
T.C.
ERCİYES ÜNİVERSİTY
MÜHENDİSLİK FAKÜLTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ
BİLGİ GÜVENLİĞİ
https://erupass.recinan.net/
ERÜPASS LOCAL
PASSWORD MANAGER
HAZIRLAYANLAR
Emir Ahmet YILMAZ 1030510692
Recep İNAN 1030510582

https://erupass.recinan.net/

Kasa Yönetimi ve Yönlendirme

İstemci uygulaması, kullanıcının kimlik doğrulama durumuna göre arayüzünü dinamik olarak şekillendirir ve sağlam bir yönlendirme mantığı kullanır. VaultContext içindeki useVault hook'u tarafından yönetilen dört temel durum—unknown, init, locked ve unlocked—hangi arayüzün görüntüleneceğini belirler.

Bu bilinçli mimari seçim, öğe veri yönetiminin (ItemsContext) her zaman kimlik doğrulama durumuna (VaultContext) tabi ve bağımlı olmasını sağlar.

Yetkisiz Oturumlar ve Otomatik Kilitleme

Bir oturum başladığında, istemci tarafından yapılan tüm yetkili API çağrıları `customFetch` yardımcı programı aracılığıyla yönetilir. Bu işlev, her isteğe otomatik olarak `Authorization: Bearer <token>` başlığını ekler.

Sunucu tarafında, korumalı uç noktalar `get_unlocked_key_or_401` işleviyle güvence altına alınır. Bu, gelen jetonu doğrular ve ilgili şifreleme anahtarını bellekteki oturum deposundan alır.

Geçersiz veya süresi dolmuş jetonlarla yapılan istekler, güvenlik protokollerini güçlendirerek 401 Unauthorized hatasıyla reddedilir.

Çift Taraflı Otomatik Kilitleme Mekanizması

Önemli bir proaktif güvenlik özelliği, hem istemci hem de sunucu taraflarında eşzamanlı olarak çalışan 180 saniyelik (3 dakikalık) otomatik kilitleme mekanizmasıdır.

İstemci Tarafı Otomatik Kilitleme

`ERÜPassContext` içinde, bir zamanlayıcı (`setInterval`), `touchActivity` işlevi aracılığıyla kullanıcı etkileşimlerini izler. 3 dakika boyunca herhangi bir etkileşim olmazsa, `lockERÜPass()`'u tetikler, istemci tarafı oturumu sonlandırır ve durumu "kilitli" olarak ayarlar.

Sunucu Tarafı Otomatik Kilitleme

`get_key_by_token` işlevi, her jeton doğrulaması sırasında oturumun `last_used` zaman damgasını kontrol eder. Son kullanımdan bu yana 180 saniyeden fazla zaman geçtiyse, oturum sunucu belleğinden otomatik olarak silinir ve `_zeroize` ile güvenli bir şekilde temizlenir.

Scrypt ile Sağlam Anahtar Türetme

Kullanıcının ana parolasından 256-bit simetrik şifreleme anahtarını türetmek için sistem, Scrypt algoritmasını kullanır.

Scrypt, özellikle hesaplama ve bellek yoğun olacak şekilde tasarlanmıştır, bu da onu kaba kuvvet saldırılarına karşı oldukça dirençli hale getirir.

Scrypt parametreleri `KdfParams` içinde tanımlanır ve her kasa için `vault_meta` tablosunda saklanır, bu da güvenlik standartları geliştikçe gelecekteki güncellemelere olanak tanır.

Gelişmiş Güvenlik için Benzersiz Tuzlar

Brute-force ve rainbow table saldırılarını önlemek için, her kasa oluşturma işleminde `generate_salt()` fonksiyonu kullanılarak 16 baytlık, kriptografik olarak güvenli, benzersiz bir "salt" değeri üretilir.

Bu salt, anahtar türetme sürecine dahil edilerek, aynı parolaların farklı kasalarda farklı anahtarlar üretmesini sağlar.

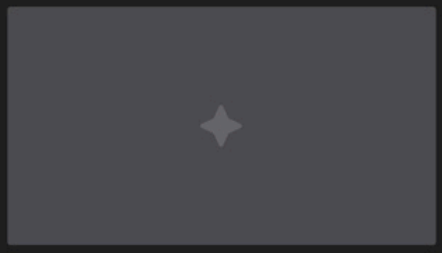
Bu, önceden hesaplanmış saldırı tablolarını etkisiz hale getirerek kritik bir savunma katmanı ekler.

