**Procedure CDP09 – IT Security** *(version 3.0)*

# Risk assessment report (10 points)

You should write a report (max 4 pages of A4) describing the main **threats** posing a **risk** to your project, as well as possible **solutions** where appropriate.

Topics to be discussed may include (but not be limited to):

* SQL injection
* Cross Site Scripting (XSS)
* Session management
* Password policies and Encryption
* Server misconfiguration
* Cross-Site Request Forgery (CSRF)
* Denial-of-service attacks (DDOS)

Impact on **Business Continuity** should be considered. Risks should be sorted by the severity of possible consequences (data breach, loss of income, loss of reputation, criminal charges etc.) Your Project Manager should be kept informed, so that appropriate resources (e.g. training, development time) can be allocated.

## What to submit

* A written report (e.g. Word document)

## Scale

The following scale should be used as a guideline when evaluating this objective:

|  |  |
| --- | --- |
| 10 points | A detailed account of the points listed above, showing a good understanding of the subject matter.  **References have been used** to underpin the work. |
| 8 points | A detailed account of the points listed above, showing a good understanding of the subject matter.  **References have not been used** to underpin the work. |
| 5 points | A partial account of the points listed above, but not all aspects are covered.  A good understanding is shown. |
| 2 points | A partial account of the points listed above, with very little understanding shown. |
| 0 point | No work submitted towards this objective |

# Implementation (10 points)

You should apply your findings (see previous section) to the product being developed, and implement security measures at all levels, including:

* Application code (e.g. PHP)
* Database (e.g. encryption)
* Functional level (access levels, password policy etc.)

Note: You should implement the measures yourself, or assist the development team in doing so.

## What to submit

* Code listing, highlighting your contributions
* Screenshots of any other security contributions (e.g. encrypted passwords in MySQL)

## Scale

The following scale should be used to evaluate the points above:

|  |  |
| --- | --- |
| Security measures implemented in application code. | 4 points |
| Security measures implemented in database | 3 points |
| Security measures implemented at functional level (access levels, password policy etc.) | 3 points |
| *Total* | *10 points* |

# Security testing (10 points)

You should create a **test plan** based on your research in order to fully test the application against the most common security threats.

You should then **perform some security testing**, either manually, or using an automated security testing tool.

## What to submit

* A written report (e.g. Word document)
* Screenshots of contributions to GitLab issues

## Scale

The following scale should be used to evaluate the points above:

|  |  |  |
| --- | --- | --- |
| Test plan  *5 points* | A detailed test plan was submitted, covering **all** security threats | 5 points |
| A **partial** test plan was submitted, but **not all** security threats are covered | 2 points |
| No test plan submitted | 0 point |
| Security testing  *5 points* | Testing was performed  Issues/bugs **were** created in Version Control system, and followed up | 5 points |
| Testing was performed  Issues/bugs **were** created in Version Control system, but **not** followed up | 3 points |
| Testing was performed  Issues/bugs were **not** created in Version Control system | 2 points |
| No testing performed | 0 point |