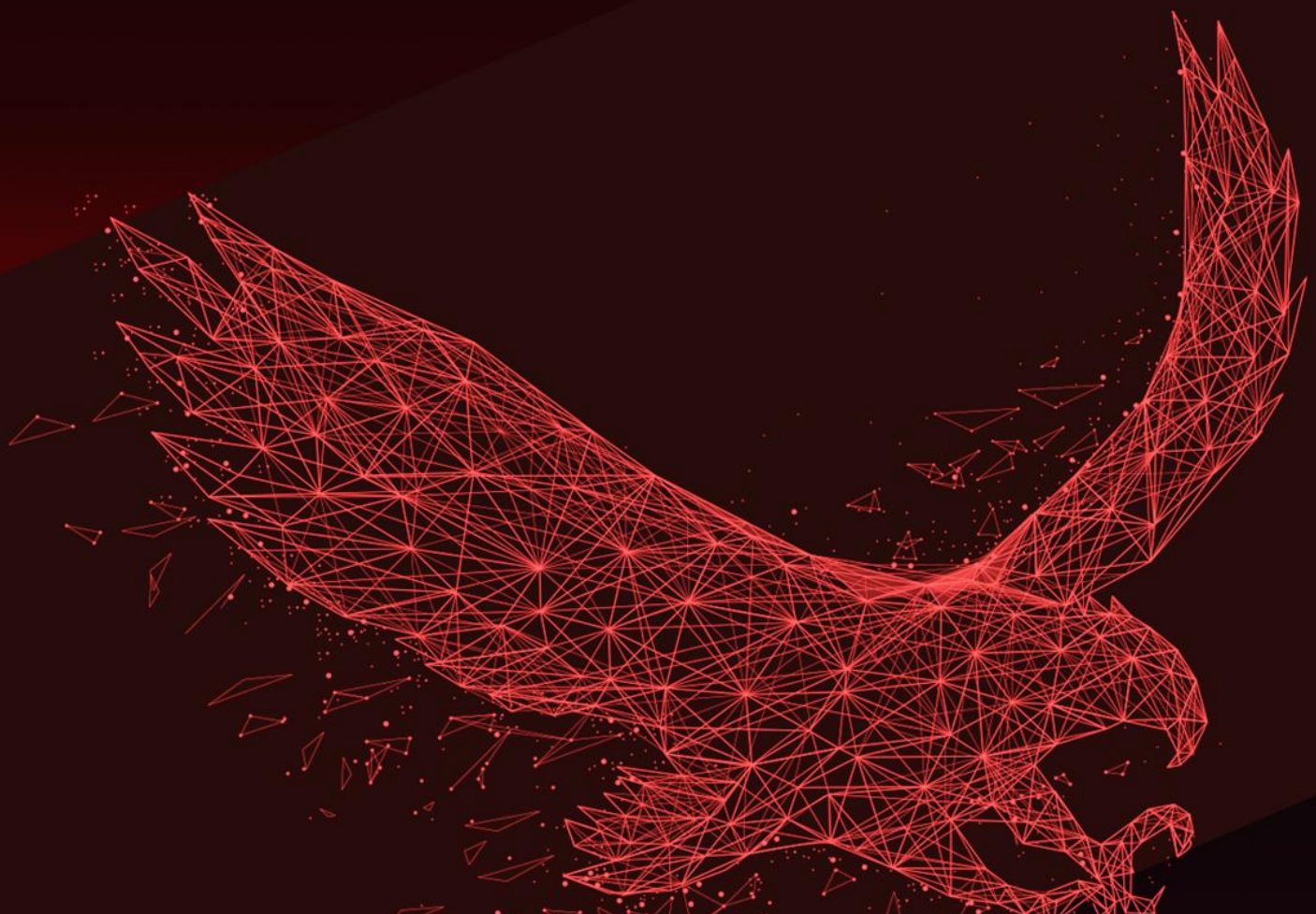
Privia SECURITY



Web Uygulama Güvenliği Sızma Testi Hizmeti

Profesyonel Offensive Security Hizmetleri

"Uygulama Güvenliğinizi Bir Adım Öne Taşıyın!"

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

+90 (216) 514 72 14

www.priviasecurity.com

"Web uygulamalarında potansiyel güvenlik açıklarını tespit ederek, dijital dünyada güvenli bir deneyim sunuyoruz. Privia Security'nin uzman ekibi ile uygulamalarınızı siber tehditlere karşı daha güvenli bir hale getirin."

