It is necessary to know which are the vulnerabilities to which a web server, application sever, and web application are exposed in order to minimise any potential security risks with an aware and structured approach suited to the destination environment.

There are several reasons for which the malicious might be interested to attack the North East Events web site, and not necessarily the unique purpose is to obtain information or alter them to compromise the web site of interest. In fact, it may be only a means to obtain sensitive information about users that then could be used for further attacks, such us a fraud attempted.

Without a broader view and full knowledges about Cyber Security, we would be led to think that the North East Events web site is not subject to attacks same as one referred above, not having any payments procedure planned, and consequently be concerned to design a security system contextualising only on what and how may be compromise our web site.

This is a necessary premise before to discuss the techniques that should be adopted in order to guarantee the security for the company and the users.

Cyber Security is based on the three pillars confidentiality, Integrity, and Availability. Any choice will be taken to achieve each of those in order that the North East Events web site will suffer no impact.

Unfortunately, implementation of firewalls would leave the security vulnerable.

Switching from HTTP to HTTPS is a paramount, using a good certificate authority (such as SSL or TLS). In this way, all data that transits through HTTPS is encrypted.

However, this might not be enough and we need to enforce the browser to reject HTTP requests.

To achieve this, the HTTP Strict-Transport-Security (HSTS) header must be included in the server responses, and every time that the client sends a HTTP request to the server, the browser redirects the encrypted version (HTTPS).

Another header that might be included is the HTTP Content-Security-Policy to control the sources that the client can require and how these should be required.

If the HTTPS will be implemented to best can guarantee the origin, integrity and confidentiality of data.

It is our concern to prevent entering malicious information by attackers, or also put errors inside a web application.

As starting point, an authentication system should be included so as to grant a limited access to the administration area.

Certainly needed is to store no plaintext passwords, but that might not be enough to protect the system and users. Some ex-post mitigations might be insert, such as the second authentication factor in addition to the ordinary credentials (username and password), or/and a maximum number of attempts before to block the account.

Least Privilege is only one of the several paradigms to consider in relation of the database security; each user should have the right to access only to what need. Broader privileges might led access to confident information.

Moreover, each parameters inputted by form has been checked for their validity and has been sanitised to prevent SQL injections, also where the attribute “required” has been used, because to alter the HTML code might be a simple means for malicious as attempt to attack.