Privia SECURITY

Mobil Uygulama Sızma Testi Hizmeti

Profesyonel Offensive Security Hizmetleri

"Mobil Tehditlere Karşı Güçlü Savunma!"

Küçükbakkalköy Mah. Kocasinan Cad.
Privia Plaza No:42 Ataşehir, İstanbul

+90 (216) 514 72 14

www.priviasecurity.com

“Mobil uygulamanızdaki potansiyel zafiyetleri belirleyip olası riskleri en aza indirgiyoruz.”

Mobil uygulamalar, günümüzde bireylerin ve işletmelerin en önemli iletişim ve iş yapma araçları haline gelmiştir. Bu durum, mobil uygulamalara yönelik siber saldırıların artmasına ve uygulamaların güvenliğinin her zamankinden daha kritik hale gelmesine neden olmuştur. Privia Security olarak, mobil uygulamalarınızın güvenlik açıklarını tespit etmek ve bu açıkları gidermek için kapsamlı bir sızma testi hizmeti sunuyoruz.

Sızma testlerimiz, OWASP Mobil Güvenlik Test Kılavuzu (MSTG) ve OWASP Mobil Uygulama Doğrulama Standardı (MASVS) metodolojilerine göre gerçekleştirilir. Bu testlerde uygulama analizi, kullanıcı girişi ve kimlik doğrulama, veri güvenliği, iletişim güvenliği ve genel uygulama güvenliği gibi başlıkları ele alarak mobil uygulamanızın zafiyetlerini tespit ediyoruz. Farklı mobil platformlarda (iOS, Android) kullanılan çeşitli geliştirme dillerine ve frameworklere bağımsız olarak gerçekleştirilen bu kapsamlı testler, mobil uygulamanızın güvenlik standartlarına uygunluğunu değerlendirir ve geliştiricilere güvenlik iyileştirmeleri için öneriler sunar.

Mobil Uygulama Sızma Testleri sonucunda tespit edilen tüm güvenlik zafiyetleri detaylı bir rapor halinde sunulur. Bu raporda zafiyetlerin önemi, olası etkileri ve kapatılması için gerekli çözüm önerileri yer almaktadır. Mobil uygulamalarınızın güvenliğini sağlamak ve kullanıcılarınızın verilerini korumak için Privia Security'nin sızma test hizmetlerinden yararlanın.

Hizmete Ait Bileşenler

Uygulama Analizi

Mobil uygulamanın yapısı, bileşenleri ve işlevselliğinin incelenmesini içerir. Bu süreçte, uygulamanın potansiyel güvenlik zafiyetlerine işaret eden durumlar tespit edilerek riskler belirlenir. Analiz sonucunda elde edilen bulgular, uygulamanın güvenlik seviyesini daha sağlam hale getirmek için kullanılacak iyileştirmelerin temelini oluşturur.

Kimlik Doğrulama ve Veri Güvenliği

Kullanıcı girişi ve kimlik doğrulama mekanizmaları, uygulamanın güvenliğinin en kritik bileşenlerinden biridir. Bu bileşenlerin güvenliğini sağlamak için kapsamlı testler yapılarak olası zafiyetler değerlendirilir. Ayrıca, uygulamanın veri güvenliği, özellikle hassas verilerin korunması açısından incelenir. Yapılan çalışmayla, veri bütünlüğünün sağlanması ve veri kaybı risklerinin minimize edilmesi hedeflenir.

İletişim Güvenliği ve Platform Uyumluluğu

Uygulamanın iletişim güvenliği, dış dünya ile bağlantılarında veri bütünlüğünün korunması için önemli bir aşamadır. Bu bileşen kapsamında ağ trafiği ve veri şifreleme süreçleri detaylı bir şekilde değerlendirilir. Ayrıca, mobil uygulama sızma testleri, iOS, Android gibi farklı mobil platformlarda ve çeşitli geliştirme dillerine (Swift, Kotlin, React Native, Xamarin gibi) uygun olarak gerçekleştirilir.

