Mentör: Yusuf Nas

Öğrenci: Naci Balcı

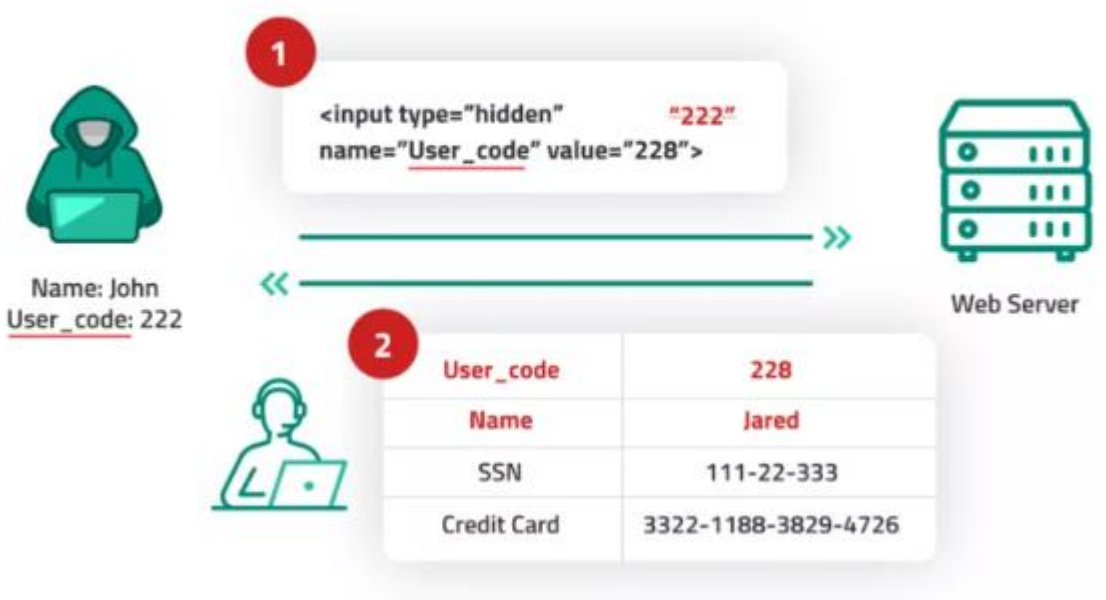
OWASP Top Ten

1-Broken Access Control (A01:2021):

Yetkisiz kullanıcılar veya yöneticiler, hassas verilere erişebilir ya da yönetici işlemleri gerçekleştirebilir. Sorunun nedeni yetkilerin kontrol edilmemesi veyahut yetkisiz şekilde erişimi olmaları.

Nasıl Önlenir?

1. **Kullanıcı rollerini ve yetkilerini doğru yapılandırıp bir sistem ile bunu denetlememiz gerekir.**
2. **Sunucu tarafından denetleme yapılabilir.**
3. **Kullanıcılara minimum yetki vermeye özen gösterilmelidir.**



2- Cryptographic Failures (A02:2021):

Zayıf veya yanlış uygulanmış şifreleme sonucunda veri güvenliğinin tehlikeye girmesi olarak adlandırılır.

Nasıl Önlenir?

1. **Güvenli şifreleme yöntemleri kullanılarak bunun en görünmez şekilde işlenmesi işlemlerin gerçekleşmesi gerekir.**

Mentör: Yusuf Nas

Öğrenci: Naci Balcı

3- Injection (A03:2021):

