TELNET

ZAFİYET NEDİR: Telnet bağlantıları şifrelenmediği için, ağ üzerindeki veriler kolayca yakalanabilir ve saldırganlar tarafından kullanıcı adları, şifreleri gibi hassas bilgiler ele geçirilebilir.

NASIL OLUŞUR: Genellikle ağ üzerindeki verilerin açık metin olarak iletilmesi veya şifrelenmemiş olması durumunda ortaya çıkar. Saldırgan ağ trafiğini dinleyerek (sniffing) iletilen verileri kolayca yakalayabilir.

ETKİLERİ: Saldırgan hassas bilgilere erişebilir ve bunları kötü niyetli amaçlar için kullanabilir.

NASIL ÖNLENİR: Şifreli İletişim protokolleri kullanmak, güvenli bağlantı yöntemleri kullanmak, ağ trafigini şifrelemek

FTP

ZAFİYET NEDİR: Anonim erişim özelliği, sunucuya kimlik doğrulaması yapmadan erişim sağlama imkanı sunar. Bu durum, güvenlik açısından risk oluşturabilir ve "FTP anonim erişim zafiyeti" olarak bilinir.

NASIL OLUŞUR: Genellikle sunucu yapılandırmasındaki yanlışlıklardan veya güvenlik önlemlerinin yetersizliğinden kaynaklanır.

ETKİLERİ: Gizli bilgiler sızdırılır, kötü amaçlı yazılımlar yayılır, kurumlar tehlikeye girebilir.

NASIL ÖNLENİR: Güvenlik duvarları ve izleme sistemleri kurulabilir, anonim erişimi devre dışı bırakmak.

QUERY GATE

ZAFİYET NEDİR: Hedef makineye nmap ile bir tarama yaptığımız zaman mysql veritabanında bir açıklık oldugunu farkediyoruz. Gerekli parametreleri yazdıktan sonra kendimizi en yetkili kullanıcıya yükseltiyoruz. Güvenlik duvarlarının yetersizliğidir.

NASIL OLUŞUR: Zayıf şifreler, güvenlik duvarlarının yetersiz kullanılması, güncel olmayan yazılım sürümleri, güvenlik açıklıklarından meydane gelebilir.

ETKİLERİ: Veritabanından veri sızabilir, hizmet kesintisi yaşanabilir, finansal kayıplar yaşanabilir.

NASIL ÖNLENİR: Güvenlik bilincinin artırılması, güvenlik denetimlerinin çoğaltılması, izin ve erişim kontrollerinin sisteme girilmesi, daha güçlü şifreler kullanılması.

DİSCOVER LERNAEAN

ZAFİYET NEDİR: CVE-2021-4177 , CVE-2016-0778

NASIL OLUŞUR: Dizin geçişleri sırası doğrulama hatası ile dizin atlatma zafiyeti ortaya çıkabilir. Kötü tasarım, kod hataları gibi benzer sebeblerden ortaya çıkar.

ETKİLERİ NELERDİR: Yetkisiz erişim, veri sızıntısı, hizmet kesintisi gibi etkiler yaratabilir.

NASIL ÖNLENİR: Yazılım güncellemelerini sık sık yapmak. Dizin geçişleri sırasındaki doğrulama hatalarını gidermek.

BEE

ZAFİYET NEDİR: SQL Injection zafiyeti, bir uygulamanın veritabanıyla etkileşime girdiği her yerde bulunabilir ve genellikle kullanıcı girdilerinin yeterince doğrulanmamasının nedeniyle oluşur. File upload zafiyeti, kullanıcılar tarafından yüklenen dosyaları yeterince kontrol edilmeden sunucu tarafından kabul edilmesi sonucu ortaya çıkar.

ETKİLERİ NELERDİR: Hassas bilgilerin ifşa edilmesi, verilerin değiştirilmesi veya silinmesi gibi sonuçları olabilir. File upload zafiyeti için ise zararlı kodları içeren dosyaları yüklenebilir, sunucuya erişim kazanabilir.

NASIL ÖNLENİR: SQL ınjection zafiyeti, paremetre bağlama ve hazır sorgular kullanma, uygun kodlama, güvenlik duvarı oluşturma gibi önlemler alınabilir. File upload zafiyeti, dosya yükleme sırasında virüs tarayıcısı kullanmak, yüklenen dosyaları harici bir dizinde saklamak.

LEAF

ZAFİYET NEDİR: Web uygulamarının kullanıcı girdilerini yeterince doğrulamaması ve template motorunun bu girdileri doğrudan işlemesi sonucu ortaya çıkar.

ETKİLERİ NELERDİR: yetki yükseltme, veri sızdırma, kod yürütme gibi sonuçlar ortaya çıkabilir.

NASIL ÖNLENİR: Kullanıcı girdilerin doğru işlenmesi, sablon motorunun doğru işlenmesi.

VENOMOUS

ZAFİYET NEDİR: url üzerinden page parametresi manipüle ederek başka dosyalara erişim sağlamak.

NASIL OLUŞUR: Genellikle web uygulamarında kullanıcı girdilerinin yeterince doğrulanmaması sonucu veya güvenli bir şekilde işlenmemesi sonucu ortaya çıkabilir.

ETKİLERİ NELERDİR: Hassas dosyalara erişim, kötü niyetli dosya yürütme

NASIL ÖNLENİR: Dosya yollarının sabitlenmesi, dosyaya erişim kontrolleri getirilmesi, kullanıcı girdilerinin doğrulanması.

SUPER PROCESS

ZAFİYET NEDİR: SUID yetkisi, güvenlik açıklarına neden olabilir. Suıd olarak işaretlenmiş bir dosyayı kullanarak sistemdeki ayrıcalıklı erişim seviyelerine ulaşmalarını sağlayabilir. Bu durumda yetkisiz erişime olanak sağlar.

NASIL ÖNLENİR: Gereksiz suıd dosyalarını kaldırarak, gerekli olan kullanıcıların sadece suıd dosyalarını çalıştırmasına izin vermek.

ETKİLERİ NELERDİR: Veri sızıntısı, sistem dışına veri aktarmak, ayrıcalıklı erişim gibi büyük riskli sonuçlar ortaya çıkabilir.

GLİTCH

ZAFİYET NEDİR: Nostromo web sunucunun güvenlik kontrollerini yeterince sağlayamamasından zafiyet ortaya çıkar. Sunucuda yetkisiz kod yürütebilirler ve sistemde istimarlara neden olur.

NASIL ÖNLENİR: Güncellemere dikkat etmek, yeni yama varsa uygulamak, güvenlik ile ilgili politikaları dikkatlice okumak.

ETKİLERİ NELERDİR: Sisteme sızan kişi uzaktan kod yürütebilir, yetkisi olmayan bir kişi kendini en yetkili kişiye yükseltebilir, veri sızıntısı olabilir.