NESİL
TEKNOLOJİ

METODOLOJİ

MOBİL UYGULAMA PENETRASYON TESTİ

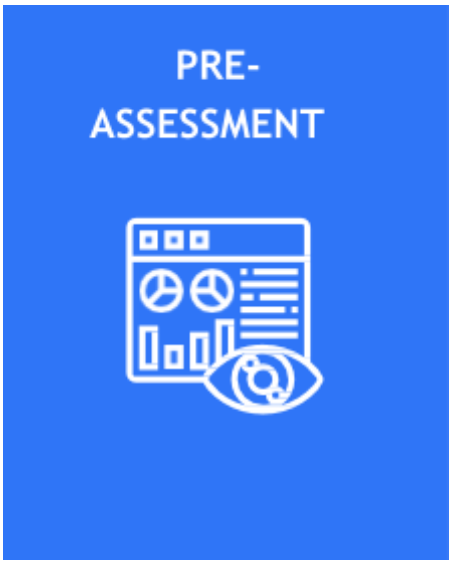
MOBİL

BAŞVURU DEĞERLENDİRME

Nesil Teknoloji'nin mobil uygulama değerlendirme metodolojisi, mobil uygulamalardaki ve altyapıdaki güvenlik zayıflıklarını tespit eder. Sıfır, kısmi veya tam bilgiyle yapılabilen bu değerlendirmeler, bir kuruluşun altyapısındaki uygulamaların numaralandırılması ve analiz edilmesiyle başlar. Daha sonra değerlendirme ekibi, mobil uygulama güvenliği eksikliklerini keşfetmek için uzman rehberliğinde test tekniklerinin yanı sıra hem endüstri standardı hem de dahili araçları kullanır. Ekip, güvenlik açıklarını belirledikten sonra, mobil dağıtımın hem istemci cihazındaki hem de sunucu tarafındaki hassas verileri, kimlik bilgilerini ve sistemleri tehlikeye atmak için kataloglanmış zayıf noktalardan manuel olarak yararlanır. Son olarak değerlendirme, ayrıntılı iyileştirme önerileri ve adımları da dahil olmak üzere, hedef ortamda bulunan tüm güvenlik sorunlarının kapsamlı bir raporuyla sonuçlanır.

SÜRECE GENEL BAKIŞ

Aşama 1



Aşama 2 ve 3

Aşama 4

AŞAMA 1: ÖN DEĞERLENDİRME

Projenin zamanında ve başarılı bir şekilde tamamlanmasını sağlamak için gerekli değerlendirme gereksinimlerinin karşılanması gerekir.

ÖN DEĞERLENDİRME GEREKSİNİMLERİ

VARLIKLAR	Mobil uygulama değerlendirmesine başlamadan önce değerlendirme ekibi aşağıdaki bilgileri ister: • İstemci ve sunucu mimarisi tasarım belgeleri • Uygulama belgeleri ve veri akışı diyagramları • İlgili sürümleri de dahil olmak üzere uygulamada kullanılan üçüncü taraf kütüphaneler • Mobil sürüm(ler) ve donanım (ör. telefon, Kindle vb.) desteklenir • Uygulamayı dağıtmak için kullanılan platform veya eğer yoksa APK ve IPA ikili dosyası • Mobil uygulama değerlendirmesi hibrit uygulama değerlendirmesinin parçasıysa Android Studio projesi veya Xcode projesi ve tüm bağımlılıklar • Varsa sunucu tarafı kaynak kodu • Kuruluşun mobil altyapısında kullanılmak üzere yapılandırılmış protokoller ve süreçler • Her uygulama rolü için iki kimlik bilgisi kümesi
HEDEFLER	İş başlamadan önce Nesil Teknoloji, sözleşmenin kapsamını, kısıtlamalarını ve aşağıdakileri içerebilecek ana hedeflerini belirlemek için müşterinin ekibiyle işbirliği yapar: • Ayrıcalıkların dikey/yatay olarak artırılması • Kısıtlanmış kaynaklar, hesap kimlik bilgileri veya hassas müşteri verileri gibi değerli varlıklara erişim elde etme
GEREKLİ ÖZEN	Değerlendirme ekibi, mobil uygulama ve bunun altında yatan API ve altyapı üzerindeki olası olumsuz etkilerini değerlendirmek için tüm ön değerlendirme bilgilerini ve önerilen test faaliyetlerini inceler. Bu inceleme, tüm birincil ve ikincil hedeflerin belirlenmesini içerir.

