

#FIRMA

Güvenlik Test Raporu

**-GİZLİ-**

**Doküman Detayları**

|  |  |
| --- | --- |
| Hazırlayan |  |
| Onaylayan |  |
| Müşteri Yetkilisi |  |
| Sürüm |  |
| İlk Yayın Tarihi |  |

#FIRMA yetkilisinin dikkatine,

Kurumunuz sistemlerindeki güvenlik zafiyetlerinin tespit edilmesi amacı ile gerçekleştirilen Güvenlik Testleri #START# - #END# tarihleri arasında gerçekleştirilmiştir. Bu rapor, testler sırasında tespit edilen zafiyetlerin detaylarını ve çözüm önerilerini içermektedir.

Çalışmalar sırasında ekibimize sağladığınız kolaylık ve göstermiş olduğunuz anlayış için teşekkür ederiz.

**Yasal Sorumluluklar**

İşbu rapor #FIRMA sistemlerine yönelik yapılan güvenlik denetimleri ve sızma testleri sonuçlarını içermektedir. Rapor içeriği gizli olup her iki tarafın yazılı mutabakatı olmadan üçüncü taraflara sözlü, yazılı ya da elektronik ortamda paylaşılamaz.

Rapor, tarama süresi içinde varlığı bilinen ve tarafımızca tespit edilen güvenlik açıklarını içermektedir. Tarama işlemi bittikten sonra rapor teslim edilene kadar geçen süre içerisinde çıkabilecek yeni güvenlik açıklarına dair eksikliklerden dolayı Test Ekibi sorumlu tutulamaz.

İnternet üzerinden gerçekleştirilen testler sırasında oluşturulan trafiğin üçüncü taraf gerçek kişiler ya da tüzel kişiler (ISP) tarafından kaydedilme ihtimali bulunmaktadır. Trafiğin üçüncü kişiler tarafından dinlenilmesi veya gözlenmesi sonucunda ortaya çıkabilecek kayıplardan Test Ekibi sorumlu tutulamaz.

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

Güvenlik Testleri önceden belirlenen bir kapsam çerçevesinde kısıtlı bir zaman dilimi içerisinde yapılmaktadır. Daha fazla kaynağa ve zamana sahip saldırganlar, test ekibinin tespit ettiğinden daha fazla zafiyeti tespit edip kötüye kullanabilir. Testler sırasında tespit edilemeyen veya test sonrası ortaya çıkan güvenlik açıklarından Test Ekibi sorumlu tutulamaz.

İçindekiler Tablosu

[**1.** **Yönetici Özeti** 6](#_Toc30491753)

[**1.1** **Bulgu Dağılımı** 7](#_Toc30491754)

[**1.2** **Bulgu Özeti** 7](#_Toc30491755)

[**1.3** **Kapsam** 8](#_Toc30491756)

[**1.4** **Test Ekibi** 8](#_Toc30491757)

[**1.5** **Risk Derecelendirme** 9](#_Toc30491758)

[**1.6** **Testler Sırasında Kullanılan Kullanıcı Profilleri** 9](#_Toc30491759)

[**2.** **Güvenlik Test Bulguları** 10](#_Toc30491760)

[**2.1** **#HIZMET-TURU#** 10](#_Toc30491761)

[**2.2** **Testler Sırasında Kullanılan Araçlar** 11](#_Toc30491762)

# **Yönetici Özeti**

# BU KISIM TESTE ÖZEL ELLE DOLDURULACAK

## **Bulgu Dağılımı**

#BULGU\_PIE\_CHART

## **Bulgu Özeti**

|  |  |
| --- | --- |
| Bulgu Adı | Önem Derecesi |

|  |  |
| --- | --- |
|  |  |

## **Kapsam**

Güvenlik Testleri sırasında kurum tarafından belirlenen aşağıdaki sistemlere karşı sızma testleri, yapılandırma denetimleri ve zafiyet taramaları gerçekleştirilmiştir.

