

# SQL injection

Autor: Bruno Chenoll



# Qué es SQLi

Inyectar sentencias maliciosas a través de un campo de entrada para que se ejecuten en una base de datos



```
SELECT * FROM usuarios WHERE  
email='$mail' and password='$passwd'
```

## Típica consulta en php para consultar la base de datos

A menos que el contenido de \$mail o \$passwd esté hardcodeado en el código, necesitaremos pedírselo al usuario

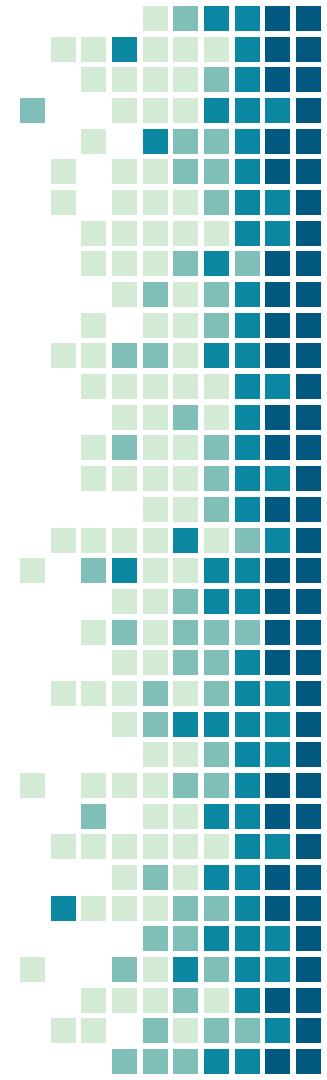
¿Puede meter cualquier cosa? Mientras pase nuestras comprobaciones de si es un email o si la contraseña tiene un mínimo de caracteres sí.



```
SELECT * FROM usuarios WHERE  
email='$mail' and password='$passwd'
```

**¿Qué sucede si introducimos un email y de contraseña "" or 1=1--"?**

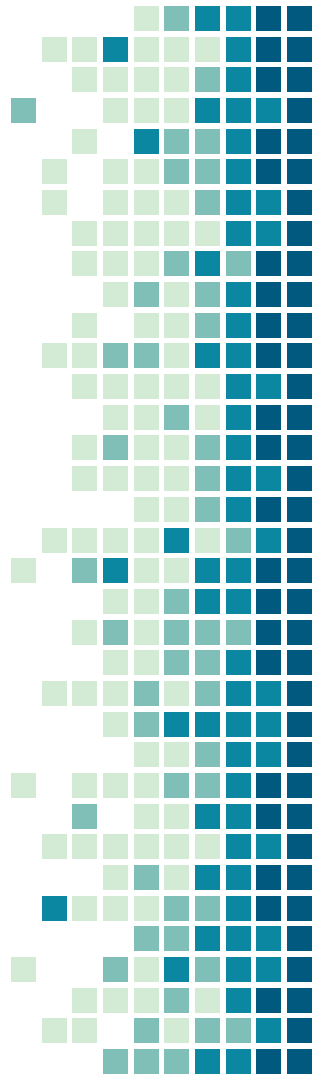
Nada bueno(o sí).



```
SELECT * FROM usuarios WHERE  
email='admin@ugr.es' and  
password="" or 1=1--'
```

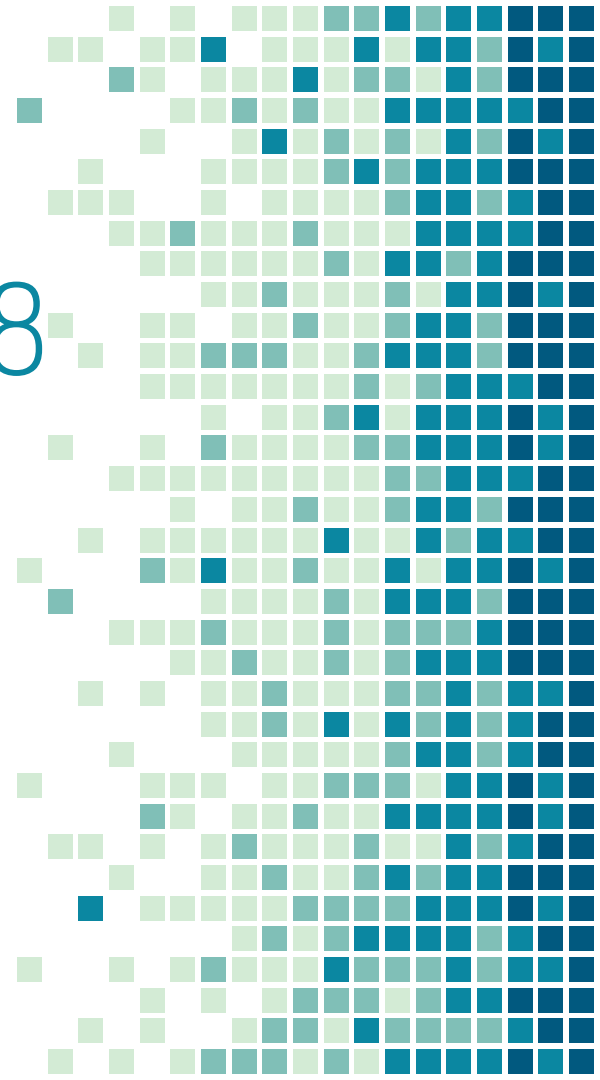
**Lógica ->  $x \text{ or TRUE} = \text{TRUE}$**