Uygulama Zafiyetleri ve Raporlama

Uygulama içindeki potansiyel zafiyetlerin tespit edilmesi ve bu zafiyetlerin giderilmesi sürecinde yapılan testler, uygulamanın genel güvenlik seviyesini artırmaya yöneliktir. Sızma testi sonucunda, uygulamada tespit edilen tüm güvenlik zafiyetleri rapor halinde sunulur. Bu raporda zafiyetlerin önem derecesi, olası etkileri ve kapatılması için öneriler yer almaktadır. Geliştiricilere yönelik bu öneriler, uygulamanın daha güvenli hale getirilmesi için rehberlik eder.

Kriptografi ve Veri Şifreleme

Mobil uygulamalarda kullanılan kriptografik algoritmalar ve veri şifreleme yöntemleri, hassas bilgilerin güvenliğini sağlamak için büyük önem taşır. Bu bileşen kapsamında, kullanılan şifreleme protokollerinin ve anahtar yönetim süreçlerinin güvenliği detaylı bir şekilde değerlendirilir. Şifreleme yöntemlerinin doğru ve güvenilir bir şekilde uygulandığından emin olunarak, veri gizliliği ve bütünlüğü garanti altına alınır.

Sık Sorulan Sorular

Mobil uygulama sızma testi nedir ve neden önemlidir?

Mobil uygulama sızma testi, mobil uygulamalardaki güvenlik zafiyetlerini belirlemek ve tespit edilen zafiyetleri gidermek amacıyla yapılan güvenlik testidir. Günümüzde mobil uygulamalar, kullanıcı verilerini barındırmakta ve finansal işlemleri yönetmekte olduğundan, bu uygulamaların güvenliği kritik öneme sahiptir. Mobil Uygulama Sızma testleri güvenlik zafiyetlerini erkenden tespit ederek saldırganların potansiyel tehditlerine karşı koruma sağlar.

Mobil uygulama sızma testi ne zaman yapılmalıdır?

Mobil uygulama sızma testleri, uygulama geliştirme döngüsünün farklı aşamalarında yapılmalıdır. Testler, uygulama ilk geliştirilirken, önemli güncellemeler öncesinde veya sonrasında, üçüncü taraf bileşenlerin entegre edilmesinden sonra ve herhangi bir uyumluluk denetimi için yapılması gerekebilir. Yayına çıkacak olan yeni uygulamaların Güvenlik denetimleri yayına çıkmadan önceki son test aşamasında gerçekleştirilir. Bu süreçler boyunca düzenli olarak test yapmak, olası güvenlik açıklarının anında tespit edilerek uygulamanın güvenlik seviyesini yüksek tutmaya yardımcı olur.

Mobil uygulama sızma testi nasıl yapılır?

Mobil uygulama sızma testi, manuel ve otomatik araçların kombinasyonu kullanılarak gerçekleştirilir. İlk olarak, uygulama analizi ve risk değerlendirmesi yapılır. Ardından, OWASP Mobil Güvenlik Test Kılavuzu (MSTG) ve OWASP Mobil Uygulama Doğrulama Standardı (MASVS) gibi uluslararası metodolojilere uygun şekilde veri güvenliği, kimlik doğrulama, yetkilendirme ve iletişim protokolleri değerlendirilir. Mobil uygulama sızma testleri sırasında, uygulamanın yapısı ve işlevleri detaylı şekilde analiz edilir ve çeşitli sızma teknikleriyle olası güvenlik zafiyetleri ortaya çıkarılır.

Mobil sızma testi sonuçlarında neler yer alır?

Mobil uygulama sızma testi sonucunda, uygulamada tespit edilen güvenlik zafiyetlerini ve bu zafiyetlerin olası etkilerini detaylı şekilde açıklayan bir rapor sunulur. Sunulan raporda yönetici özeti, zafiyetlerin giderilmesi için gerekli teknik adımlar, öneriler ve çözüm yöntemleriyle birlikte yer alır. Raporda yer alan tespitler sayesinde geliştiricilere, uygulamanın güvenlik seviyesini artıracak öneriler sunar.

Mobil sızma testi hangi tür zafiyetleri tespit eder?