|  |  |
| --- | --- |
|  |  |

## **Test Ekibi**

|  |  |
| --- | --- |
|  |  |

## **Risk Derecelendirme**

|  |  |  |
| --- | --- | --- |
| ACİL |  | Acil öneme sahip açıklıklar, niteliksiz saldırganlar tarafından uzaktan gerçekleştirilen ve sistemin tamamen ele geçirilmesi veya kullanıcı mahremiyetinin ihlali ile sonuçlanan saldırılara sebep olan açıklıklardır. |
| KRİTİK |  | Kritik öneme sahip açıklıklar, nitelikli saldırganlar tarafından uzaktan gerçekleştirilen ve sistemin tamamen ele geçirilmesi veya kullanıcı mahremiyetinin ihlali ile sonuçlanan saldırılara sebep olan açıklıklardır. |
| YÜKSEK |  | Yüksek öneme sahip açıklıklar, uzaktan gerçekleştirilen ve kısıtlı hak yükseltilmesi veya hizmet dışı kalma ile sonuçlanan, ayrıca yerel ağdan ya da sunucu üzerinden gerçekleştirilen ve hak yükseltmeyi sağlayan saldırılara sebep olan açıklıkları içermektedir. |
| ORTA |  | Orta öneme sahip açıklıklar, yerel ağdan veya sunucu üzerinden gerçekleştirilen ve hizmet dışı bırakılma ile sonuçlanan ataklara sebep olan açıklıkları içermektedir. |
| DÜŞÜK |  | Düşük öneme sahip açıklıklar ise etkilerinin tam olarak belirlenemediği ve literatürdeki en iyi sıkılaştırma yöntemlerinin izlenmemesinden kaynaklanan eksikliklerdir. |

## **Testler Sırasında Kullanılan Kullanıcı Profilleri**

|  |  |
| --- | --- |
| **Profil** | **Açıklama** |
| Anonim | İnternet üzerinden, kuruma ait sistemlere erişebilen ancak kurum tarafından tanımlanmış herhangi bir kullanıcı hesabı olmayan ya da internet üzerinden herkesin yaratabileceği bir kullanıcı hesabına sahip kullanıcıyı temsil eder. |
| Yerel | Kurum çalışanlarını ve kurum tarafından sistemlere erişmek üzere yetkilendirilmiş kullanıcıları temsil eder. |
| Yetkili | Mevcut sistem üzerinde yönetici hakları bulunan kullanıcıyı temsil eder. |

# **Güvenlik Test Bulguları**

## **#HIZMET-TURU#**

Kurumun test kapsamındaki sistemlerine internet üzerinden gerçekleştirilen saldırı ve sızma testlerinin bulguları bu bölümde listelenmiştir. Testler sırasında #21KUTU yöntemi kullanılmıştır. Gerçekleştirilen denetimlerin detayları Test Metodolojisi başlığı altında bulunabilir.

|  |  |  |
| --- | --- | --- |
|  | |  |
| **Etkisi** |  | |
| **Erişim Noktası** |  | |
| **Kullanıcı Profili** |  | |
| **Bulgu Tanımı** |  | |
|  | | |
| **Çözüm Önerisi** |  | |
| **Ek Bilgiler** |  | |
|  |  | |

##

## **Testler Sırasında Kullanılan Araçlar**

|  |  |
| --- | --- |
| Burp Suite | [Ağ](https://portswigger.net/burp) trafiğini yakalayıp, trafikte değişiklik yapmak için kullanılmıştır. |
| Wireshark | [Ağ](https://www.wireshark.org) trafiğini kaydetmek ve analiz etmek için kullanılmıştır. |
| Sqlmap | Muhtemel [SQL](http://sqlmap.org/) Injection zafiyetlerini tespiti için kullanılmıştır. |
| Apktool | [Apk](https://ibotpeaches.github.io/Apktool/) dosyalarını ‘decomoile’ etmek için kullanılmıştır. |
| Nessus | [Ağ](https://www.tenable.com/products/nessus/nessus-professional)da zafiyet taraması yapmak için kullanılmıştır. |
| Web Inspect | [Web](https://www.microfocus.com/en-us/products/webinspect-dynamic-aznalysis-dast/overview) uygulamalarının zafiyet taraması için kullanılmıştır. |
| Fortify | [Kaynak](https://www.microfocus.com/en-us/products/static-code-analysis-sast/overview) kod analizi için kullanılmıştır. |