Ek Kimlik Doğrulamalı Veri (AAD)

Sistem, gizli olmasa bile bütünlüğü çok önemli olan bağlamsal bilgileri korumak için Ek Kimlik Doğrulamalı Veri (AAD) desteği sunar.

`aad` parametresi, `b"item:web"` gibi veriler içerir. Bu veriler, şifre çözme sırasında kimlik doğrulamadan geçer.

AAD ile oynanırsa, şifre çözme başarısız olur ve veri manipülasyonuna ve tekrar oynatma saldırılarına karşı ek bir koruma katmanı sağlar.



	id	type	title	encrypted_data	created_at	updated_at
1	a8e387e6-e7bf-4928-83c7-890be3a14adc	web	asdasd	v1:5GJ_ZenhygCqXNV8:T_zdJgU4_sxvIf-WPADqcPZnJIQ0-	1,767,003,453	1,767,003,453

AES-256-GCM ile Veri Şifreleme

AES-256-GCM, verilerinizin güvenliğini sağlamak için kullanılan gelişmiş bir şifreleme standardıdır. Bu algoritma, endüstriyel güvenlik protokollerinin temelini oluşturur ve aşağıdaki kritik özellikleri sağlar:

Gizlilik

Verilerinizi yetkisiz erişime karşı korur, yalnızca belirlenmiş alıcılar tarafından okunabilmesini sağlar.

Bütünlük

Verinin değiştirilmediğini veya bozulmadığını garanti eder, aktarım sırasında manipülasyonları engeller.

Gerçeklik

Verinin gerçekten iddia edilen kaynaktan geldiğini doğrular, taklit ve kimlik avı saldırılarına karşı koruma sağlar.

verify_blob Aracılığıyla Şifre Doğrulaması

ERÜPass, şifre karmalarını depolamak yerine daha güvenli bir verify_blob mekanizması kullanır, böylece şifre karmaları ele geçirilirse çevrimdışı kaba kuvvet saldırısı riskini ortadan kaldırır.

Kasa Oluşturma

Ana şifreden türetilen şifreleme anahtarı kullanılarak `b"vault-check"` gibi sabit bir metin şifrelenir ve `verify_blob` olarak depolanır.

Şifre Girişi

Kullanıcı şifresini girdiğinde, anahtar yeniden türetilir.

Sunucu Doğrulaması

Sunucu, yeni türetilen anahtarı kullanarak depolanan `verify_blob`'u çözmeye çalışır.

Başarılı Şifre Çözme

Şifre çözme başarılı olursa ve metin orijinal `b"vault-check"` ile eşleşirse, şifre doğrudur. `AES-GCM`'nin yanlış anahtarlar için sabit zamanlı hatası, zamanlama saldırılarını önler.

Bu yaklaşım, geleneksel şifre karmalamaya göre önemli bir güvenlik iyileştirmesidir.

Veritabanı Güvenliği: Şifreli Veri ve Meta Veri

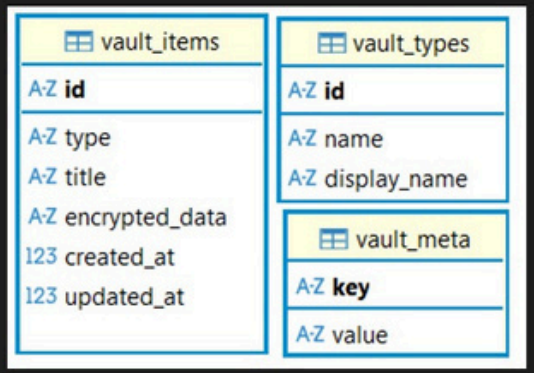
`encrypted_data` sütunu, veritabanının hiçbir zaman düz metin görmemesini sağlar. Tüm şifreleme ve şifre çözme işlemleri, kullanıcının ana parolasından türetilen ve yalnızca bellekte tutulan bir anahtar kullanılarak uygulama katmanında gerçekleşir.

vault_types Tablosu

Önceden tanımlanmış öğe türlerini (web, email, ssh, note) ve bunların kullanıcı arayüzü temsilini tanımlar; kategorizasyon ve filtreleme için kullanılır.

vault_meta Tablosu

Kritik kasa meta verileri için bir anahtar-değer deposudur, `meta_get` ve `meta_set` fonksiyonları tarafından yönetilir. Kriptografik yükseltmelere izin vererek `kdf_salt`, `verify_blob` ve Scrypt parametrelerini (`kdf_n`, `kdf_r`, `kdf_p`) saklar.