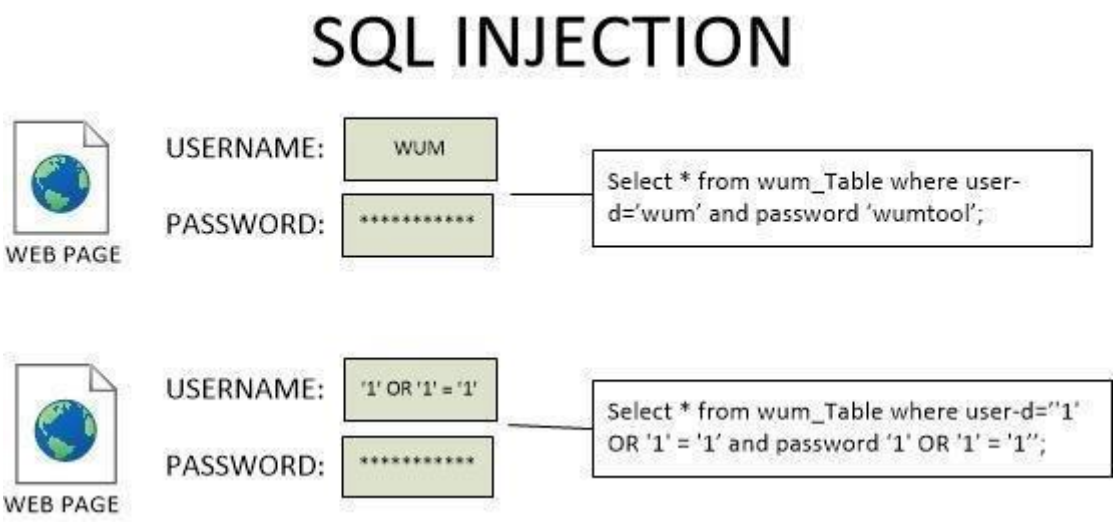
Kullanıcının inputları üzerinden zararları kodların inject edilmesiyle ortaya çıkar.

Türleri:

1. **SQL Injection (SQLi)**
2. **Cross-Site Scripting (XSS)**
3. **Command Injection**
4. **Css Injection**
5. **LDAP Injection**
6. **XML External Entity Injection (XXE)**
7. **NoSQL Injection**
8. **XPath Injection**

Nasıl Önlenir?

1. **Kullanıcıdan alınan verilerin denetlenip gerekli kontrollerden geçirildikten sonra iletilmesi gerekir.**

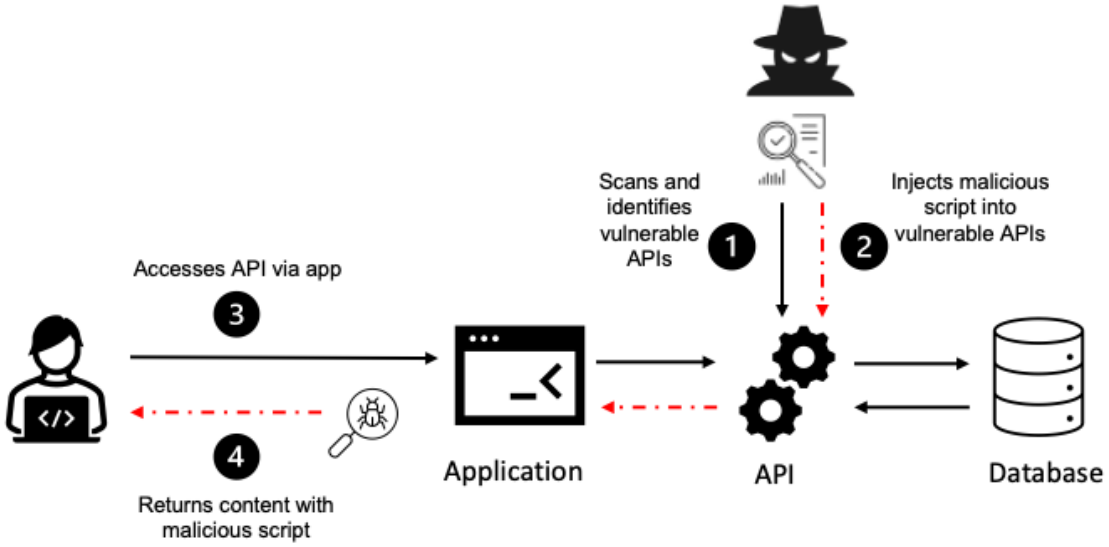


4- Insecure Design (A04:2021):

Güvenlik açısından zayıf mimari ve tasarım kararlarının verilmesi.

Nasıl Önlenir?

