

GamaAPP Uygulama güvenlik denetimi, **GamaSEC**'nin ileri seviye web uygulaması denetim metodolojisini kullanır ve web uygulamanız en güncel tekniklerle değerlendirilir. **GamaSEC** danışmanları öncelikle web uygulamanızın fonksiyonallığı ve risk profilini çıkarır. Bu temelden yola çıkan değerlendirme, uygulamanızın güvenlik açıklarının tespiti için tam kapsamlı bir çalışmadır.

Kazanımlarınız

➤ Olacakları bilmek: Sisteminize internet üzerinden gelecek gerçek bir saldırı durumunda başınıza gelecek kayıpları zarar görmeden tecrübe etmek

➤ Mevcudu onaylamak: Mevcut güvenlik mekanizmalarınızı, saldırı tespit ve cevap sistemlerinizi deneyimli **GamaSEC** güvenlik uzmanlarına karşı sınavdan geçirmek ve güvenilirliğini onaylamak

➤ Düşmanı tanımak: Sisteminizin dışarıdan nasıl görüldüğünü ve düşmanın neler yapabileceğini görmek, gerçekte yaşayacağınız zararı yaşamadan düşmanınızı tanımak

➤ Farkındalık: Organizasyonun tüm seviyelerinde farkındalık yaratarak şirket güvenlik politikasının gelişimine katkı sağlamak

GamaAPP - Denetim Metodolojisi

- Uygulama Haritasının Oluşturulması
- Yapılandırma Açıkları Taraması
- Uygulama Platformu Açıklarının Taraması
- Otomatize Araçlar ile Güvenlik Açığı Taraması
- Uygulama Harici Modüllerinin Analiz Edilmesi
- Yayınlanmamış Güvenlik Açığı Taraması
- Güvenlik Açıkları Kullanılarak Yetki Kazanılması
- Saptanan Güvenlik Açıklarının Değerlendirilmesi
- Çözüm Geliştirme ve Rapor Hazırlığı

Yapılandırma Açıkları Taraması ve Haritalama

Yapılandırma Açıkları Taraması, lojik bir yapı çerçevesinde uygulama sunucusuna yapılan HTTP isteklerinin ve bu isteklere gelen cevapların yorumlanmasından oluşmaktadır. Manuel taramada öncelikli olarak uygulama yapısı analiz edilerek, sunucunun üzerinde bulunduğu yapı ortaya çıkarılır.

- Uygulama Haritalama
- Dizin Listeleme
- Gizli Web Dizinleri
- Yedek Dizin Kontrolleri

Otomatize Araçlar ile Güvenlik Açığı Taraması

Otomatize güvenlik açığı tarama yazılımları, web uygulamalarında bulunan yayınlanmış güvenlik açıkları ve bilinen saldırı yöntemlerini kullanarak güvenlik açığı taramakta ve raporlamaktadır. Çeşitli programlama dilleri ile çalışabilmeleri, yayınlanmış güvenlik açıklarını takip edebilmeleri, farklı web teknolojilerine verdikleri destek ve destekledikleri doğrulama yöntemleri doğrultusunda verimli olarak güvenlik açıklarını saptamaktadırlar.

Özelliklerinin yetersiz olduğu durumlar ve birçok web uygulamasının standart dışı olması nedeniyle sağladıkları verim kısıtlıdır.

Çıkarılan yapı üzerine, aşağıda belirtilen uygulama zaafiyetleri çerçevesinde sayısız test, manuel olarak bütün parametrelere uygulanır.

- Doğrulanmamış Girdi Kabul Edilmesi
- Çapraz Site Komut Çalıştırması
- Bellek Taşması
- Hatalı Giriş Kontrolü
- Hatalı Doğrulama ve Oturum Yönetimi
- Enjeksiyon Kusurları
- Uygunsuz Hata İşleme
- Güvensiz Saklama
- Güvensiz Yönetim Arabirimi

GamaSEC Denetim Hizmetleri

- GamaNET İnternet Güvenlik Denetimi
- GamaAPP Web Uygulama Güvenlik Denetimi
- GamaLAN Yerel Ağ Güvenlik Denetimi
- GamaAUDIT Bilişim Sistemleri Denetimi
- GamaWIRELESS Kablosuz Ağ Güvenlik Denetimi
- GamaSCAN Otomatize Güvenlik Denetimi
- GamaVPN Sanal Özel Ağ Güvenlik Denetimi
- GamaDMZ DMZ Ağı Güvenlik Denetimi

