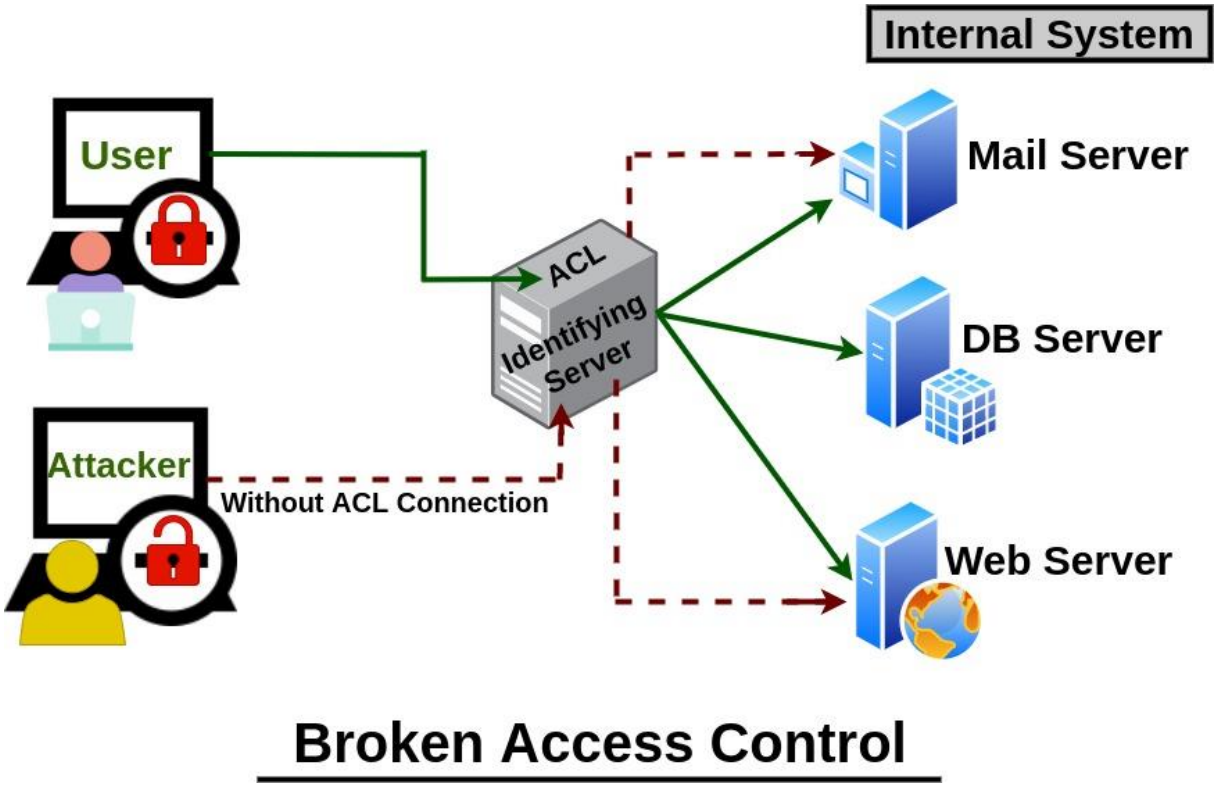
OWASP Top 10 Raporu

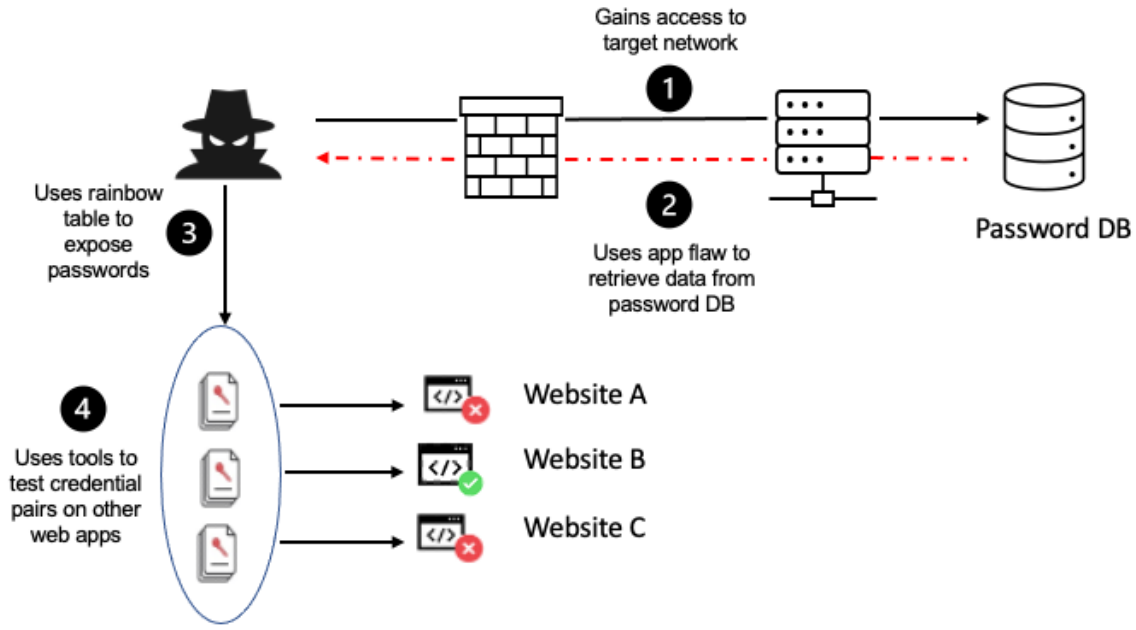
Broken Access Control

- **Zafiyet Nedir:** Kullanıcıların yetkileri dışında işlemler yapabilmesine sebep olan bir güvenlik açığıdır.
- **Neden Kaynaklanır:** Eksik veya yanlış kodlanmış erişim ve denetim mekanizmalarından kaynaklanır.
- **Türleri:**
    - Yetkisiz Dosya Erişimi
    - Yetkisiz API Erişimi
    - Yetkisiz Veri Değiştirme
- **Nasıl Önlenir:** Erişim kontrolünü doğru yapılandırmak, test etmek ve düzenli olarak denetlemekle önlenebilir.



