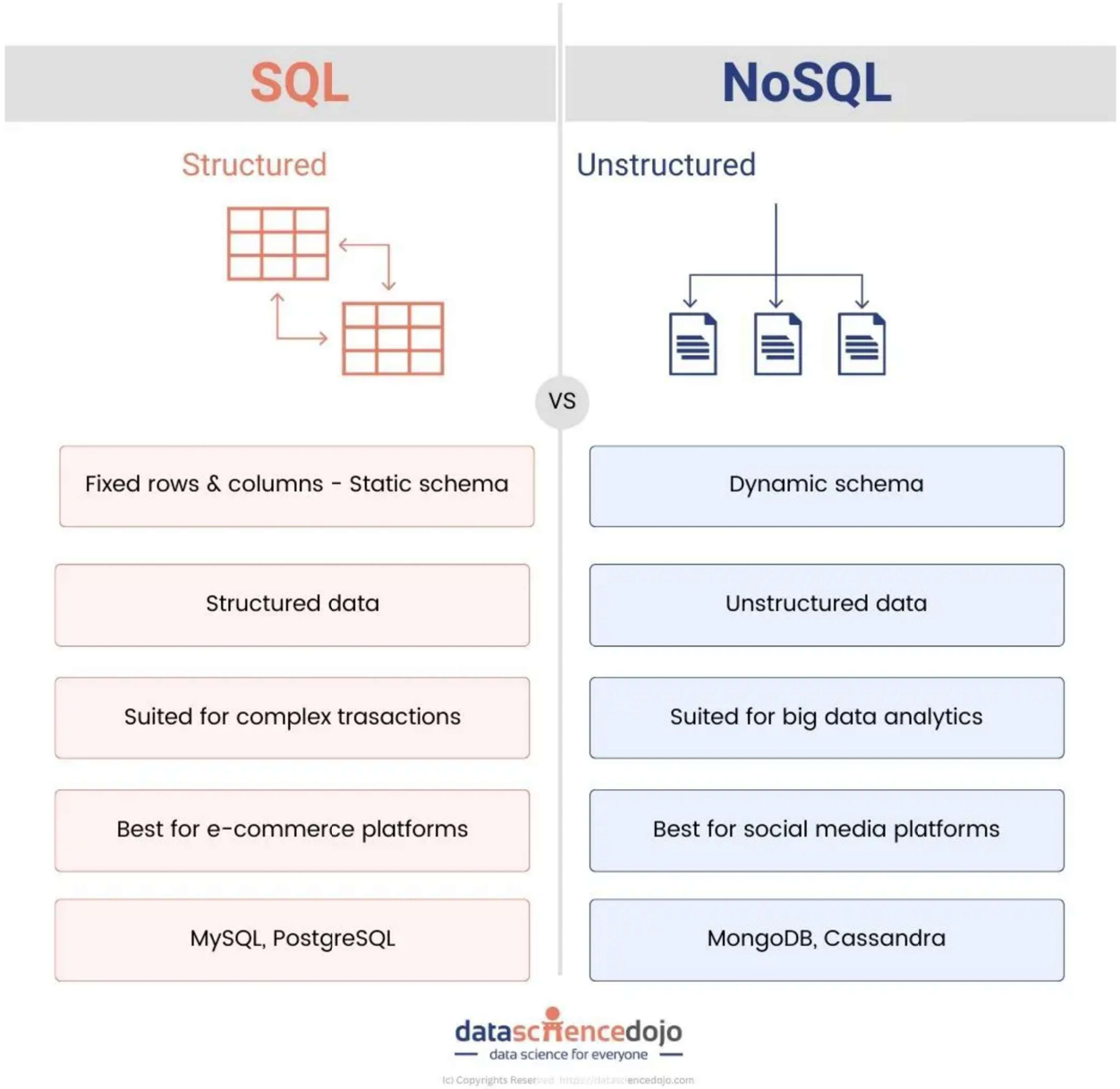
TURKISH TECHNOLOGY

NoSQL Injection

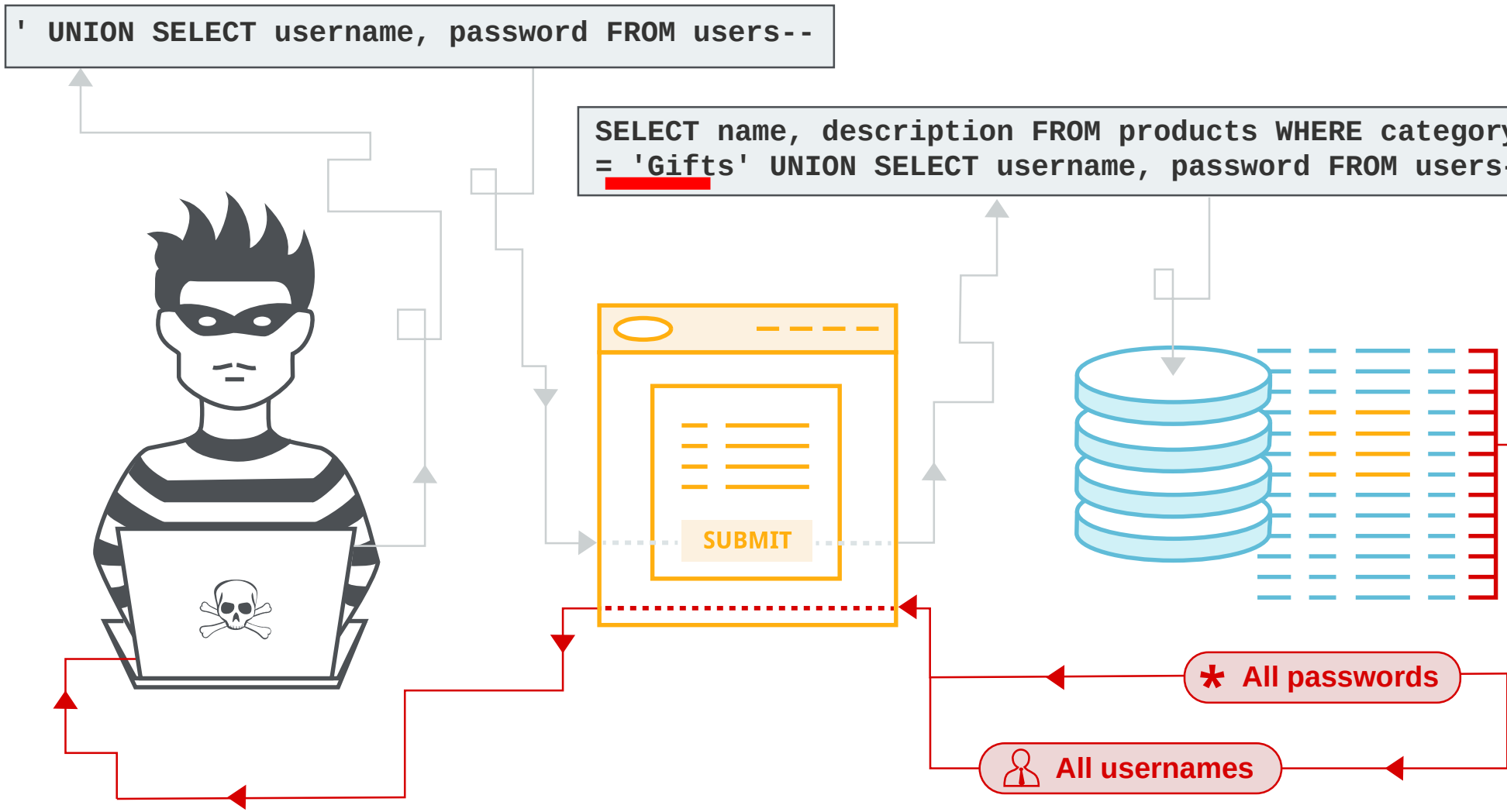
SQL ve NoSQL Nedir ?

- **SQL (Structured Query Language),** ilişkisel veritabanlarını yönetmek ve sorgulamak için kullanılan bir programlama dilidir.
- **NoSQL (Not Only SQL)**, ilişkisel olmayan veritabanlarını yönetmek için kullanılan, genellikle esnek şema yapısına sahip ve büyük ölçekli veri depolama için optimize edilmiş bir veri tabanı yaklaşımıdır.

