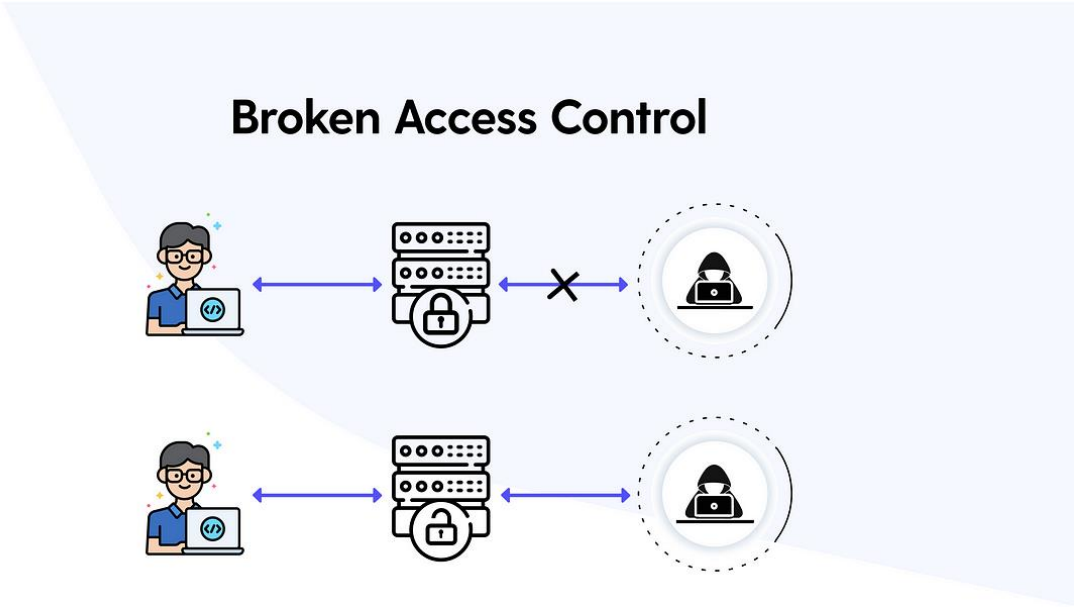
OWASP TOP 10

Broken Access Control :

Broken access control, web uygulamalarında bulunan yanlış yapılanma ve erişim ayarlarından dolayı oluşan çok ciddi bir açıktır.Bu zafiyet sayesinde yetkisiz kullanıcılar yetkisi dışında bulunan kaynaklara erişim sağlayabilmekte ve kendi yetkilerini yükseltebilmektedir.



Broken access control türleri:

Dikey yetki yükseltme:

Saldırganın düşük yetki seviyesinden yüksek yetki(administrator/root) seviyesine çıkmasıdır.

Yatay yetki yükseltme:

