# Cross-site scripting e Cross-site request forgery

## Introdução

A web é ainda um mundo em expansão, todos os dias novas aplicações aparecem na web que servem para os mais variados objectivos, temos desde as redes sociais ao *home banking* e não só cada vez há mais aplicações como também existem novos utilizadores. Com o aumento da utilização da web também começou o aumento do número de ataques a estas aplicações, sendo que estes ataques podem ser mais ou menos graves consoante a aplicação atacada. Neste documento vai-se falar de dois dos ataques mais utilizados e os danos que estes podem causar se as aplicações forem vulneráveis.

## Cross-site scripting (XSS)

### O que é?

XSS é um ataque que consiste em o atacante injectar código script (ex. JavaScript) na aplicação, sendo que este irá mais tarde ser executado quando for enviado para algum cliente, com os meus privilégios que a aplicação podendo ultrapassar algumas protecções tais como “*same-origin policy*”.

### Quando acontece?

Este tipo de ataques acontece quando é dada a possibilidade ao utilizador de introduzir algum tipo de informação, por exemplo, num registo quando se introduz os dados ou num motor de pesquisa quando se introduz a *query* de pesquisa. Se a aplicação não sanitizar esses dados é dada a possibilidade ao utilizador injectar código, que poderá ser malicioso.