Podemos acceder a la cuenta de [admin@ugr.es](mailto:admin@ugr.es) sin necesidad de saber su contraseña



# Fallo descubierto en 1998

Tiene más de 20 años



# T10

## OWASP Top 10 Application Security Risks – 2017

### **A1:2017- Injection**

Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

### **A2:2017-Broken Authentication**

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

### **A3:2017- Sensitive Data Exposure**

Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

### **A4:2017-XML External Entities (XXE)**

Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

### **A5:2017-Broken Access Control**

Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

# ¿Cómo solucionarlo?

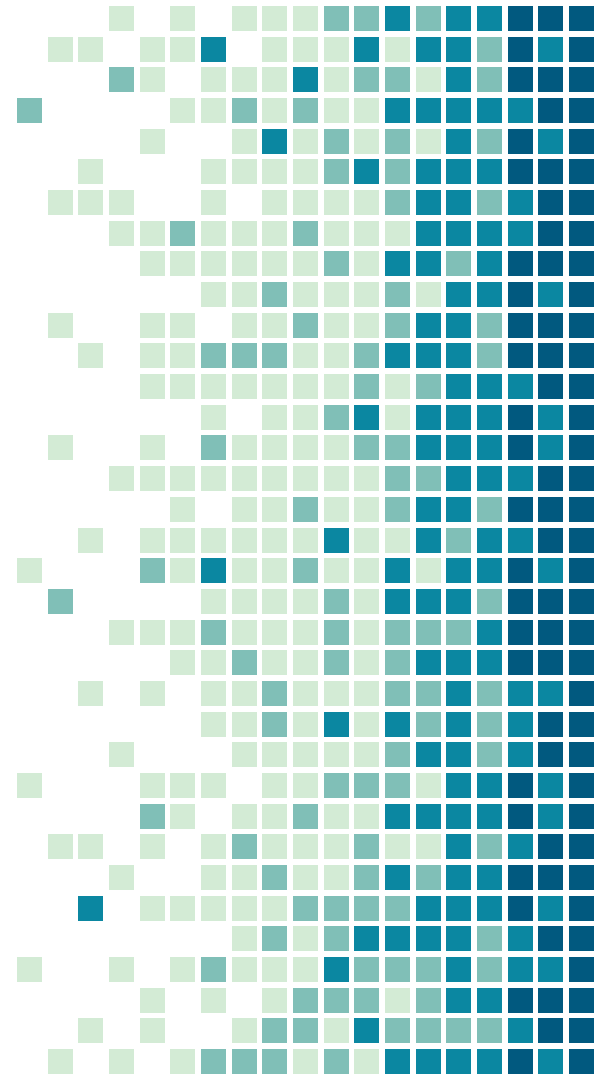
- Filtrando caracteres raros
- Escapando caracteres (\')
- Analizar entrada en busca de patrones de ataque
- Regular permisos





¿Es suficiente?