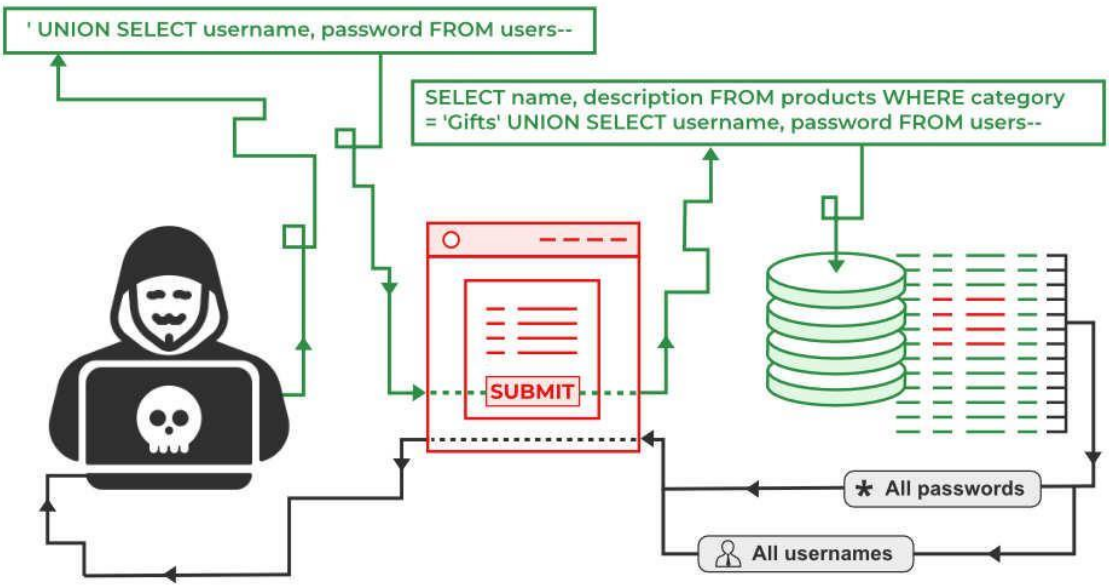
Cryptographic Failures (Eski adıyla Sensitive Data Exposure)

- **Zafiyet Nedir:** Gizli verilerin düzgün korunmaması durumudur.
- **Neden Kaynaklanır:** Zayıf şifreleme algoritmaları veya eksik şifreleme kuralları nedeniyle ortaya çıkar.
- **Türleri:**
    - Yetersiz Şifreleme
    - Güvensiz Şifreleme Anahtarı Yönetimi
- **Nasıl Önlenir:** Güçlü şifreleme standartlarının kullanılması, şifreleme anahtarlarının güvenli bir şekilde yönetilmesiyle önlenebilir.



