NESİL TEKNOLOJİ

METODOLOJİ

WEB UYGULAMASI PENETRASYON TESTİ

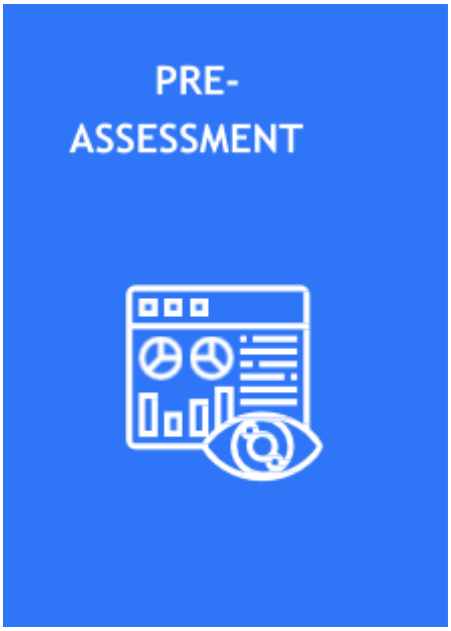
BAŞVURU

PENETRASYON TESTİ

Nesil Teknoloji, uygulamalardaki güvenlik açıklarını ortaya çıkarmak için otomatik ve manuel test yöntemlerinin bir kombinasyonunu kullanır. Süreç, uygulamanın taranması ve bilgi toplanmasıyla başlar. Daha sonra ekip, güvenlik açıklarını taramak için otomatik araçlar kullanır ve bulguları manuel olarak onaylar. Son olarak, hassas bilgilere ve ayrıcalıklı işlevlere erişim kazanmak için uygulamanın mantığındaki ve altyapısındaki herhangi bir hata veya zayıflıktan manuel olarak yararlanırlar.

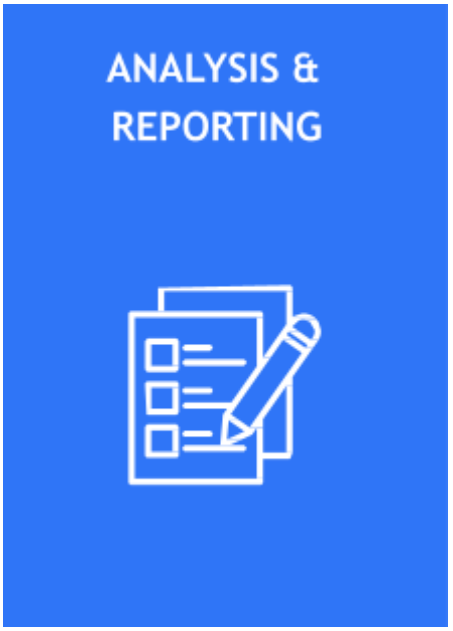
SÜRECE GENEL BAKIŞ

Aşama 1



Aşama 2 ve 3

Aşama 4



AŞAMA 1: ÖN DEĞERLENDİRME

Saha çalışmasına başlamadan önce, projenin zamanında ve başarılı bir şekilde tamamlanmasını garanti altına almak için gerekli değerlendirme kriterlerinin karşılanması esastır.

ÖN DEĞERLENDİRME GEREKSİNİMLERİ

UYGULAMA BİLGİLERİ	Değerlendirme ekibinin başvuru hakkında aşağıdakiler gibi kapsamlı bilgilere ihtiyacı vardır: • Başvuruyla ilgili her türlü belge • Tamamlanmış bir Uygulama Değerlendirme Kapsam Belirleme Anketi.
ÇEVRE ERİŞİMİ	Değerlendirme ekibinin, aşağıdakiler de dahil olmak üzere uygulamanın dağıtım ortamıyla ilgili kaynaklara erişmesi gerekebilir: • Dahili bir test ortamına erişim için VPN erişimi • Nesil Teknoloji'nin test altyapısının güvenlik cihazlarını atlamasına izin vermek için IP adreslerinin beyaz listeye alınması.
UYGULAMA ERİŞİMİ	Değerlendirme ekibinin aşağıdakiler de dahil olmak üzere başvuruyla ilgili kaynaklara erişmesi gerekebilir: • Her uygulama rolü için iki kimlik bilgisi kümesi • Farklı kiracılara ait olan veya farklı veri kümelerine erişimi olan hesaplar.
GEREKLİ ÖZEN	Değerlendirme sırasında Nesil Teknoloji, özellikle otomatik tarama, manuel doğrulama veya sızma testi gerçekleştirirken ağ kullanılabilirliği kesintilerini en aza indirmeye çalışır. Testten önce, değerlendirme ekibi müşteri ile çevresel istikrara yönelik riskleri tartışacak ve herhangi bir aksaklık gözlemlenmesi durumunda izlenecek süreci belirleyecektir.