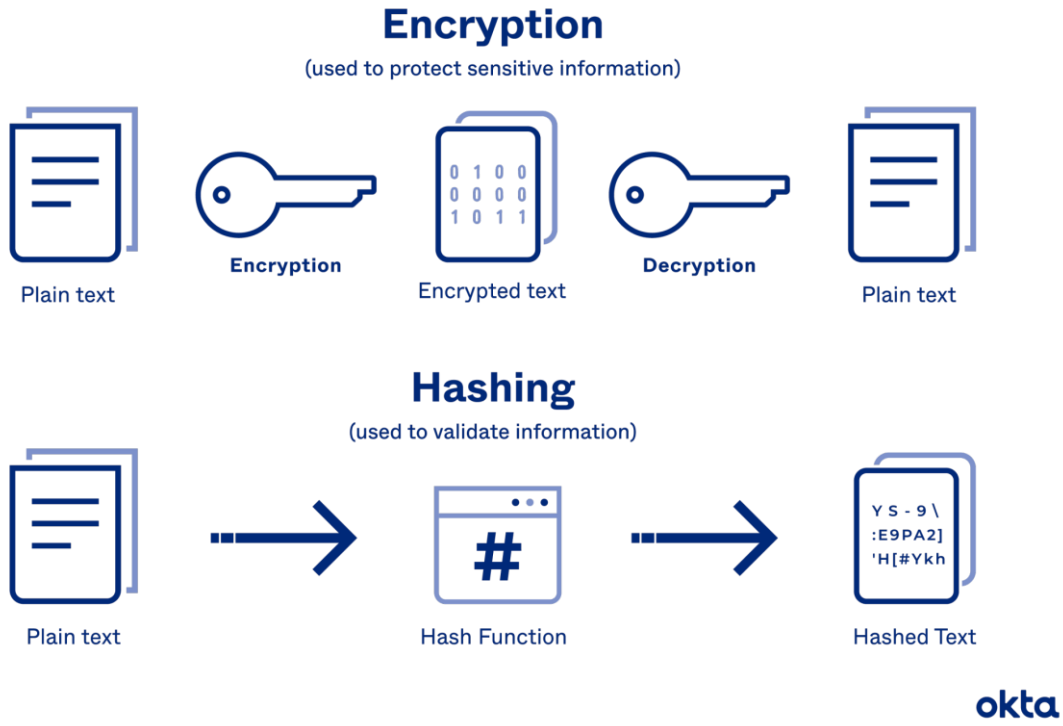
Saldırganın bulduğu yetki seviyesiyle aynı yetki seviyesine sahip kullanıcılar arasında geçiş yapmasıdır.

Nasıl Engellenir:

- Güçlü kimlik bilgileri ve parolalar kullanılmalıdır.
- Kullanıcı yetkileri mümkün olan en düşük düzeyte tutulmalıdır.
- Yanlış yapılandırma ve güvenlik açıkları kontrol edilmelidir.

Cryptographic Failures :

Zamanı geçmiş , açığa çıkmış ve geçerlilğini yitirmiş algoritmalarla şifrelenmiş metinlerin şifresinin kırılmasıyla veri gizliliğini ihlal eden zafiyettir.



Nasıl Engellenir:

- Güçlü şifreleme algoritmalari kullanılmalıdır.
- Veri iletiminde kullanılan protokollerin yükseltilmiş hali kullanılmalıdır.(http->https)
- Anahtar kullanımlarına dikkat edilmelidir.

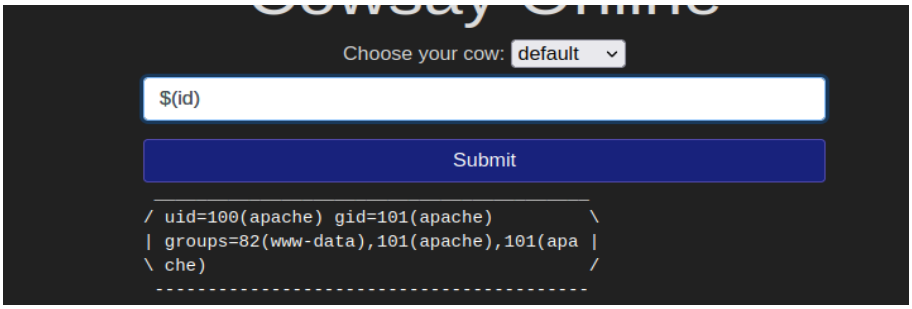
Injection:

kullanıcıdan girilen veriler sonucu oluşan bir zafiyettir. Kullanıcıdan alınan veriler filitrelenmez veya doğrulanmazsa oluşur.

Injection Türleri:

Command Injection:

Saldırgan kullanıcı tarafından girilen kod sunucuda uygulama yetileriyle çalıştırılır.