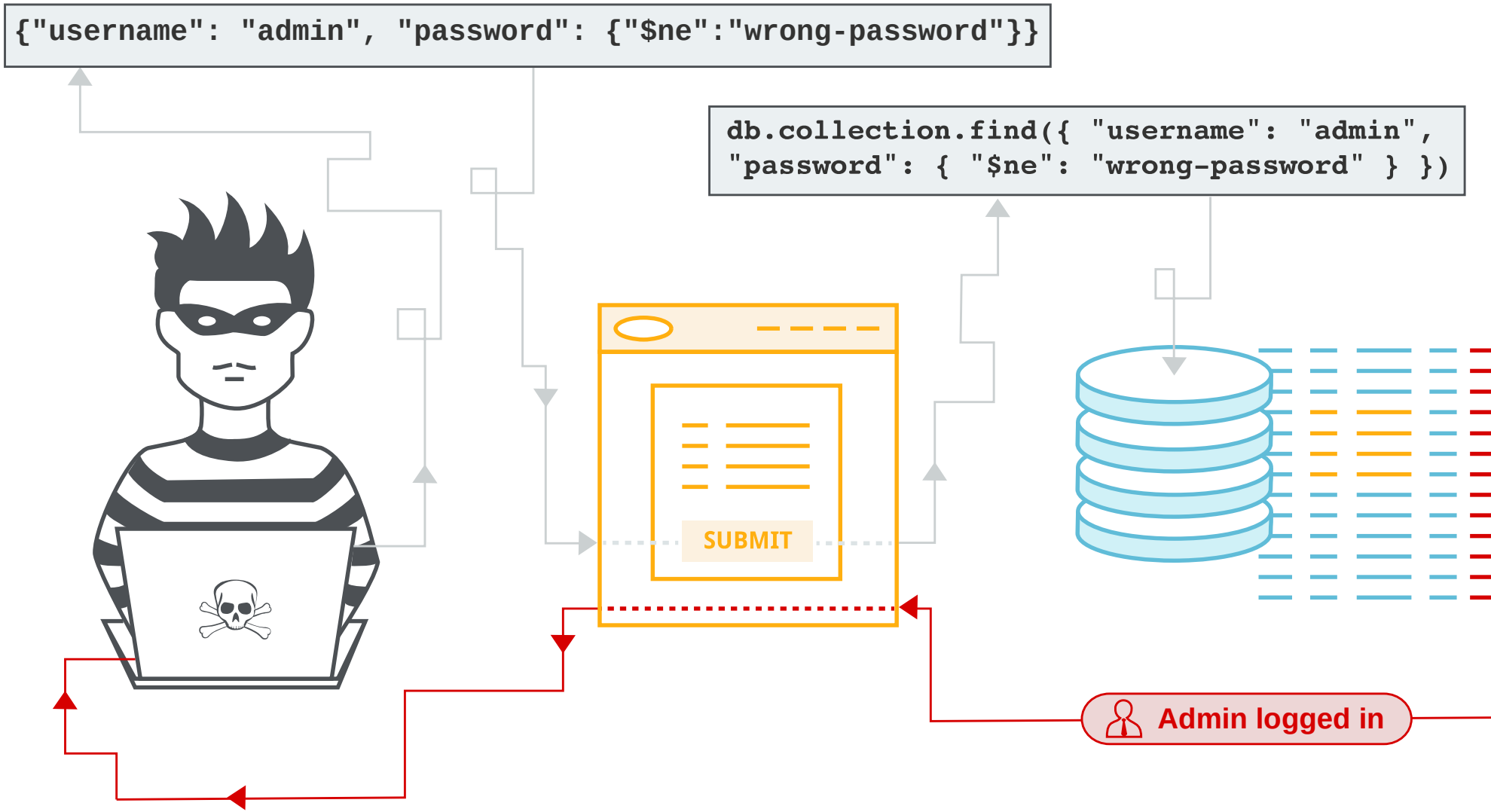
SQL vs NoSQL


SQL
NoSQL
Structured
Unstructured
VS
Fixed rows & columns - Static schema
Dynamic schema
Structured data
Unstructured data
Suited for complex trasactions
Suited for big data analytics
Best for e-commerce platforms
Best for social media platforms
MySQL, PostgreSQL
MongoDB, Cassandra
datasciencedojo
data science for everyone
(c) Copyrights Reserved. https://datasciencedojo.com

SQL Injection



NoSQL Injection



NoSQL Injection

- **Syntax Injection**, NoSQL sorgularının sözdizimini manipüle ederek beklenmeyen sorgular çalıştırmayı hedefleyen bir saldırıdır.

```
this.category == 'fizzy'
this.category == 'fizzy' || '1'=='1'
```

- **Operator Injection**, NoSQL sorgularında **$ne**, **$gt**, **$or** gibi operatörleri enjekte ederek doğrulama mekanizmalarını atlatmaya çalışan bir saldırı türüdür.

```
{"username":"admin","password":"peter"}
```

```
{"username":"admin", password": {"$ne":"invalid"} }
```

```
{"username": {"$in":["admin","administrator","superadmin"]} ,"password"
```

LABS

NoSQL Injection

https://portswigger.net/web-security/all-labs#nosql-in

NoSQL Injection Önleme

NoSQL teknolojisine göre değişse de genel olarak aşağıdaki önlemler alınabili

- Kullanıcı girdisi beyazliste yaklaşımı ile doğrulanıp, temizlenir.
- Kullanıcı girdisi direkt olarak concat yerine parameterize sorgular kullanılar eklenir.
- Operator injection'ı önlemek için beyazliste key değerleri oluşturulup kontr edilir.