HACKVISER GENEL ÖDEVİ

ZAFİYETLER HAKKINDA RAPOR

1) Arrow

Zafiyet Nedir?

Bu makinedeki zafiyet telnet sunucusunda root için zayıf şifre kullanımıdır.

Zafiyet Nasıl Oluşur?

Root kullanıcısı için root gibi kolay tahmin edilebilir bir şifre kullanılmasıyla oluşur.

Etkileri Nelerdir?

- Sisteme yetkisiz erişim sağlanabilir.
- Veriler çalınabilir veya sisteme zarar verilebilir.

Kapatılması İçin Öneriler

- Varsayılan şifreler güçlü parolalarla değiştirilmeli.
- Alternatif olarak sadece belli IP'lere erişim izni de verilebilir.

2) File Hunter

Zafiyet Nedir?

Bu makinedeki zafiyet, FTP sunucusunda anonymous login özelliğinin açık olması ve kullanıcı bilgilerini içeren bir dosyanın bulunmasıdır.

Zafiyet Nasıl Oluşur?

FTP sunucusunda anonymous girişlerin aktif olması ile oluşur.

Etkileri Nelerdir?

- Saldırganlar anonim giriş yaparak dosyalara erişip kullanıcı bilgilerini çalabilir.
- Sistem güvenliği ciddi şekilde tehlikeye girer, veri sızıntısı yaşanabilir.

Kapatılması İçin Öneriler

- FTP'de anonymous giriş devre dışı bırakılmalı.
- Hassas bilgi içeren dosyalar daha güvenli bir şekilde saklanmalı.

3) Secure Command

Zafiyet Nedir?

Bu makinedeki zafiyet, bir SSH kullanıcısının root hesabına root şifresi ile kolayca giriş yapabilmesidir.

Zafiyet Nasıl Oluşur?

SSH sunucusunda root hesabı için zayıf bir şifre kullanılması ve root girişinin izinli olması, yetkisiz erişim riskini artırır.

Etkileri Nelerdir?

- Saldırganlar root yetkilerine erişerek sistemi tamamen kontrol edebilir.
- Tüm kullanıcı ve veritabanı bilgileri tehlikeye girer.

Kapatılması İçin Öneriler

- Root için güçlü ve karmaşık bir şifre kullanılmalı.
- SSH üzerinden root erişimi devre dışı bırakılmalı.

4) Query Gate

Zafiyet Nedir?

Bu makinedeki zafiyet, MySQL sunucusuna root kullanıcı adıyla şifre sorulmadan giriş yapılabilmesidir.

Zafiyet Nasıl Oluşur?

MySQL sunucusunun root kullanıcısına şifre atanmadığında, herhangi bir kimlik doğrulama olmadan yetkili erişim sağlanır ve bu da sistemin güvenliğini ciddi şekilde tehlikeye atar.

Etkileri Nelerdir?

- Saldırganlar veritabanına tam erişim sağlayarak verileri çalabilir veya değiştirebilir.
- Veritabanı üzerinde tam kontrol sağlanarak tüm sistem tehlikeye atılabilir.

Kapatılması İçin Öneriler

- MySQL root hesabına güçlü bir şifre atanmalı.
- Root erişimi yalnızca belli IP'ler ile sınırlandırılmalı.

5) Discover Learnean

Zafiyet Nedir?

Bu makinedeki zafiyet, web sunucusunda bulunan file manager servisinin varsayılan şifreyle korunmasıdır.

Zafiyet Nasıl Oluşur?

Varsayılan şifrenin değiştirilmemesi, saldırganların internetten bu şifreyi kolayca bulup sisteme erişmesine olanak tanır.

Etkileri Nelerdir?

- Saldırganlar file manager üzerinden dosyalara erişim sağlayarak hassas verileri çalabilir.
- Tüm web sunucusunun güvenliği tehlikeye girer ve veri bütünlüğü bozulabilir.

Kapatılması İçin Öneriler

- Varsayılan şifre güçlü bir şifre ile değiştirilmelidir.
- File manager erişimi yalnızca belli IP'ler ile sınırlandırılmalı.

6) Bee

Zafiyet Nedir?

Bu makinedeki zafiyet, web sunucusunda giriş kısmında SQL injection ve profil resmi yükleme bölümünde file upload zayıflıklarıdır.

Zafiyet Nasıl Oluşur?

Kullanıcı giriş formuna kötü niyetli SQL kodları eklenerek veritabanına izinsiz erişim sağlanabilir. Profil resmi yükleme bölümünde gerekli denetimlerin yapılmaması, zararlı dosyaların sunucuya yüklenmesine olanak tanır.

Etkileri Nelerdir?

- SQL injection sayesinde saldırgan, veritabanına erişip kullanıcı bilgilerini çalabilir.
- File upload zafiyeti, saldırganların sunucuya zararlı yazılımlar yüklemesine ve sistemi ele geçirmesine neden olabilir.

Kapatılması İçin Öneriler

- Giriş formlarında kullanıcı girdileri temizlenmeli ve parametrik sorgular kullanılmalıdır.
- File upload alanında dosya türleri ve boyutları sınırlanmalı, yüklenen dosyaların içeriği kontrol edilmelidir.

7) Leaf

Zafiyet Nedir?

