XSS

Most Info given here : https://portswigger.net/web-security/cross-site-scripting

Cross-site scripting (XSS) is a security vulnerability typically found in web applications. Its a type of injection which can allow an attacker to execute malicious scripts and have it execute on a victims machine.
A web application is vulnerable to XSS if it uses unsanitized user input. XSS is possible in Javascript, VBScript, Flash and CSS. The extent to the severity of this vulnerability depends on the type of XSS, which is normally split into two categories: persistent/stored and reflected. Depending on which, the following attacks are possible:

- Cookie Stealing - Stealing your cookie from an authenticated session, allowing an attacker to login as you without themselves¬†having to provide authentication.

- Keylogging - An attacker can register a keyboard event listener and send all of your keystrokes to their own server.

- Webcam snapshot - Using HTML5 capabilities its possible to even take snapshots from a compromised computer webcam.

- Phishing - An attacker could either insert fake login forms into the page, or have you redirected to a clone of a site tricking you into revealing your sensitive data.

- ¬†Port Scanning - You read that correctly. You can use stored XSS to scan an internal network and identify other hosts on their network.

- Other browser based exploits - There are millions of possibilities with XSS.