



U N I V E R S I D A D
COMPLUTENSE
M A D R I D

Autenticación (resumen)

Gestión de la Información en la Web
Enrique Martín - emartinm@ucm.es
Grados de la Fac. Informática

Resumen

- Almacenar las contraseñas de tal manera que ni los propios administradores puedan saber cuáles son → **hash + sal**.
- Utilizar **métodos de cifrado conocidos** y ampliamente aceptados → deja el trabajo a los expertos.
- Intentar obtener de los usuarios **contraseñas fuertes** → evitar ataques de fuerza bruta.
- Enviar siempre la contraseña (y todos los datos privados) a través de conexiones cifradas **TLS**

Resumen

- Permitir siempre el uso de segundo factor de autenticación.
- La autenticación delegada elimina la sobrecarga de tener que gestionar datos privados de los usuarios.
- La autenticación delegada se realiza mediante OpenID Connect y OAuth 2.0. Es soportada por la mayoría de redes sociales.

Referencias

- Open Web Application Security Project (OWASP):
 - https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet
 - https://www.owasp.org/index.php/Authentication_Cheat_Sheet
 - https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet
- Salted Password Hashing - Doing it Right
 - <https://crackstation.net/hashing-security.htm>