Temel Güvenlik Özellikleri

ERÜPass, sektör standardı kriptografiyi yenilikçi savunma mekanizmalarıyla birleştirerek çok katmanlı bir güvenlik yaklaşımı uygulamaktadır.

→ Scrypt & AES-GCM

Anahtar türetme ve veri şifreleme için bu sağlam, sektör standardı algoritmaların kullanılması, veri gizliliği ve bütünlüğü için güçlü bir temel sağlar.

→ Şifre Doğrulama Bloğu (verify_blob)

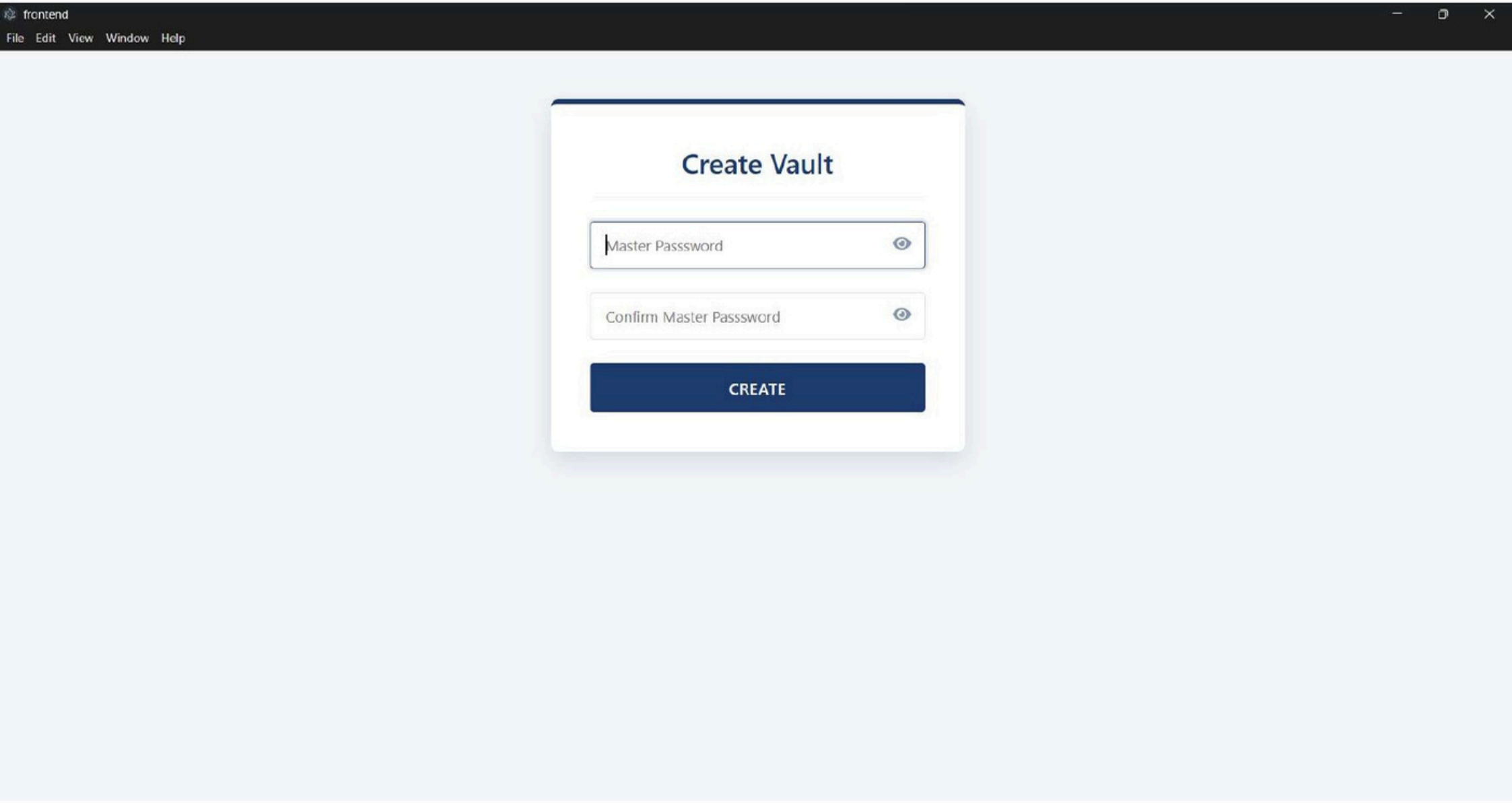
Çevrimdışı kaba kuvvet saldırılarına karşı yenilikçi bir koruma; şifre karmalarını depolamaktan kaçınarak bunun yerine şifrelenmiş bir doğrulama nesnesi kullanır.