AŞAMA 2: BİLGİ TOPLAMA

Değerlendirme ekibi, uygulamayı ve kuruluşun ortamında kullanılan ilgili hizmetleri değerlendirmek için kapsamlı veri toplama gerçekleştirir.

BİLGİ TOPLAMA FAALİYETLERİ

UYGULAMA KAYIT / BAŞLANGIÇ GÖZLEM	Değerlendirme ekibi mobil uygulamanın kayıt ve ilk lansman sürecini inceler. Ekip aşağıdaki eylemleri gerçekleştirir: Uygulamayı root erişimli bir cihaza kurma Adb pull (Android), iFunBox (iOS) veya SCP (iOS) gibi araçları kullanarak uygulama kurulum dizininin tamamını ilk kez başlatmadan önce cihazdan çıkarma Burp Suite Pro veya benzer bir müdahale proxy'si ile cihazda Ortadaki Adam (MitM) saldırısı kurma Cihazda Filemon ve/veya iSpy/Frida gibi araçları kullanarak uygulamanın başlatılması Wireshark ve Burp Suite Pro ile cihazdaki tüm ağ trafiğinin kaydedilmesi Filemon ve/veya iSpy ile tüm dosya erişimini ve oluşturulmasını izleme
SUNUCU TARAFINDAN KEŞFİ	Değerlendirme ekibi, mobil uygulama ile ilgili tüm sunucularda çeşitli açılardan taramalar gerçekleştirir: Uygulamayı destekleyen internet ve web servisleri Uygulamanın kullanabileceği harici bağlantılar Tarama süreci şunları içerir: İlgili URL'leri taramak için Burp'un kullanılması Standart TCP/UDP bağlantı noktası taramalarının gerçekleştirilmesi Diğer içerik keşif faaliyetlerinin yürütülmesi

S

•

•

AŞAMA 3: MOBİL PENETRASYON TESTİ

Tüm hazırlık gereklilikleri karşılandıktan ve ortam hakkında yeterli bilgi elde edildikten sonra değerlendirme ekibi, mobil uygulamaya özel güvenlik açıklarını keşfetmek ve bunlardan yararlanmak için aşağıdaki eylemleri gerçekleştirir.

BİLGİ TOPLAMA FAALİYETLERİ

ÇALIŞMA ZAMANI YAMALARI	Ekip, kancalama, hata ayıklama ve çalışma zamanı yama tekniklerini kullanarak istemci tarafı güvenlik önlemlerini (jailbreak önleme ve hata ayıklama önleme gibi) yakalar, değiştirir ve atlatır. Ayrıca uygulamanın iç işleyişini de inceler. Bu çalışma zamanı saldırıları her bir uygulamaya özel olarak uyarlanır.
AĞ ENGELLENMESİ	Ekip, özel bir metodoloji ve araç seti kullanarak istemci-sunucu ağ trafiğini yakalar ve inceler. Ekip, gerekirse şifreli veri akışlarını görüntülemek ve değiştirmek için SSL ortadaki adam saldırılarından yararlanıyor. Ekip, Sosyal Güvenlik numaraları veya kredi kartı verileri gibi hassas bilgilerin ifşa edilmesiyle ilgili sorunları tespit etmek için uygulama trafiğini analiz ediyor.
DOSYA SİSTEMİ DEPOLAMA	Ekip, özellikle kimlik bilgileri, kişisel olarak tanımlanabilir bilgiler (PII), şifreleme anahtarları ve saldırganın yararlanabileceği diğer veriler gibi hassas bilgilere odaklanarak, istemci uygulamasının bıraktığı izleri bulmak için cihazın dosya sistemini tarar.
CİHAZ ANAHTAR DEPOLAMA DEPOLAMA	Mümkün olduğunda ekip, cihazın anahtar deposunda/anahtarlığında depolanan bilgileri almaya çalışır ve hassas bilgileri tanımlamak için verileri manuel olarak inceler.