Injection

- **Zafiyet Nedir:** Zararlı input verilerinin uygulama tarafından işlenerek istenmeyen komutların çalıştırılmasıdır.
- **Neden Kaynaklanır:** Kullanıcı girişlerinin yeterince doğrulanmaması veya filtrelenmemesi durumunda oluşur.
- **Türleri:**
    - SQL Injection
    - Command Injection
    - LDAP Injection
    - HTML Injection
- **Nasıl Önlenir:** Kullanıcı girişlerinin doğrulanması, hazırlıklı ifadelerin kullanılması, parametreli sorgular ve girişlerin doğru bir şekilde filtrelenmesiyle önlenebilir.z



Insecure Design

- **Zafiyet Nedir:** Güvenlik önlemlerinin tasarım aşamasında dikkate alınmaması durumudur.
- **Neden Kaynaklanır:** Uygulamanın geliştirilme sürecinde güvenlik tasarım ilkelerine uyulmaması sebebiyle ortaya çıkar.
- **Nasıl Önlenir:** Güvenli yazılım geliştirme yaşam döngüsünün (SDLC) uygulanması, güvenlik tasarım incelemelerinin yapılmasıyla önlenebilir.

Security Misconfiguration

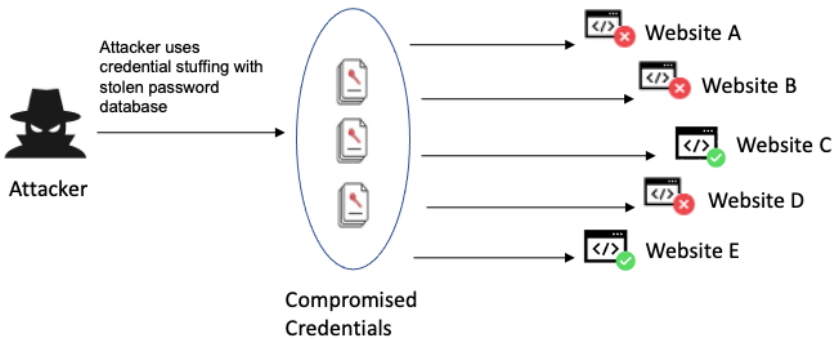
- **Zafiyet Nedir:** Yanlış yapılandırma veya eksik güvenlik önlemleri nedeniyle sistemlerin savunmasız kalmasıdır.
- **Neden Kaynaklanır:** Yanlış yapılandırılmış sunucular, hatalı dosya izinleri, varsayılan şifrelerin değiştirilmemesi gibi nedenlerden kaynaklanır.
- **Nasıl Önlenir:** Sistemlerin doğru yapılandırılması, gereksiz özelliklerin devre dışı bırakılması ve varsayılan ayarların değiştirilmesiyle önlenebilir.

Vulnerable and Outdated Components

- **Zafiyet Nedir:** Eski veya güvenlik açıkları bulunan yazılım bileşenlerinin kullanılmasıdır.
- **Neden Kaynaklanır:** Uygulamaların eski sürümlerinin kullanılması veya güncellemelerin yapılmaması nedeniyle oluşur.
- **Nasıl Önlenir:** Yazılım bileşenlerinin güncel tutulması, düzenli olarak zafiyet taraması yapılmasıyla önlenebilir.