SQL Injection:

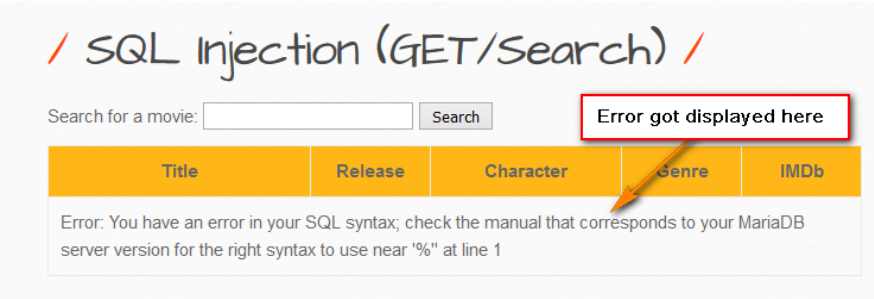
Kullanıcı tarafından girilen SQL sorgularının web uygulaması tarafından çalıştırılması sonucu oluşan zafiyetlerdir.En basit fakat en çok bulunan injection türleridir.

In-Band SQL Injection:

sorguların ve sonuçların aynı yerde göründüğü sql injection türüdür. 2 ye ayrılır

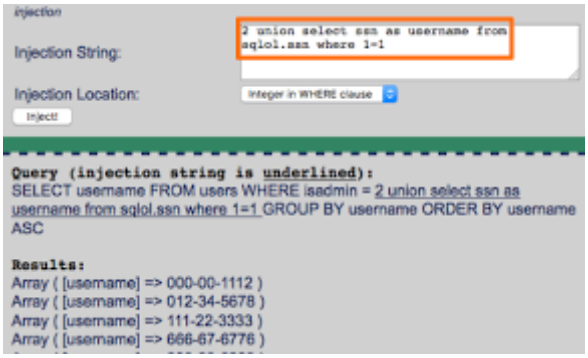
Error-Based :

Gönderilen sorgunun databasede hata oluşturumasıyla bulunan ve dönen mesaja göre sömürülen injection türüdür.



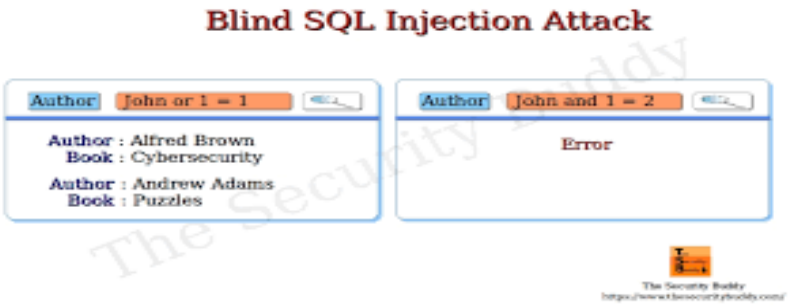
Union-Based:

Union ve select sorguları kullanılarak veritabanından bilgi ve veri elde edilmesidir.



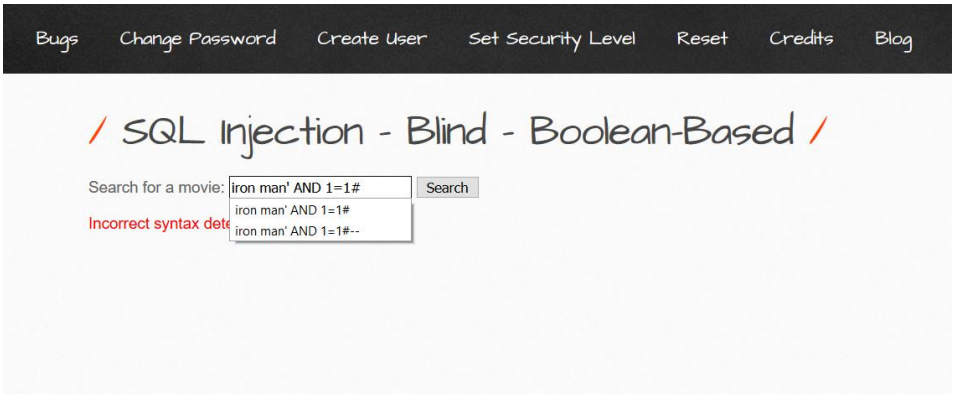
Blind SQL injection:

Herhangi bir sonuç görünmemesine rağmen web uygulamasının davranışları gözetilerek ve sürekli payloadlar denenerek database'in içeriği öğrenilmeye çalışılır.



