Bankacılık Uygulamalarında Güvenli Yazılım Tasarımı İncelemesi

- ***Proje Tanımı***

Günümüzde, mobil bankacılık uygulamaları finansal işlemleri gerçekleştirmek için yaygın olarak kullanılmaktadır. Bu uygulamalar, hassas müşteri verilerini ve finansal bilgileri barındırdıkları için siber saldırılara karşı oldukça savunmasızdır. Bu nedenle, bankacılık uygulamalarında güvenli yazılım tasarımı, finansal sistemlerin bütünlüğü ve kullanıcıların korunması için kritik önem taşımaktadır. Banka uygulamalarında güvenli yazılım tasarımının incelenmesini ve en iyi güvenlik uygulamalarını ele alacaktır.

- ***Güvenlik Prensipleri***

Gizlilik (Confidentiality): Gizlilik, kullanıcı bilgileri ve işlemlerinin yetkisiz erişimlerden korunmasını sağlar. Banka uygulamaları, verilerin yalnızca yetkili kullanıcılar tarafından görüntülenebilmesini garanti etmelidir.

Bütünlük (Integrity): Bütünlük, verilerin doğruluğunu ve tutarlılığını korur. Banka uygulamaları, verilerin yetkisiz değişikliklere karşı korunmasını ve her türlü değişikliğin izlenebilmesini sağlamalıdır.

Erişilebilirlik (Availability): Erişilebilirlik, hizmetlerin kullanıcılar tarafından kesintisiz olarak erişilebilir olmasını sağlar. Banka uygulamaları, herhangi bir saldırı veya sistem arızası durumunda dahi hizmet vermeye devam etmelidir.

- ***Güvenli Yazılım Tasarımı Yöntemleri***

Tehdit Modelleme: Tehdit modelleme, potansiyel güvenlik tehditlerini tanımlamak ve bu tehditlere karşı uygun güvenlik önlemlerini belirlemek için kullanılır. Banka uygulamalarında tehdit modellemesi, saldırı yüzeylerinin belirlenmesi ve zafiyetlerin tespit edilmesi açısından kritik öneme sahiptir.

Güvenli Kod Geliştirme Pratikleri: Örneğin, giriş doğrulaması, şifreleme, hata yönetimi ve güvenlik güncellemeleri gibi konular bu pratikler arasındadır.

Kod Gözden Geçirme ve Test: Yazılımın güvenlik açıklarını tespit etmek ve gidermek için yapılan bir inceleme sürecidir. Ayrıca, güvenlik testleri (penetrasyon testleri, statik analiz, dinamik analiz) de güvenliğin sağlanmasında önemli rol oynar.

- ***Banka Uygulamalarında Kullanılan Güvenlik Teknolojileri***

Şifreleme: Verilerin yetkisiz kişiler tarafından okunamamasını sağlar. Banka uygulamalarında hem veri aktarımı sırasında (TLS/SSL) hem de veri depolama sırasında (AES, RSA) şifreleme teknikleri kullanılmalıdır.

Çok Faktörlü Kimlik Doğrulama (MFA): Kullanıcıların kimlik doğrulama sürecini zorlaştırarak güvenliğini artırır. Parola ve SMS doğrulaması gibi birden fazla doğrulama yöntemi kullanarak yetkisiz erişimlerin önüne geçilir.

- ***Banka Uygulamalarında Güvenlik Zafiyetleri ve Çözümleri***

XSS (Cross-Site Scripting): XSS bir saldırı türüdür. XSS saldırıları, saldırganların web uygulamalarına zararlı kod yerleştirerek kullanıcıların tarayıcılarında çalıştırmasına olanak tanır. Bu tür saldırıları önlemek için kullanıcı girdilerinin doğrulanması ve kodların filtrelenmesi gereklidir.

SQL Enjeksiyonu: Saldırganların veritabanına zararlı SQL kodları enjekte ederek veri çalmasına veya manipüle etmesine olanak tanır. Bu tür saldırıları önlemek için parametreli sorgular ve ORM araçları kullanılmalıdır.

CSRF (Cross-Site Request Forgery): CSRF saldırıları, kullanıcıların bilgisi dışında zararlı isteklerin yapılmasına neden olabilir. Bu saldırıları önlemek için CSRF tokenları ve kullanıcı doğrulaması kullanılmalıdır.

- ***Sonuç:***

Banka uygulamalarında güvenli yazılım tasarımı, kullanıcı verilerinin ve işlemlerinin korunması açısından kritik öneme sahiptir. Güvenlik prensiplerinin benimsenmesi, güvenli yazılım tasarımı yöntemlerinin uygulanması ve güvenlik teknolojilerinin entegrasyonu, banka uygulamalarının güvenliğini sağlamak için gerekli adımlardır.

Uygulamada kullanılan dil, kütüphaneler ve methodlar ile ilgili bilgiler README dosyasına eklenmiştir.

GitHub Project Repository: PEKTASCH/Software-Engineering: Yazılım Mühendisliği Proje Dosyaları (github.com) (https://github.com/PEKTASCH/Software-Engineering)

- ***Kaynak:***

Anderson, R. (2001). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.

OWASP. (2021). OWASP Top Ten. Retrieved from https://owasp.org/www-project-top-ten/

https://medium.com/albaraka-tech-global/rsa-ile-encryption-decryption-i%CC%87%C5%9Flemleri-5fa70d15f3e6

https://feyzatopcu.medium.com/rsa-%C5%9Fi%CC%87freleme-algori%CC%87tmasi-78347f748ed2

https://www.clickssl.net/blog/what-is-rsa

https://laccart.medium.com/g%C3%BCvenli-yaz%C4%B1l%C4%B1m-geli%C5%9Ftirme-c9f75d12a46f

https://cahitcengizhan.com/banka-yazilimlari-ve-guvenligi/

https://www.linkedin.com/learning/csslp-cert-prep-3-secure-software-design/traditional-security-architectures?resume=false

www.mirlabs.net/jias/index.html

https://gokhana.medium.com/microservice-mimarisi-nedir-microservice-mimarisine-giri%C5%9F-948e30cf65b1

https://www.hosting.com.tr/blog/mikroservis-mimarisi/

https://www.linkedin.com/pulse/tehdit-modelleme-ara%C3%A7lar%C4%B1-murat-demircioglu-phd-cd0zc/

Gemini

ChatGPT