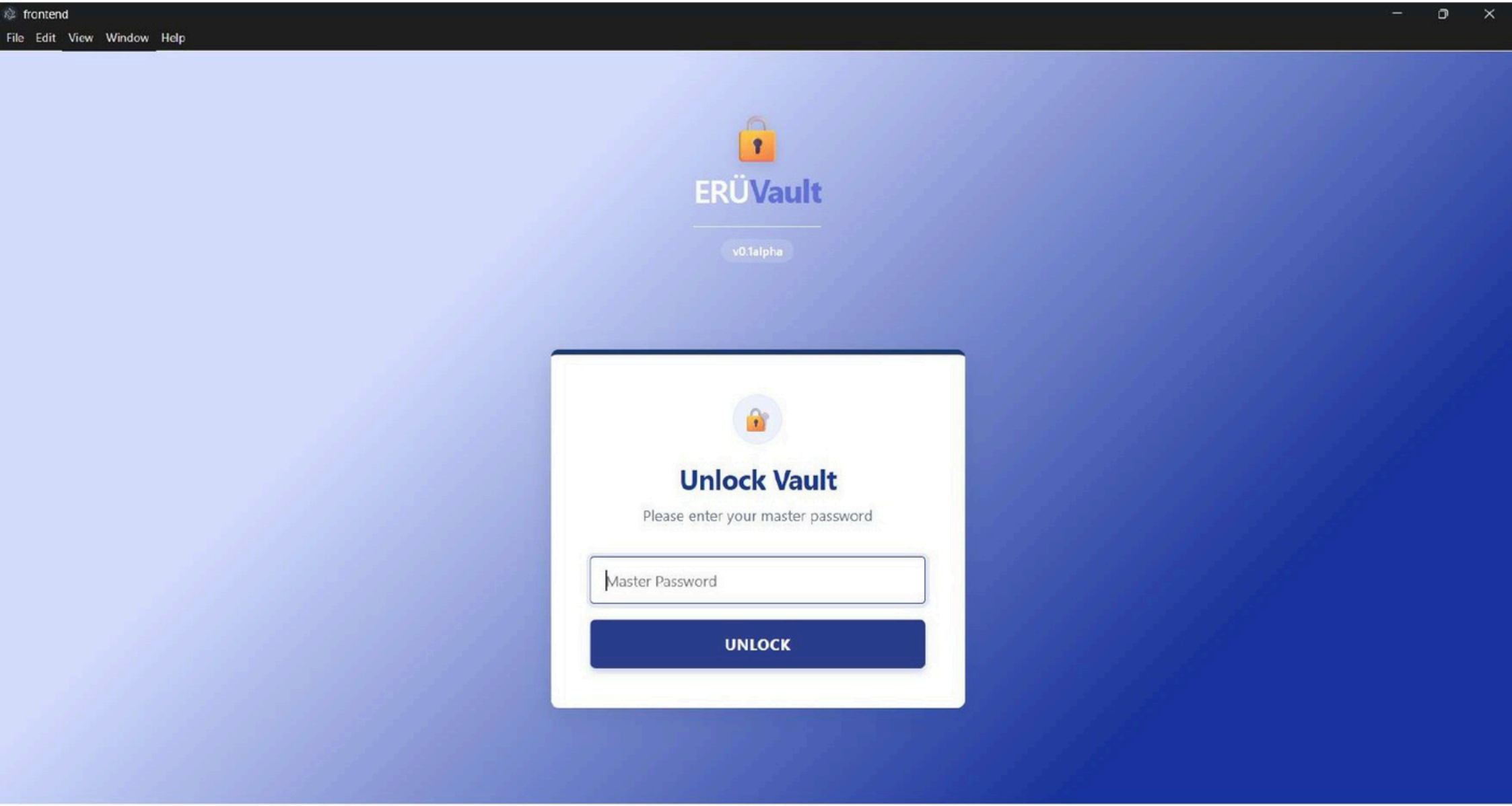
→ Çift Taraflı Otomatik Kilitleme

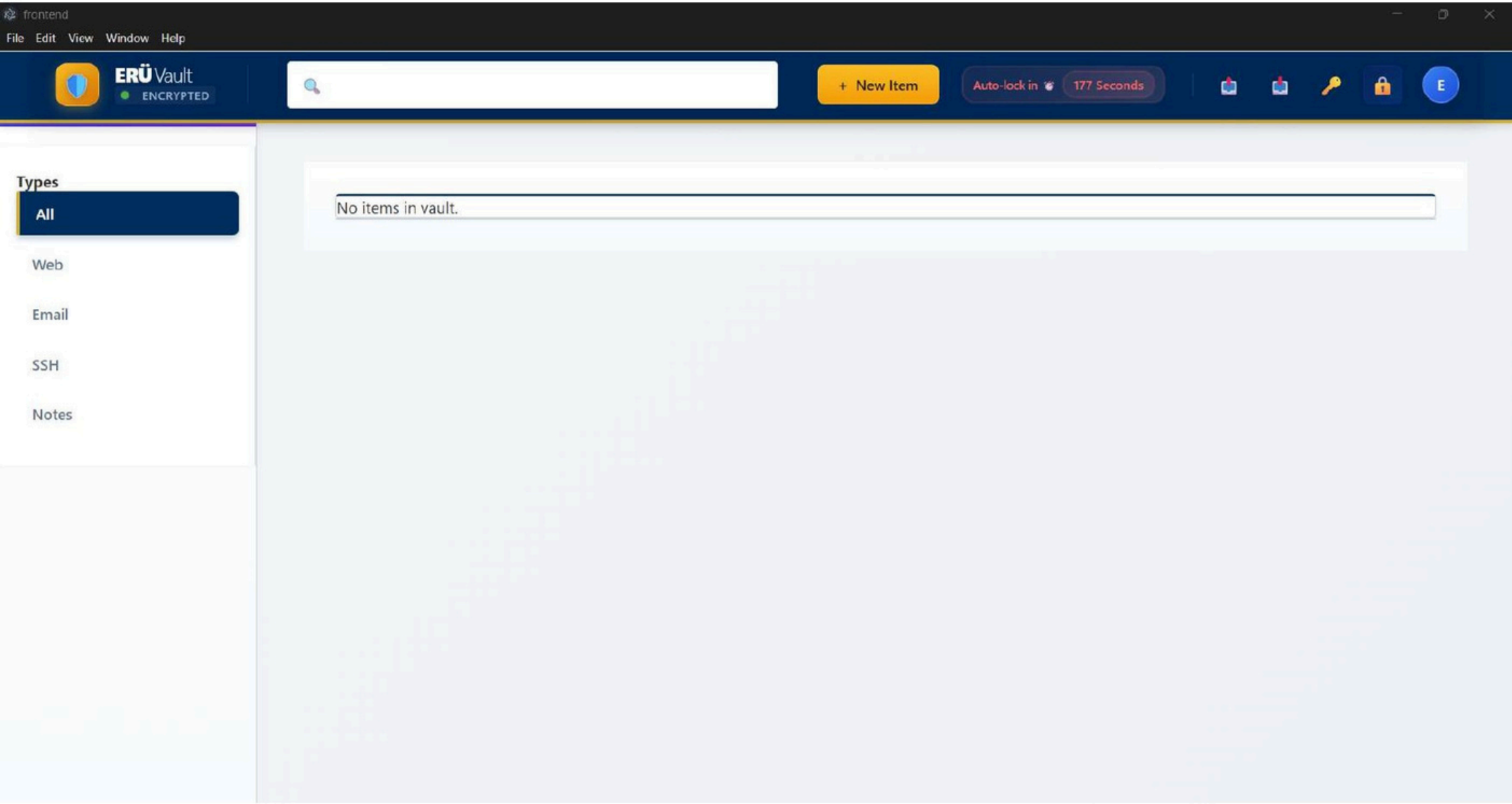
Hem istemci hem de sunucuda 3 dakikalık boşta kalma süresi, unutulmuş oturumlar veya fiziksel erişim gibi senaryolarda veri sızıntısı risklerini en aza indirir.

→ Katmanlı Saldırı Önleme

Kimlik doğrulama uç noktalarındaki Birleşik Hız Sınırlama ve Aşamalı Geri Çekilme mekanizmaları, kaba kuvvet saldırılarını pratikte imkansız hale getirir.


frontend
File Edit View Window Help
Create Vault
Master Passsword
Confirm Master Passsword
CREATE


frontend
File Edit View Window Help
ERÜVault
v0.1alpha
Unlock Vault
Please enter your master password
Master Password
UNLOCK


frontend
File Edit View Window Help
ERÜ Vault
ENCRYPTED
+ New Item
Auto-lock in 177 Seconds
E
Types
All
Web
Email
SSH
Notes
No items in vault.