Boolean-based SQL injection:

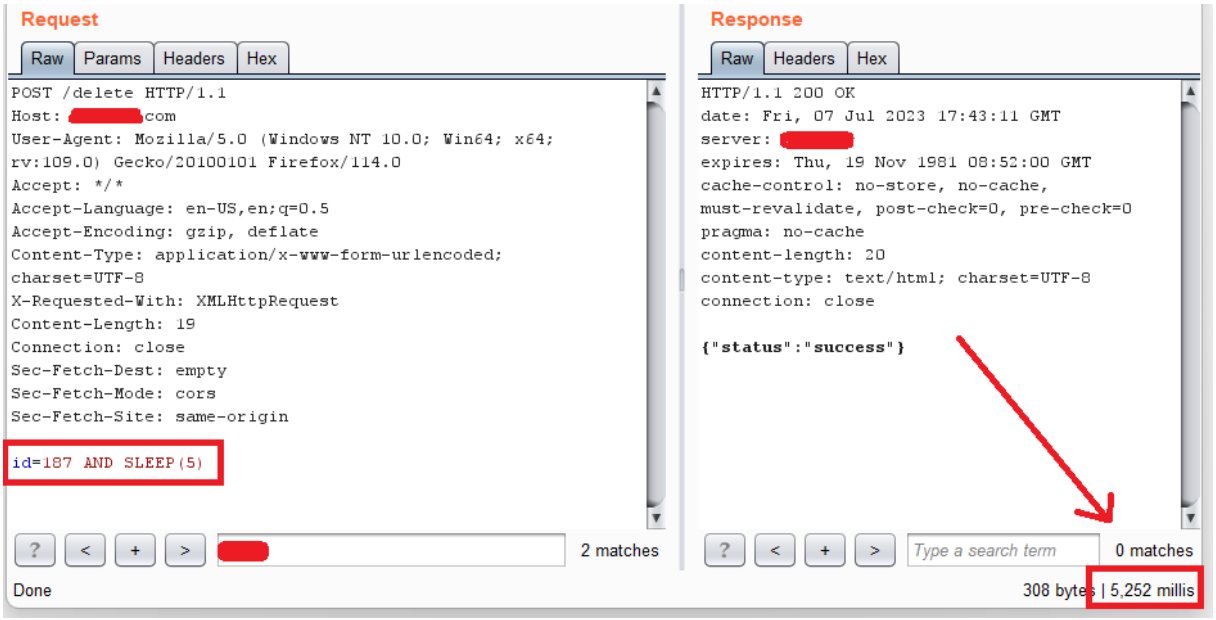
Bu injection türünde saldırgan database'e değişik sorgular yollayarak aldığı True ve False cevaplar sayesinde database'i anlamaya çalışır.



Time-Based SQL injection:

Saldırganın gönderdiği sorgunun True ve False olması sonucu database'i bekleme işlemine sokmasıdır.

Database'in verdiği tepkiye dayanarak Database'i anlamaya çalışır.