Sosyal mühendislik hizmetimiz, çalışanlarınızı hedef alan tehditleri simüle ederek, organizasyonunuzun zayıf noktalarını ortaya çıkarmayı amaçlar. Sosyal Mühendislik hizmeti, insan faktörünün siber güvenlikteki rolünü vurgulamak için kritik bir öneme sahiptir. Gerçekçi senaryolar aracılığıyla, çalışanlarınızın bilgi güvenliği farkındalığını arttırır.

Simülasyonlar, oltalama e-postaları, telefon dolandırıcılığı ve diğer sosyal mühendislik tekniklerini içerecek şekilde tasarlanır. Çalışanlar, bu tür saldırılara karşı nasıl bir tepki vereceklerini deneyimleyerek, bu tehditlere karşı daha hazırlıklı hale gelir. Elde edilen veriler, zayıf noktaların belirlenmesi ve güvenlik eğitimlerinin geliştirilmesi için kullanılır.

Sosyal mühendislik hizmetimiz, sadece zayıflıkları tespit etmekle kalmaz, aynı zamanda organizasyon içinde güvenlik bilincini artırmayı hedefler. Çalışanlar, simülasyonlar sayesinde saldırganların yöntemlerini öğrenir ve bu bilgilerle kişisel güvenliklerini sağlama konusunda daha donanımlı hale gelir. Böylece, organizasyonunuzun siber güvenlik durumu önemli ölçüde güçlendirilmiş olur.

Hizmete Ait Bileşenler

Uygulama Analizi

Web uygulamalarının mimarisi, bileşenleri ve işlevselliği detaylı bir şekilde analiz edilir. Bu süreçte, güvenlik zafiyetlerine yol açabilecek potansiyel riskler belirlenir ve iyileştirme yapılabilecek alanlar tespit edilerek raporlanır.

Kimlik Doğrulama ve Yetkilendirme

Kullanıcı kimlik doğrulama ve yetkilendirme süreçleri değerlendirilerek güvenlik zafiyetleri ortaya çıkarılır. Kullanıcı bilgilerinin korunması sağlanır ve yetkisiz erişimlerin önüne geçmek için güvenlik mekanizmaları güçlendirilir.

Veri Güvenliği

Hassas verilerin güvenliğini sağlamak için uygulamadaki veri işleme ve saklama yöntemleri incelenir. Veri şifreleme ve koruma yöntemleri test edilerek, kullanıcı ve sistem verilerinin gizliliği güvence altına alınır.

İletişim Güvenliği

Uygulamaların dış dünya ile iletişim kurduğu tüm kanallar test edilerek veri trafiğinin güvenliği sağlanır. Ağ iletişiminde veri bütünlüğünü korumak ve yetkisiz erişimleri engellemek amacıyla şifreleme protokolleri test edilir.

Zafiyet Tespiti ve Raporlama

Web uygulamalarında tespit edilen güvenlik zafiyetleri önem derecesine göre sınıflandırılır ve detaylı bir rapor halinde sunulur. Hazırlanan raporda her bir zafiyetin etkileri, giderilme yöntemleri ve çözüm önerileri yer alır. Rapor ayrıca siber güvenlik seviyesinin artırılması için rehberlik sunar.

Güvenlik Standartlarına Uyum Değerlendirmesi

Uygulamaların PCI DSS, GDPR, ISO 27001, BDDK, EPDK, SPK ve SGT gibi düzenleyici ve sektörel güvenlik standartlarına uyum sağlaması desteklenir. Düzenlemelere uygunluk sağlamak adına gerekli güvenlik önlemleri belirlenir ve öneriler sunularak regülasyonlara tam uyumlu bir yapı oluşturulması desteklenir.

Sık Sorulan Sorular

Web Uygulama Güvenlik Testi Nedir?

Web uygulama güvenlik testi, bir uygulamanın siber saldırılara karşı dayanıklılığını değerlendirmek için yapılan testler bütünüdür. Gerçekleştirilen testlerle, SQL injection, XSS ve kimlik doğrulama açıkları gibi zafiyetler tespit edilir. Testler manuel ve otomatik araçlarla gerçekleştirilir. Amaç, uygulama zafiyetleri belirleyip riskleri minimize etmek ve uygulamanın güvenli hale gelmesini sağlamaktır.

OWASP Top 10 Nedir ve Neden Önemlidir?