YETKİLİ	Hedef ağın herhangi bir kısmı üçüncü taraf sistemlerinde barındırılıyorsa, değerlendirmeye başlamadan önce üçüncü taraftan test için yazılı izin alınmalıdır.

AŞAMA 2:

KEŞİF VE ZAFİYET TARAMA

Bu aşamada, bir uygulama ayak izi oluşturmak ve olası güvenlik açıklarını tespit etmek için otomatik araçlar ve manuel teknikler birlikte kullanılır.

KEŞİF VE ZAFİYET TARAMASI	
MANUEL KRAWL İLE OTOMATİK KEŞİF	Bir uygulama izini oluşturmak için hem manuel hem de otomatik teknikler kullanılır.
UYGULAMA TARAMASI	Takım, web uygulamasındaki güvenlik açıklarını tespit etmek için ticari ve açık kaynaklı uygulama güvenliği tarayıcıları kullanır. Otomatik araçlar, takımın kapsamı genişletmesine ve sınırlı bir süre zarfında çeşitli saldırılar gerçekleştirmesine olanak tanır.

AŞAMA 3: MANUEL TEST

Otomatik tarama araçları, temel uygulama kontrolleri için gereken süreyi önemli ölçüde azaltabilir ancak manuel değerlendirmenin yerini tutamaz.

MANUEL TEST	
OTOMATİK TARAMA DOĞRULAMASI	Otomatik güvenlik açığı tarama araçları, hedef ağı değerlendirmek için gereken süreyi azaltabilir, ancak çok sayıda hatalı pozitif sonuç üretme eğilimindedirler. Değerlendirme ekibi, yanlış pozitifleri ortadan kaldırmak ve ek bulguları ortaya çıkarmak için tüm bulguları manuel olarak inceler.
MANUEL SÖMÜRGELİK TEKNİKLERİ	Uygulama mantığını incelemek ve karmaşık ve kritik güvenlik açıklarını keşfetmek için manuel değerlendirme önemlidir. Bu bulgular daha sonra uygulamaya, hassas verilere ve temeldeki işletim sistemine yetkisiz erişim sağlamak için kullanılabilir. Manuel testler şunları içerebilir: • Kimlik doğrulama ve yetkilendirme kontrollerindeki boşlukları belirleme • Oturum yönetiminin incelenmesi • Veri güvenliği ve şifreleme zayıflıklarını keşfetme • Enjeksiyon güvenlik açıklarından ve zayıf giriş doğrulamasından yararlanma • Dosya aktarım özelliğini kullanma • Uygulama mantığını atlatmak

AŞAMA 4: ANALİZ VE RAPORLAMA

Tehditleri ve güvenlik açıklarını belirledikten sonra değerlendirme ekibi aşağıdaki faaliyetleri yürütür:

TEKNİK ANALİZ AKTİVİTELERİ	
OLASILIK BELİRLEME	Her bir güvenlik açığı için değerlendirme ekibi, aşağıdaki faktörlere dayanarak bu güvenlik açığından yararlanma olasılığını belirler: • Tehdit kaynağının motivasyonu ve yeteneği • Güvenlik açığının doğası • Kontrollerin varlığı ve etkinliği.
ETKİ ANALİZİ	Değerlendirme ekibi, her güvenlik açığı için, kötüye kullanımın sistem ve verilerin gizliliği, bütünlüğü ve kullanılabilirliği üzerindeki etkisini değerlendirir ve hesaplar.
ŞİDDET BELİRLEME	Değerlendirme ekibi, istismar olasılığını ve etkisini dikkate alarak ve kritik, yüksek, orta veya düşük olarak sınıflandırarak, her bir güvenlik açığının ciddiyetini belirlemek için istismar olasılığını ve etkisini değerlendirir.

AŞAMA 5: İYİLEŞTİRME İNCELEMESİ (İSTEĞE BAĞLI)

Değerlendirme ekibi, müşteri güvenlik açıklarının giderildiğini (istenirse) doğruladıktan sonra belirlenen güvenlik açıklarının taranmasını ve test edilmesini tekrarlayabilir.