın.
- Kullanıcı oturumu kapattığında oturumun geçersiz hale getirildiğini doğrulayın.
- Oturum anahtarı değerini tutan çerez yolunun uygulamaya kısıtlı olacak şekilde ayarlandığı ve kimlik doğrulama oturum anahtarlarına ait "HttpOnly" ve "secure" niteliklerinin ayarlandığını doğrulayın.
- Content Security Policy V2'nin (CSP) satır içi Javascript kullanımını devre dışı bıraktığı veya satır içi Javacript'I CSP nonce veya özetleme ile bütünlük kontrolü sağladığını doğrulayın.

Bu gereksinimleri karşılamayan maddelerin risk seviyelerinin düşük olması nedeniyle Güven Damgası başvurusuna engel olmadığı değerlendirilmiştir. Bahse konu https://guvendamgasi.ticimaxtest.com web sitesinin güvenliği için karşılanmayan 8 maddedeki hususların giderilmesi ve gerek duyulursa söz konusu hususların giderildiğinin doğrulanması tavsiye edilmektedir.