GamaSEC Danışmanlık Hizmetleri

- GamaPOLICY Güvenlik Politikası Danışmanlığı
- GamaCON Bilgi Güvenliği Danışmanlığı

GamaSEC Tecrübesi

➤ **GamaSEC** danışmanları, kurumsal güvenlik ihtiyacınızın belirlenmesi, bilgi güvenliği yatırımınızın verimliliğinin ölçülmesi, bilgi varlıklarınıza yönelik güvenlik tehditlerinin belirlenmesi, kurumsal risk analizinizin yapılması hizmetlerini sunabilmek amacıyla en yeni teknolojileri, kendi geliştirmiş oldukları yöntemleri ve araçları kullanmaktadır.

➤ **GamaSEC** danışmanları, güvenlik denetimi ağa/sunucuya sızma sürecinde kullanmak üzere **GamaSEC** Exploit Framework yazılımını geliştirmiş, kendi geliştirmiş olduğu teknik ve araçları yazılıma entegre etmiştir. GamaSEC Exploit Framework yazılımı ile çok sayıda yayınlanmış veya ekipçe geliştirilmiş exploit merkezi yapıya sokulmuş, ağa/sunucuya sızma süreci daha verimli hale getirilmiştir.

➤ **GamaSEC** danışmanlarıncı geliştirilen bir diğer ortam olan **GamaSEC** Audit Framework ile de ticari yazılımlar, açık kaynaklı yazılımlar ve **GamaSEC** Exploit Framework arası entegrasyon sağlanmış, raporlama süreçleri iyileştirilmiş ve güvenlik denetim süreçleri yönetilebilir hale getirilmiştir.

Yayınlanmamış Güvenlik Açıkları Özel Taraması

Birçok web temelli uygulama kuruma özel olduğu için güvenlik açıkları da sadece o kuruma özel olmaktadır. Bu nedenle otomatize güvenlik açığı tarama yazılımları ile saptanamayan güvenlik açıkları, **GamaSEC** danışmanları tarafından geliştirilen araçlar, özel test yöntemleri ve açık kaynaklı "proxy" yazılımları kullanılarak denetlenmekte, böylece bilinmeyen güvenlik açıklarına yönelik testler uygulanmaktadır.

- Yapılandırma Hataları Analizi
- Programlama Hataları Analizi

Güvenlik Açıkları Kullanılarak Yetki Kazanılması

Uygulamada saptanmış olan güvenlik açıkları kullanılarak açığı barındıran veritabanı, uygulama sunucusu veya diğer sistemlere sızılmaya çalışılmaktadır. Yayınlanmış güvenlik açıklarının bir kısmının içeriği de açıklanmış ve "exploit" olarak bilinen kullanım yöntemleri yayınlanmıştır. Bir kısmının ise içeriği açıklanmamış veya açıklanmasına rağmen açığın kullanım yöntemleri belirlenememiştir. Bu sorunlara çözüm olarak **GamaSEC** danışmanları **GamaSEC** Exploit Framework yazılımını geliştirmiş, çok sayıda "exploit"i özelleştirmiş ve "exploit"i yazılmamış birçok açık için "exploit" geliştirerek tek bir yazılım altında birleştirmiştir. Ayrıca web uygulamalarına yönelik saldırılar için de özel exploit'ler hazırlanarak **GamaSEC** Exploit Framework yazılımına entegre edilmiştir.

Saptanan Güvenlik Açıklarının Değerlendirilmesi

Uygulama ve çalışma platformunda bulunan güvenlik açıkları derlenir, elde edilmiş tüm bilgiler toplanarak sınıflandırılır ve haritalandırılır. Çeşitli zayıflıklar, riski ve tahmin edilen saldırı yolları göz önüne alınarak önem derecelerine göre sıralanır. Tespit edilen güvenlik açıkları, taşıdıkları riskler değerlendirilir ve önemine göre sıralanır.

Çözüm Geliştirme ve Rapor Hazırlığı

Yukarıdaki tüm işlemler tamamlandıktan sonra, güvenlik uzmanlarımız tespit edilen bulgular ve güvenlik açıklarından hareketle her bir güvenlik açığı için çözüm önerileri oluşturur ve raporlar. Denetim Raporu, yönetici özeti, güvenlik açıklarının istatistiksel dağılımı, grafikleri, her bir açığın açıklaması ve çözüm önerilerini içermektedir. Bu rapor sayesinde güvenlik taramasına dahil edilen sistemlerin güçlü ve zayıf olduğu noktalar değerlendirilebilecektir.