OWASP Top 10, web uygulamalarında yaygın görülen en kritik güvenlik risklerini listeler. SQL injection, kimlik doğrulama eksiklikleri ve XSS gibi tehditler bu listede yer alır. OWASP, geliştiricilere ve güvenlik ekiplerine rehberlik ederek yaygın hataların önlenmesini sağlar. OWASP listesi, uygulama güvenliği için temel referans noktası olarak kabul edilir.

SQL Injection Nedir ve Nasıl Önlenir?

SQL injection, saldırı amaçlı SQL komutları kullanarak veritabanına izinsiz erişim sağlanmasına verilen yöntemin adıdır. SQL Injection, parametreli sorgular ve veri doğrulama yöntemleriyle önlenebilir. Dinamik SQL komutlarından kaçınmak güvenliği artırır. Güçlü giriş doğrulama politikaları uygulanarak saldırı riski azaltılır.

XSS (Cross-Site Scripting) Nedir ve Nasıl Önlenir?

XSS, kullanıcıların tarayıcılarında kötü niyetli kodların çalıştırılmasını sağlayan bir saldırı tekniğidir. Giriş doğrulama, içerik güvenliği politikası (CSP) ve çıktı kodlaması bu saldırıları önlemek için kullanılmaktadır. Üç tür XSS saldırısı vardır: Reflected, Stored ve DOM Based XSS. Her biri, farklı koruma yöntemleri gerektirir ve düzenli testlerle kontrol edilmelidir. Ayrıca Web Application Firewall (WAF)'lar, bu saldırıların tespiti ve önlenmesinde aktif olarak kullanılır.

Penetrasyon Testi ve Zafiyet Taraması Arasındaki Fark Nedir?

Zafiyet taraması, otomatik araçlar kullanarak bilinen zafiyetlerin taranması yöntemidir. Penetrasyon testi ise, gerçek saldırı senaryolarını simüle ederek zafiyetlerin etkisini değerlendirir. Penetrasyon testleri, içerisinde Zafiyet testlerini barındırmaktadır. Zafiyet taramaları hızlıdır ancak sınırlı tespit yapar ve zafiyetin false/positive olasılığı daha yüksektir. Penetrasyon testleri daha detaylıdır ancak daha fazla zaman ve uzmanlık gerektirmekle birlikte false/positive bulgu olasılığı daha azdır.

CSRF (Cross-Site Request Forgery) Saldırıları Nasıl Önlenir?

CSRF, kullanıcının haberi olmadan işlemler gerçekleştirilmesine yol açan bir saldırı türüdür. Anti-CSRF token kullanımı ve referer başlık doğrulaması ile önlenebilir. Özellikle bankacılık uygulamaları gibi kritik alanlarda sıkı önlemler gerektirir. Kullanıcı işlemleri için ek doğrulama yöntemleri kullanılması da önerilir.

Oturum Yönetimi Neden Kritik Öneme Sahiptir?

Oturum yönetimi, Session Fixation ve Session Hijacking gibi saldırılara karşı korunmayı sağlar. Güvenli oturumlar için kısa oturum süreleri ve şifreli oturum kimlikleri kullanılır. Çerezler yalnızca güvenli bağlantılarda iletilir. Oturumlar kullanıcının herhangi bir eylemde bulunmadığı zaman periyotlarında otomatik olarak sonlandırılmalıdır.

Güvenlik Testlerinden Sonra Hangi Aksiyonlar Alınmalıdır?

Testlerden sonra, tespit edilen zafiyetlerin önceliklendirilip hızla kapatılması gereklidir. Geliştiricilere ayrıntılı raporlar sunularak iyileştirme süreci hızlandırılır. Zafiyetlerin giderilmesi için planlanan çözümler uygulanır. Aynı zamanda yeni tehditlere karşı periyodik testler yapılması önerilir.

Web Uygulama Güvenliğini Sağlamak İçin Hangi Adımlar Atılmalıdır?

Web uygulama güvenliğini sağlamak için ilk adım, güvenli kodlama standartlarını benimsemek ve geliştiricilere OWASP yönergelerine uygun olarak kod yazmalarını öğretmektir. Çok faktörlü kimlik doğrulama (MFA) ve şifreli oturum yönetimi, kimlik avı gibi tehditlere karşı etkili koruma sağlar. Düzenli olarak zafiyet taramaları ve penetrasyon testleri yaparak uygulamanın güvenlik durumu gözlem altında tutulur. Aynı zamanda sistem bileşenlerinin güncel tutulması ve kullanıcı farkındalık eğitimlerinin verilmesi, yeni tehditlere karşı hazırlıklı olmayı sağlar.

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