Mobil uygulama sızma testi, çeşitli güvenlik zafiyetlerini tespit etmeyi hedefler. Bu zafiyetler arasında kimlik doğrulama ve yetkilendirme zafiyetleri, zayıf şifreleme algoritmaları, veri güvenliği eksiklikleri, güvenli olmayan ağ iletişimi, hatalı yapılandırma ve cihazdaki hassas bilgilerin uygunsuz şekilde depolanması gibi kritik güvenlik sorunları yer test edilir. Ayrıca, gelişmiş tehdit aktörleri tarafından sömürülebilecek zafiyetler de belirlenerek uygulamanın güvenlik seviyesi artırılır.

Mobil uygulama sızma testi ne kadar sürer ve hangi faktörler bu süresiyi etkiler?

Mobil ugyulama sızma testinin süresi, uygulamanın karmaşıklığına, kullanılan teknolojilere, uygulamanın boyutuna ve kapsamına bağlı olarak değişiklik gösterir. Küçük ölçekli bir mobil uygulama genellikle 1 hafta içinde test edilebilirken, daha karmaşık veya büyük bir uygulama için bu süre 2-5 hafta arasında değişebilir. Uygulamanın test edilmesi gereken platform sayısı (iOS, Android), üçüncü taraf entegrasyonlar ve veri şifreleme yöntemleri gibi faktörler test süresini etkilemektedir.

Siber Güvenlikte Doğru Çözüm Ortağınız

2018 yılında siber güvenliğin geleceği için yola çıkan Privia Security, kuruluşundan bu yana, müşterilerine yüksek kaliteli hizmet sunmayı amaçlamaktadır. Güçlü ve yetenekli ekibimiz, siber güvenliğin her alanında hizmet verdiğimiz organizasyonlara en güvenilir ve kapsamlı çözümleri sunarak, organizasyonların dijital dünyadaki güvenlik ihtiyaçlarını karşılamaktadır.

Günümüzde hızla gelişen ve karmaşık hale gelen siber tehditlerle mücadele etmek giderek zorlaşıyor. Bu noktada Privia Security olarak, müşterilerimize ihtiyaç duydukları hem defansif hem de ofansif siber güvenlik stratejilerini en ileri teknolojiyle sunuyoruz. İnovatif AR-GE ürünlerimiz ve stratejik danışmanlığımız sayesinde organizasyonların siber güvenlik olgunluğunu artırmayı ve onlara proaktif çözümler sunmayı hedefliyoruz. Şu anda 300'den fazla büyük kuruluşun güvenliğini sağlamaktan gurur duyuyoruz.

Uluslararası ve Yerel Siber Güvenlik Çözümleri

Privia Security olarak, Avrupa, Asya, Ortadoğu ve Amerika dahil olmak üzere geniş bir coğrafyaya siber güvenlik hizmetleri sunmaktayız. Offensive, Defensive ve Forensic alanlarında uzmanlaşmış ekiplerimiz, kritik altyapılar, aviyonik sistemler, kurumsal ağlar ve askeri alanlar gibi farklı sektörlerde faaliyet gösteren organizasyonlara özel çözümler geliştirmektedir.

Ayrıca savunma kapasitelerini güçlendirmek isteyen ülkelere yönelik geliştirdiğimiz PriviaHub siber savaş simülasyonu ile siber savaş stratejilerinin test edilmesi, tatbikatların yürütülmesi ve uzmanların niteliklerinin ölçülmesi için kapsamlı çözümler sunuyoruz. Bu inovatif platform özel sektör, akademi ve askeri alanlarda tatbikat ihtiyaçlarını karşılamak üzere tasarlanmıştır.

İleri Teknoloji ile Güvenli Gelecek

İstanbul, Ankara, Londra ve Cumhuriyet Teknopark'taki Ar-Ge merkezimizde, müşterilerimize değer katan projeler geliştiriyoruz. Penetrasyon testleri, Red Team operasyonları, siber güvenlik eğitimleri ve kurumlara özel siber güvenlik çözümlerimizle sektörde fark yaratmaya devam ediyoruz. "Privacy For You" sloganımızla, güvenlik ve gizliliğe yenilikçi bir bakış açısı getiriyor ve müşterilerimizin dijital geleceğini güvence altına alıyoruz.

Privia
SECURITY