

Validación del lado del cliente vs. del lado del servidor

Validación del lado del cliente vs. del lado del servidor

La validación de entrada debe implementarse en el servidor antes de que las funciones de una aplicación procesen los datos, ya que cualquier validación de entrada basada en JavaScript realizada en el cliente puede ser eludida por un atacante que deshabilite JavaScript o utilice un proxy web.

Se recomienda implementar tanto la validación basada en JavaScript del lado del cliente para la experiencia de usuario (UX), como la validación del lado del servidor para garantizar la seguridad, aprovechando cada una por sus respectivas ventajas.

Lado del servidor

- Protege la lógica del sistema.
- No puede ser eludido por el usuario final.
- Es esencial para la integridad y seguridad de la aplicación.

```
# Registration form submission
post '/register' do
  username = params[:username]
  password = params[:password]
  confirm_password = params[:confirm_password]

  if password != confirm_password
    flash[:error] = "Las contraseñas no coinciden"
    redirect '/register'

  if username.nil? || username.empty? || password.nil? || password.empty?
    flash[:error] = "Username and password are required"
    redirect '/register'
  elsif users[username]
    flash[:error] = "Username already exists"
    redirect '/register'
  else
    # Hash the password before storing
    hashed_password = BCrypt::Password.create(password)
    users[username] = { password: hashed_password }

    flash[:success] = "Registration successful! Please log in."
    redirect '/login'
  end
end
```

Figura 1: Porción de código tomado desde la parte del servidor.

Lado del cliente

- Mejora la experiencia del usuario (UX).
- Permite respuestas más rápidas sin necesidad de esperar una respuesta del servidor.
- Puede ser manipulado o deshabilitado por usuarios maliciosos.

```
<script>
document.getElementById('registerForm').addEventListener('submit', function(event) {
  var password = document.getElementById('password').value;
  var confirmPassword = document.getElementById('confirm_password').value;

  if (password !== confirmPassword) {
    event.preventDefault(); // Evitar el envío del formulario
    alert('Las contraseñas no coinciden.');// Mostrar mensaje de error
  }
});
</script>
```

Figura 2: Porcion de codigo tomado desde la parte del cliente.