1. **Varsayılan Olarak Güvenli: Sistem, varsayılan olarak güvenli olacak şekilde tasarlanmalı; bu, yalnızca açıkça izin verilmiş olan işlemlere izin verilmesi gerektiği anlamına gelir.**
2. **Fail-Secure (Güvenli Hata Durumu): Bir hata meydana geldiğinde, sistemin güvenli bir duruma geçmesini sağlayın. Örneğin, kimlik doğrulama sisteminde hata oluşursa, erişimi engelleyin.**



5- Security Misconfiguration (A05:2021):

Yanlış yapılandırmalardan veya uygun olmayan güvenlik önlemlerinden kaynaklanan güvenlik açıkları.

Nasıl Önlenir?

1. **Tüm varsayılan kullanıcı adları ve şifreleri değiştirilmelidir.**
2. **Uygulamalar ve sistem bileşenleri, güvenli varsayılan ayarlarla kurulmalı ve çalıştırılmalıdır. Gerekmediğinde varsayılan özellikleri devre dışı bırakın.**

6- Vulnerable and Outdated Components (A06:2021):

Güncellemesi unutulmuş yanlış bileşenler kullanan yazılımın kullanılması.

Nasıl Önlenir?

1. **Yazılım bileşenlerinin desteklenen ve güncel sürümlerini kullandığınızdan emin olun. Sürüm kontrol araçlarını kullanarak güncellemeleri sağlayabiliriz.**
2. **Bileşenlerdeki güvenlik açıklarını tespit etmek için otomatik zafiyet tarama araçları kullanılabilir**

7- Identification and Authentication Failures (A07:2021):

Kimlik doğrulması ve oturum yönetim hataları olarak geçer.

Nasıl Önlenir?

1. **Kullanıcı parolalarının karmaşık, benzersiz ve güvenli olmasını sağlayın. Ayrıca, çok faktörlü kimlik doğrulama kullanarak, kimlik doğrulama sürecine ek güvenlik katmanı eklenmeli.**
2. **Oturumların güvenliğini sağlamak için kullanıcı oturumlarını etkili bir şekilde yöneterek, otomatik zaman aşımı ve tekrar oturum açmayı zorunlu kılın. Bu, özellikle hassas verilere erişim durumunda önemlidir.**
3. **OWASP yönergelerine uygun, güvenli kimlik doğrulama protokollerini ve kütüphanelerini kullanarak, yanlış yapılandırma ve hatalı kimlik doğrulama işlemlerinden kaynaklanan güvenlik açıklarını azaltın.**

8- Software and Data Integrity Failures (A08:2021):

Yazılım ve veri bütünlülüğü sorunu,güvenilmeyen kaynaklardan güncelleme almak.

Nasıl Önlenir?

1. **Yazılım ve verilerin bütünlüğünü korumak için dijital imzalar, hash fonksiyonları veya checksum yöntemleri kullanılmalı. Bu, kod veya veri değişikliklerinin yetkisiz bir şekilde yapılmasını önler ve olası manipülasyonları tespit etmeye yardımcı olur.**
2. **Yazılım güncellemelerini ve üçüncü taraf kütüphaneleri güvenilir ve resmi kaynaklardan indirilmesi gerekir.**

9- Security Logging and Monitoring Failures (A09:2021):

Güvenlik olaylarının tespit edilmesi ve izlenmesindeki eksiklikler.

Nasıl Önlenir?

1. **Sistem ve uygulama etkinliklerini kapsayan ayrıntılı loglar oluşturun. Kayıtlar, kimlik doğrulama hataları, erişim denemeleri, veri değişiklikleri gibi önemli olayları içermelidir. Bu loglar, güvenlik olaylarının hızlı bir şekilde tespit edilmesine ve analiz edilmesine yardımcı olur.**

10-Server-Side Request Forgery (SSRF) (A10:2021):

Sunucu tarafına müdahalede bulunup isteklerin manipüle edilmesi.

Nasıl Önlenir?

1. **Kullanıcı tarafından sağlanan URL ve diğer girişlerin titizlikle doğrulanması ve temizlenmesi, potansiyel zararlı isteklerin önlenmesine yardımcı olur.**
2. **SSRF saldırılarına karşı korunmak için sunucuya gelen ve sunucudan giden trafiği sınırlandırın.**
3. **Uygulamanın yalnızca güvenilir ve izin verilen URL'lere erişmesine izin verilmeli.**