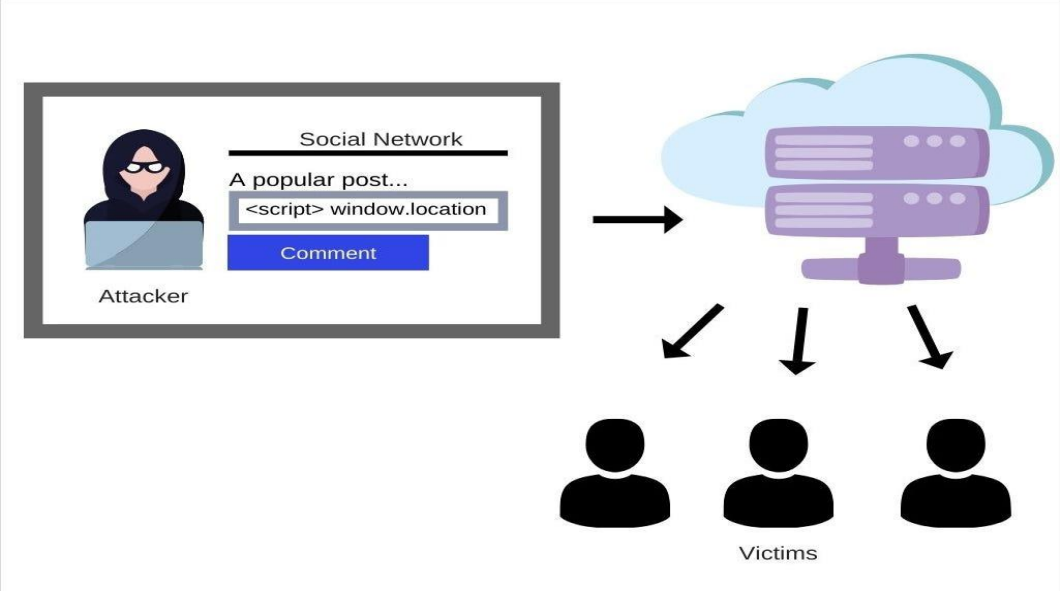


CROSS-SİTE SCRİPTİNG (XSS)

Siteler arası komut dosyası çalıştırma saldırısı , kullanıcı yorum kuturları,giriş formları ,arama kutuları vb. girdi formları aracılığıyla kötü huylu kod enjekte eder. Diğer injection yöntemlerinden farklı olarak web uygulamasını hedef almaz kullanıcıyı hedef alır**.**

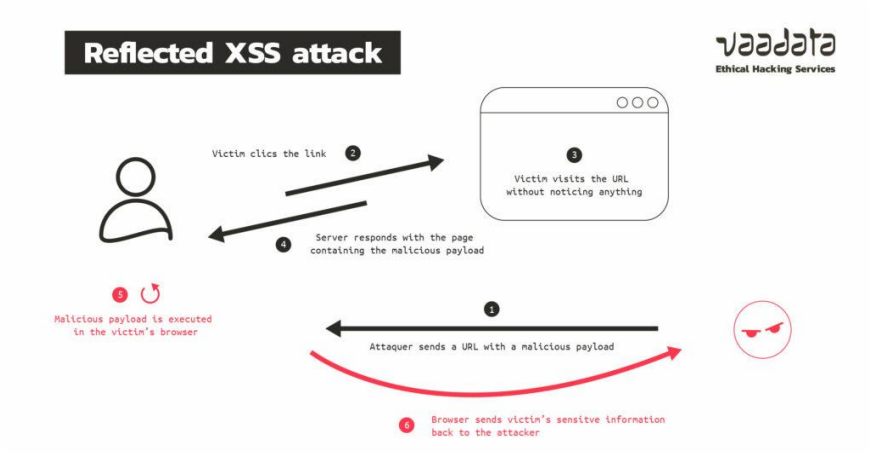
Stored-XSS:

Saldırgan tarafından enjekte edilen payload databasede kaydedilerek web uygulaması her açılıdığında çalışır.



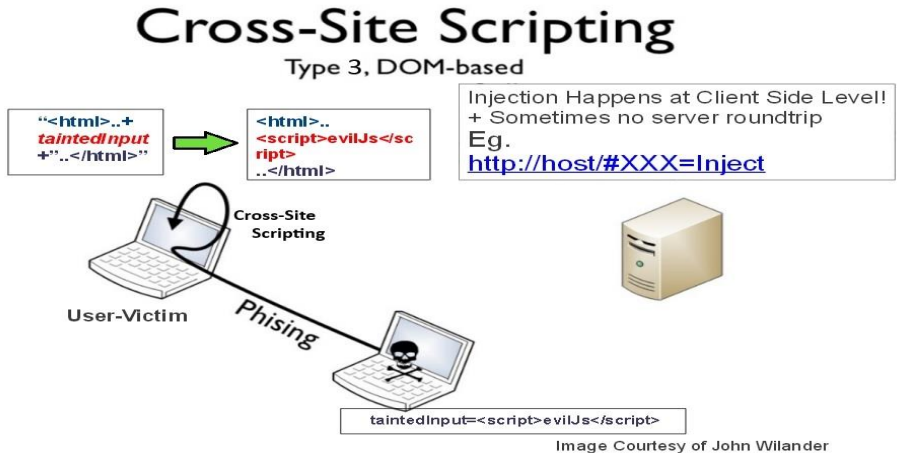
Reflected-XSS:

Saldırgan payload'ı veritabanına kaydetmez bunun yerine bir http isteğine enjekte ederek bir kullanıcıyı hedef alır.



Dom-XSS:

Saldırgan DOM modelini manipüle ederek bu saldırıyı gerçekleştirir. URL bağlantısına enjecte edilen paload URL e tıklandığında çalışır ve kullanıcının DOM'ını değiştirerek arka planda kotü amaçlı kodlarını çalıştırır.

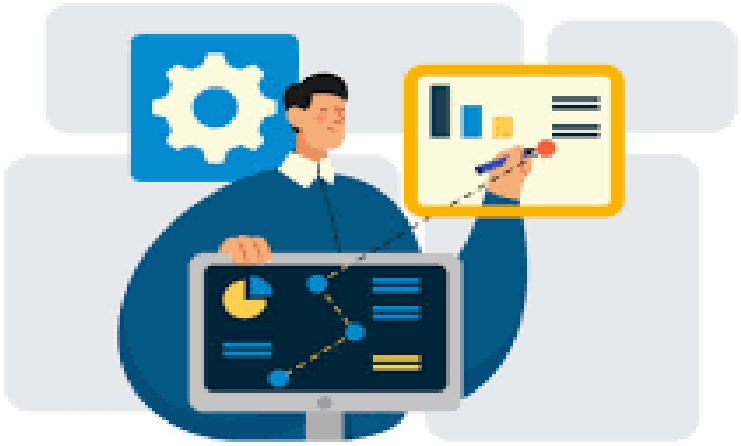


Nasıl Engellenir:

- White list ,black list oluşturulabilir.
- Bağımlılıkların güncelliği kontrol edilir.
- Veritabanı izni ve ayrıcalıkları kontrol edilir.

Insecure Design

Bu zafiyet web uygulamasının tasarımı ve mimarisindeki kusurlardan dolayı oluşur. Bu zafiyetin giderilmesi çok zordur.Bu zafiyet saldırganın web uygulamasının veri giziliğini , bütlüğünü,yetkisiz erişimini ve kimlik doğrulamasını etkiledği bir zafiyettir.

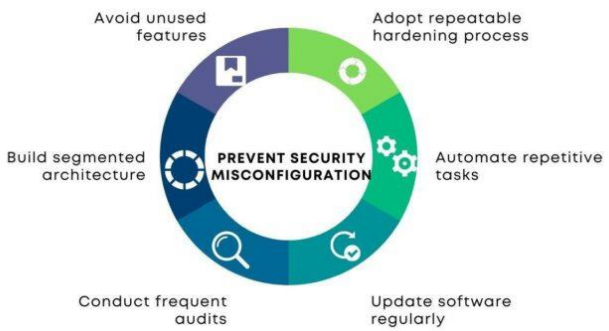


Nasıl Engellenir:

- Tasarım yapılırken uygulama güvenliğinde uzman kişilere başvurulmalıdır.
- Tehdit modelleme yapılabilir.
- Kullanıcı veya hizmet kaynak tüketimi ihtiyaç duyulan sevide tutulmalıdır.
- Oluşan güvenlik açıkları araştırılıp düzeltilmelidir.

Security Misconfiguration

Bir yazılım uygulamasının güvenliğini sağlamak için yazılım bileşenlerinin güvenli bir şekilde yapılanması gerekir. Default olarak yapılandırılan yazılım bileşenleri önemli güvenlik açıkları ortaya çıkarır.