Bu makinedeki zafiyet, web sunucusundaki ürün yorumları bölümünde SSTI (Server-Side Template Injection) açığıdır.

Zafiyet Nasıl Oluşur?

Kullanıcılar, ürün yorumlarına kötü niyetli kodlar ekleyerek sunucu tarafında çalıştırılmasını sağlayabilir. Bu durum, şablon motorunun yeterince güvenli olmamasından kaynaklanmaktadır.

Etkileri Nelerdir?

- Saldırganlar, sunucu üzerinde zararlı komutlar çalıştırarak sistemde tam kontrol sağlayabilir.
- Kullanıcı bilgileri çalınabilir veya veri manipülasyonu yapılabilir.

Kapatılması İçin Öneriler

- Kullanıcı girdileri, sunucu tarafında sıkı bir şekilde doğrulanmalı ve temizlenmelidir.
- Şablon motorlarının güvenliğini artırmak için güvenli kodlama uygulamaları benimsenmelidir.

8) Venomous

Zafiyet Nedir?

Bu makinedeki zafiyet, fatura görüntüleme sayfasında LFI (Local File Inclusion) açığıdır.

Zafiyet Nasıl Oluşur?

LFI, kullanıcının girdiği dosya yolunu kontrol etmeyen bir uygulama sayesinde oluşur. Bu durumda, kullanıcılar zararlı dosyaları sunucuya dahil edebilir ve istenmeyen dosyaları görüntüleyebilir.

Etkileri Nelerdir?

- Sunucu üzerindeki hassas dosyalara erişim sağlanarak sistem bilgileri ele geçirilebilir.
- Uygulamanın güvenliği ve bütünlüğü tehlikeye girebilir.

Kapatılması İçin Öneriler

- Dosya yolları için beyaz liste yöntemleri kullanılmalı, yalnızca belirlenen dosyaların erişimine izin verilmelidir.

9) Super Process

Zafiyet Nedir?

Bu makinedeki zafiyet, web sunucusunda çalışan eski Supervisor sürümünden kaynaklanan RCE (Remote Code Execution) açığıdır.

Zafiyet Nasıl Oluşur?

Eski Supervisor sürümü, uzaktan kötü niyetli kodların çalıştırılmasına izin veren güvenlik açıkları barındırmaktadır. Ayrıca, sistem içinde bulunan SUID bitli dosyalar bu açıkların istismarını kolaylaştırmaktadır.

Etkileri Nelerdir?

- Saldırganlar, uzaktan sistem üzerinde yetkisiz kod çalıştırabilir ve sisteme tam erişim sağlayabilir.
- Sistemin bütünlüğü, güvenliği ve veri gizliliği ciddi şekilde tehlikeye girebilir.

Kapatılması İçin Öneriler

- Supervisor sürümü güncellenmeli ve güvenlik yamaları uygulanmalıdır.
- Sistem güvenlik politikaları gözden geçirilmeli ve sıkı bir erişim kontrolü sağlanmalıdır.

10) Glitch

Zafiyet Nedir?

Bu makinedeki zafiyet, web sunucusunda çalışan Nostromo servisinin eski sürümünden kaynaklanan RCE (Remote Code Execution) açığıdır. Ayrıca, sunucunun Linux sürümünde de yetki yükseltme (privilege escalation) zafiyeti bulunmaktadır.

Zafiyet Nasıl Oluşur?

Nostromo servisinin eski sürümü, uzaktan kötü niyetli kodların çalıştırılmasına olanak tanıyan güvenlik açıkları barındırır. Sunucudaki Linux sürümü, bilinen güvenlik açıkları veya zayıf yapılandırmalar nedeniyle yetki yükseltme işlemlerine olanak tanır.

Etkileri Nelerdir?

- Saldırganlar, uzaktan sisteme kötü niyetli kod yükleyebilir ve çalıştırabilir.
- Sistemin bütünlüğü, güvenliği ve veri gizliliği ciddi şekilde tehlikeye girebilir.

Kapatılması İçin Öneriler

- Nostromo servisi güncellenmeli ve güvenlik yamaları uygulanmalıdır. Linux sunucu sürümü de güncellenmeli.

11) Find and Crack

Zafiyet Nedir?

Bu makinedeki zafiyet, kullanılan GLPI servisinin eski sürümünde bulunan RCE (Remote Code Execution) açığıdır.

Zafiyet Nasıl Oluşur?

GLPI'nin eski sürümleri, güvenlik açıkları nedeniyle uzaktan kötü niyetli kodların çalıştırılmasına olanak tanıyan hatalar barındırmaktadır. Bu açıklar, saldırganların sistem üzerinde yetkisiz eylemler gerçekleştirmesine neden olabilir.

Etkileri Nelerdir?

- Saldırganlar, uzaktan GLPI servisine kötü niyetli kod yükleyerek çalıştırabilir.
- Sistem üzerinde tam kontrol sağlanarak hassas verilere erişim elde edilebilir.

Kapatılması İçin Öneriler

- GLPI servisi hemen güncellenmeli ve güvenlik yamaları uygulanmalıdır.
- Sistem üzerindeki erişim kontrolleri sıkılaştırılmalı ve gereksiz yetkiler kaldırılmalıdır.