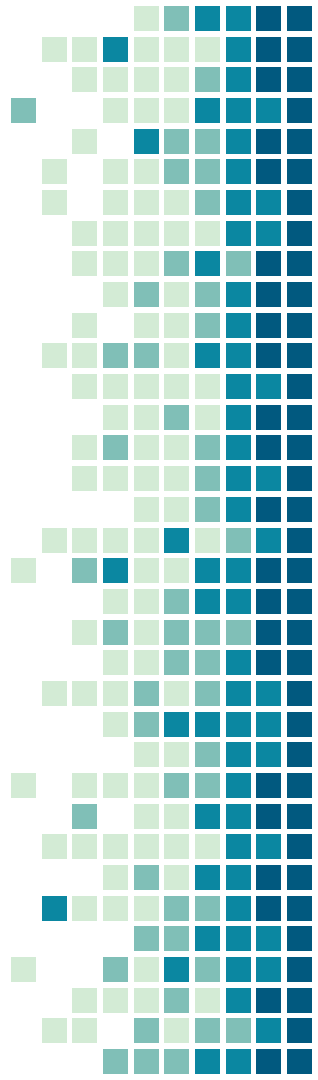




# ¿Qué problema puede haber entonces?

Imaginemos que tenemos una tienda en internet

Nos va bien y cada vez tenemos más productos y más categorías





**CATEGORÍAS** Ver todas >

Moda hombre

Moda mujer

Telefonía

Informática

Electrónica

Joyería y relojes

Casa y jardín

Bolsos y calzado

Mamá y bebé

Deportes y ocio

Salud y belleza

Motor

Bricolaje

**PLAZA, envíos desde España**

**Zona Marcas**

**Ofertas relámpago**

**Menos de \$5**

**LIVE**

**Estilo Invierno**

Vestidos

Chaquetas

Sudaderas

Suéteres

Cuero y Suede

Parkas

Parkas y plumas

Calcetines y Calcetería

**Lencería y Pijama**

Bras

Bragas

Pijama

Vestidos de noche



**Moda femenina**

Tops

Camisetas

Blusas y camisas

Monos

Trajes y blazers

**Pantalones y faldas**

Pantalones y Capris

Pantalones vaqueros

Leggings

Pantalones cortos

Faldas

Sujetador  
adhesivo



**Bodas y eventos**

Vestidos de novia

Vestidos dama de honor

Vestidos damita de honor

Vestidos de gala

Vestidos de cóctel

Complementos de boda

**Complementos**

Gafas de sol

Cinturones

Accesorios Para el cabello

Guantes y Mitones

Sombreros y Gorras

Bufandas



Simplee

HDY  
HAODUOYI

TWOTWINSTYLE

EVER♡PRETTY



DUCUI  
FASHION

AQFLY

IANOSI

MIEGOFCE

TOYOUTH

Miss and

WEmage

SheIn  
Show Out

gagaopt

Sisjuly

JAZZEPAR

ONLY

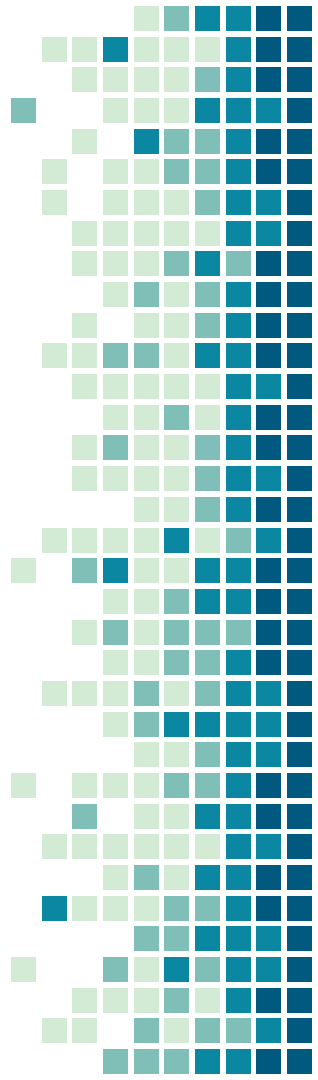
WESTLINK

32 queries diferentes sólo para acceder a una sección de mujer, hay 13 categorías por lo que podríamos estimar 416 accesos además del login

# Mucho que filtrar

Hay que pensar que cualquier fallo en el filtrado puede desencadenar en una desgracia

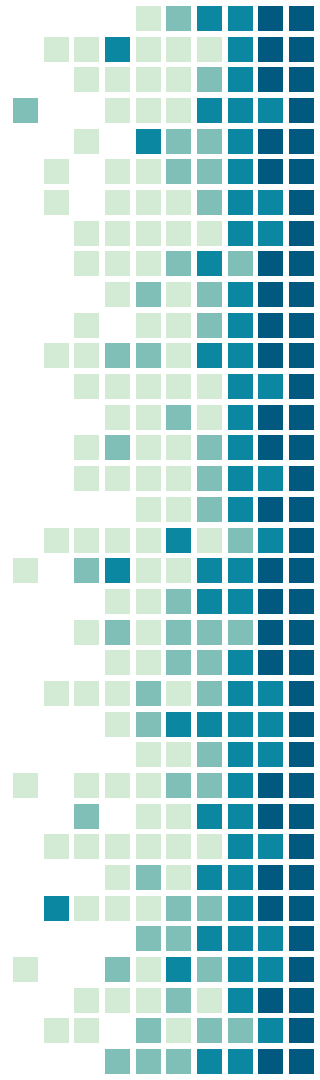
Además, si utilizamos cookies u otros métodos donde su contenido termine en una query, hay que filtrar



# Pero esto no acaba en el filtrado

En la vida real no trabajamos con una base de datos que hemos creado y tenemos acceso exclusivo, el fallo humano acecha en todos los rincones.

Para reducir los daños que nos pueden causar, tenemos que preocuparnos en administrar bien los privilegios



“ *¿Por qué debería preocuparme por la posteridad? ¿Qué ha hecho la posteridad por mí?*

*Groucho Marx*