SECURITY MISCONFIGURATION: PREVENTION

Nasıl Engellenir:

- Yazılım bileşenleri yapılandırılırken varsayılan ayarlar değiştirilebilir.
- Hizmetlerin güncelliği kontrol edilmelidir.
- Kullanılmayan özellikler,bileşenler ve hizmetler kaldırılmalıdır.

Vulnerable and Outdated Components

Zafiyeti açığa çıkmış ve desteklenmeyen yazılımlar sonucu ortaya çıkar . Bu zafiyet çok kritiktir saldırganın terminal elde etmesine kadar gidebilir.

Nasıl Engellenir:

- Yazılım bileşenlerinin sürüm güncellemeleri yapılmalıdır.
- Desteklenmeyen yazılımlar değiştirilmelidir .
- CVE gibi zafiyet paylaşılan siteler takip edilmelidir.
- Kullanılmayan yazılım ürünleri veya programlar kaldırılmalıdır.

Identification and Authentication Failures

Bu zafiyet kullanıcıların kimlik doğrulamaları ve yetkilendirilmelerinin doğru yapılamaması sonucu oluşur. Zayıf parolalar, Brute-Force saldırıları , Kimlik doğrulama yapılmaması ve MFA kullanılmaması bu zafiyeti sağlayabilir. Saldırganlar bu zafiyet sayesinde sistemlere ve verilere yetkisiz erişebilir.

Nasıl Engellenir:

- Kimlik doğrulama faktörleri kullanılabilir.
- Güçlü şifre politikaları kullanılmalıdır.
- Captcha kullanılabilir.
- Başarısız oturum açma girişimlerinin sayısı kısıtlanabilir.

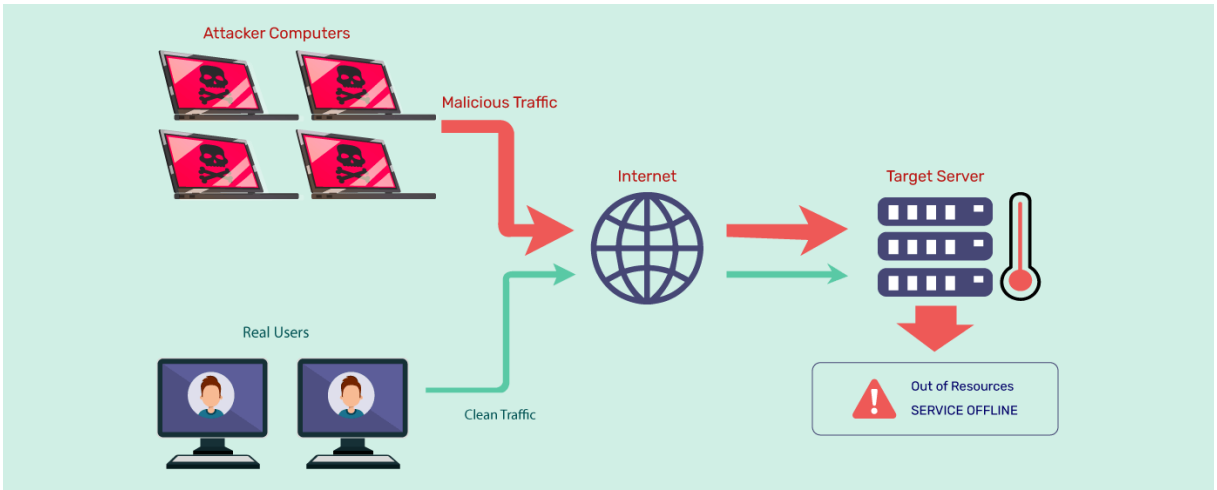
Software and Data Integrity Failures

Bu zafiyet türü veririn yetkisiz bir şekilde değiştirilmesi sonucu oluşur. Saldırgan bu zafiyetde yazılım ve veri bütünlüğü ihlali yapar , bu sayede sistem üzerinde yetki sahibi olur .