BINARY REVERSE ENGINEERING	Gerektiğinde ekip, anti-jailbreak tespiti veya lisans anahtarı doğrulaması gibi istemci tarafı güvenlik önlemlerini atlamak için istemci uygulamasında ikili düzeyde tersine mühendislik yapar ve değiştirir.

SERVER-SIDE TESTING

API	Değerlendirme ekibi, mobil istemci uygulamasının etkileşime girdiği tanımlanmış uygulama sunucusu dağıtımlarına karşı standart web API sızma testi yöntemlerini kullanır. Keşfedilen sorunlar şunları içerebilir: • Kimlik doğrulama ve yetkilendirme kontrollerini atlamak • Rastgele komutlar ekleme • Uygunsuz oturum yönetiminin kötüye kullanılması • Veri güvenliği ve şifrelemedeki zayıflıkların belirlenmesi • İstemci tarafı doğrulamayı atlamak • Sorgu ekleme ve giriş doğrulamanın kötüye • kullanılması Dosya aktarım yeteneklerinin • kullanılması Uygulama ve hizmet mantığını atlamak

AŞAMA 4:ANALİZ VE RAPORLAMA

Nesil Teknoloji, güvenlik açıklarına önem dereceleri atamak için dahili uzmanlığı ve endüstri standardı metodolojileri kullanır. Her bulgunun ciddiyeti bağımsız olarak değerlendirilir ve daha yüksek derecelendirmeye sahip olanlar daha az bağımlılıkla daha yüksek teknik ve iş etkisine sahiptir.

TEKNİK ANALİZ FAALİYETLERİ

OLASILIK BELİRLEME	Her bir güvenlik açığı için değerlendirme ekibi, aşağıdaki faktörlere dayalı olarak bu güvenlik açığından yararlanma olasılığını değerlendirir: • Potansiyel tehdit kaynağının motivasyonu ve yeteneği • Güvenlik açığının özellikleri Karşı önlemlerin varlığı • ve etkinliği • Bir cihaza fiziksel erişimin ve/veya jailbreak'in gerekli olup olmadığı.
ETKİ ANALİZİ	Başarıyla yararlanılabilecek her bir güvenlik açığı için değerlendirme ekibi, güvenlik açıklarından yararlanmanın kuruluş ve müşterileri üzerindeki etkilerini gizlilik, bütünlük ve kullanılabilirlik açısından inceler ve değerlendirir.
ŞİDDET BELİRTİSİ	Nesil Teknoloji, dahili uzmanlığı ve Açık Web Uygulama Güvenliği Projesi (OWASP) ve Ortak Güvenlik Açığı Puanlama Sistemi (CVSS) gibi yaygın olarak kullanılan derecelendirme metodolojilerini kullanarak önem derecelerini atar. Her bulgunun ciddiyeti diğer bulgulardan bağımsız olarak değerlendirilir. Önem derecesi daha yüksek olan güvenlik açıklarının teknik ve iş etkisi daha fazladır ve diğer zayıflıklara daha az bağımlılık.

AŞAMA 5: İYİLEŞTİRME İNCELEMESİ (İSTEĞE BAĞLI)

İstenirse değerlendirme ekibi, müşteri güvenlik açıklarının giderildiğini onayladıktan sonra belirlenen güvenlik açıklarının taramasını ve testini tekrarlayabilir.