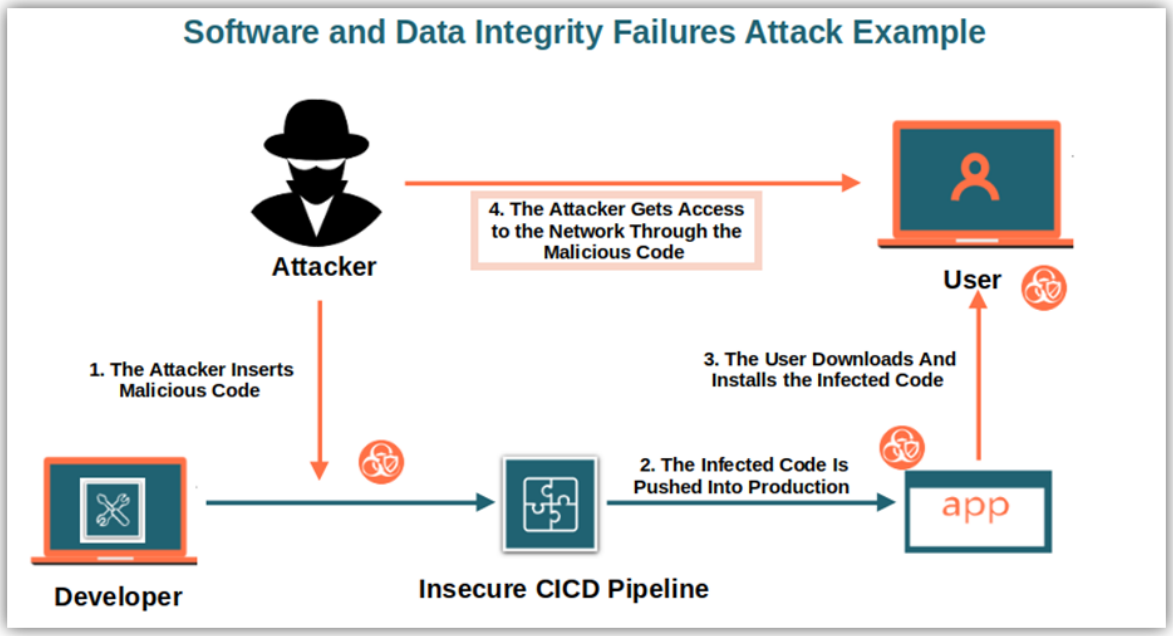
Identification and Authentication Failures

- **Zafiyet Nedir:** Kimlik doğrulama mekanizmalarının zayıf olması veya eksik olmasıdır.
- **Neden Kaynaklanır:** Güvensiz parola politikaları, çok faktörlü kimlik doğrulamanın olmaması gibi nedenlerle oluşur.
- **Nasıl Önlenir:** Güçlü parola politikalarının uygulanması, çok faktörlü kimlik doğrulamanın etkinleştirilmesiyle önlenebilir.



Software and Data Integrity Failures

- **Zafiyet Nedir:** Yazılım ve verilerin bütünlüğünün sağlanamaması durumudur.
- **Neden Kaynaklanır:** Yazılım güncellemelerinin doğrulanmaması, verilerin bütünlüğünün kontrol edilmemesi gibi nedenlerden kaynaklanır.
- **Nasıl Önlenir:** Dijital imza kullanımı, yazılım ve veri bütünlüğünün düzenli olarak kontrol edilmesiyle önlenebilir.



Security Logging and Monitoring Failures

- **Zafiyet Nedir:** Güvenlik olaylarının yeterince izlenmemesi veya kayıt altına alınmamasıdır.
- **Neden Kaynaklanır:** Yetersiz veya eksik loglama ve izleme mekanizmaları nedeniyle oluşur.
- **Nasıl Önlenir:** Etkili loglama ve izleme sistemlerinin kurulması, düzenli olarak gözden geçirilmesiyle önlenebilir.

Server-Side Request Forgery (SSRF)

- **Zafiyet Nedir:** Uygulamanın, kullanıcı tarafından kontrol edilen URL'lere istek göndermesi ve bu isteklerin kötüye kullanılmasıdır.
- **Neden Kaynaklanır:** Uygulamanın dış istekleri kontrolsüz bir şekilde kabul etmesi nedeniyle oluşur.
- **Nasıl Önlenir:** Kullanıcı tarafından gönderilen URL'lerin doğrulanması, erişim kontrolü uygulanmasıyla önlenebilir.