Software and Data Integrity Failures türleri:

DOS Saldırıları:

Saldırganın internet ortamından ele geçirdiği makinler yani zombi makineler tarafından sistem kaynaklarını aşırı yükleme sonucu sistemin hizmet verememesi ,kullanıcıların sisteme erşimini engelleme şekilinde gerçekleşen saldırı türürüdür.

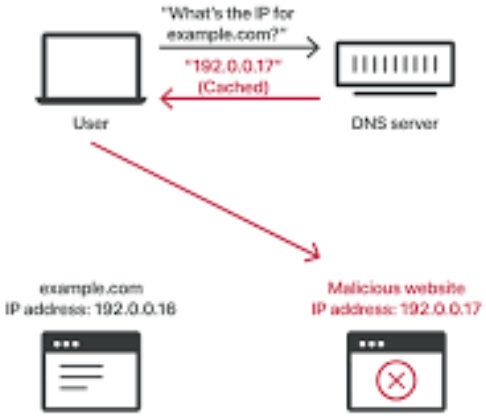


Code Execution:

Saldırganın özel veya genel ağ üzerinden bir makine üzerinde rastgele kod yürütmesidir.

Cache poisoning:

Web önbelleklerinde değişiklik yapılarak kod yürütülmesidir.



Nasıl Engellenir:

- Verilerin bütünlük kontrolleri yapılmalıdır.
- Erişim kontrolleri yapılmalıdır.
- Ağ güvenlik duvarları , WAF , Ağ taramaları yapılmalıdır.
- Kod ve Konfigürasyon kontrolleri yapılmalıdır.

Security Logging and Monitoring Failures

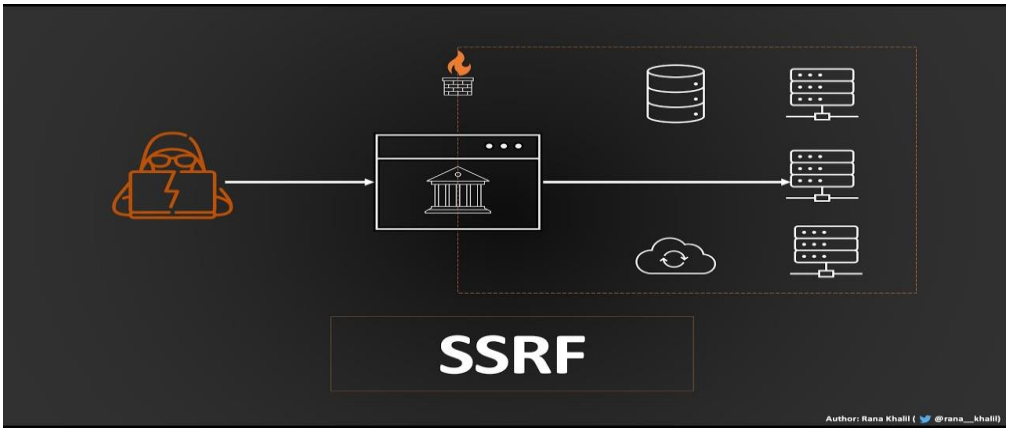
Loglama ve izleme sürecinin düzgün yapılmaması sonucu oluşan zafiyettir. Bu iki uygulama düzgün bir şekilde yapılırsa saldırganlar erken seviyede fark edilebilir.

Nasıl Engellenir:

- Düzenli penetration testing yapılmalıdır.
- Güvenlik prosedürleri düzenli olarak denetlenmelidir.
- Etkili izleme ve uyarı sistemleri oluşturulmalıdır.

Server-Side Request Forgery (SSRF)

Saldırgan zafiyetli bir web sunucusu üzerinden istediği sunucuya istek atabilmesini sağlayan zafiyettir. Saldırgan zafiyetli sunucu üzerindeki parametreleri değiştirip isteğin varış noktasını manipüle eder.



Nasıl Engellenir:

- Güvenlik duvarı kurulabilir.
- URL şeması güvenli olmalıdır.
- Tüm ağ akışının kaydı tutulmalıdır.