BIT695 TM4 Task 1

# OWASP Testing of case study application

The security testing procedures outlined by the Open Web Application Security Project (OWASP) testing guide (2014) feature 91 different tests divided into eleven sections which are:

* + Information Gathering
  + Configuration and Deploy Management Testing
  + Identity Management Testing
  + Authentication Testing
  + Authorization Testing
  + Session Management Testing
  + Data Validation Testing
  + Error Handling
  + Cryptography
  + Business Logic Testing
  + Client Side Testing

The purpose of the tests on the checklist (OWASP Testing Guide v4.0, p. 28) is to check what information could potentially be leaked to an attacker, check for potential ways an attacker to alter the web application, or ways that an attacker might gain access to files, databases or the server itself.

Information that could be passed may include user passwords; server details; the type of framework being used; links to backend files; database access information; author or company details. This type of information can be found by viewing the source code of a web-application, which any browser is capable of doing.

Access to files or the ability to alter the web application could arise from script injections; html injections; sql code injections, etc. These types of injections can come from point of user inputs, for example, a submittal form.

Once testing has completed, a list of potential vulnerabilities, or “threat”, can be compiled and reviewed, with each threat assessed for its potential risk. A decision can be made at this point as how to deal with the “threat”. For example, leaking the company address – while it is an information leak, will it affect the running of the web application if an attacker knows the address of the company? – Only if the attacker was to physically attack the address – But, a form not performing validation properly might allow for an sql injection, letting an attacker gain unauthorized access to the database, where they could corrupt data, mine user information, or worse...

Reviewing our case study web application from TM1, we find that there are some serious potential threats to the application or server. Including the unused file “form\_template.html” in the web application directory is dangerous. An attacker could access this file by brute force, fill out the forms with scripts or injection code, which has the potential to cause irreverent damage to the server, set up information collecting malware, etc.

# Confidentiality, Integrity, Availability – The CIA triad.

The CIA triad is a model designed to achieve information security, by using the three-fold headings information can be assured secured by:

* Protecting information from unauthorised access.
* Providing accurate information that can only be changed by authority. This information must “*remain unchanged during storage, transmission and usage*…” (Henderson, 2017)
* Making sure information is available when and where it is required.

## E-commerce

An e-commerce application, in the context of the CIA triad, should place the importance of availability as its lowest priority. The first priority should be the integrity of the information – a user needs to be assured the values they are receiving are correct before executing a transaction. The second priority is confidentiality – the user needs to be assured their personal details (like credit card details) remain secure if they make a transaction.

The impact availability has on an e-commerce application effects the end user experience more than integrity or confidentiality. Without available information when the user wants it, they are unable to assess integrity or confidentiality.

## Modern web application

The CIA triad model has limitations with a modern web application. Functions like local storage and local session storage, facilitating offline access, affect the integrity of a web application. The user cannot be assured that the information they have is the most up-to-date and accurate. For example:

* a user checks out an e-commerce site on their mobile device at work, this information is stored in local storage on their device.
* They then travel home, during this time the network goes offline and at the same time the e-commerce site changes its prices.
* The user arrives home opens the web application, the locally stored information is displayed, they begin to process a transaction, as they submit the transaction the network comes online.
* The e-commerce server receives a message to purchase item and makes the transaction.
* The user is charged a different price to the one they believed the transaction was worth.

Although availability and confidentiality can be addressed successfully on a modern web application, without the application being able to verify that every user has the most up-to-date information stored on their devices integrity cannot be addressed.

# References

Henderson, A. (2017, March 25). *The CIA Triad: Confidentiality, Integrity, Availability*. Retrieved from Panmore Institute: http://panmore.com/the-cia-triad-confidentiality-integrity-availability

The OWASP Foundation. (2014). *OWASP Testing Guide v4.0.* Retrieved from OWASP: https://www.owasp.org/index.php/OWASP\_Testing\_Project