Joe Williams

Reboot games  [Company address]

HOW TO REDUCE VULNERABILITIES IN A SYSTEM?

Contents

[Introduction 2](#_Toc511641210)

[What happens during development? 2](#_Toc511641211)

[Vulnerabilities 2](#_Toc511641212)

[Example of vulnerabilities being used in a business environment. 2](#_Toc511641213)

[Social engineering 2](#_Toc511641214)

[What can be done to reduce vulnerabilities? 3](#_Toc511641215)

[Case studies 3](#_Toc511641216)

[Case study 1 3](#_Toc511641217)

[Case study 2 3](#_Toc511641218)

[Primary research 4](#_Toc511641219)

## Introduction

This report is about the vulnerabilities during development and how to reduce the amount of vulnerabilities during the development stage of a product or application. It will also go over what a vulnerability is and what is means when it is found or created during development.

## What happens during development?

The development process is used when creating a product of application and is always used during this stage. The development process is when the game is created from a basic state to the final product.

The development of a product or application involves a lot of stages which will add certain features and unique man into the application or product. For example, in the reboot games Elevator action reboot project development will involve splitting up the development process into developing the different features of the game into parts. Such as the jumping feature being created in one step and the next step being enemy AI. (<https://github.com/HORNETJOE/Capstone-Project>)

## Vulnerabilities

Vulnerabilities are discovered when creators leave errors, unfinished or mistakes are left in a final product. These vulnerabilities can lead to many different problems such as cheating, data theft etc. These vulnerabilities can be devastating to a company if they are discovered within a system. These vulnerabilities can cost companies thousands if they are discovered after the final product has been released. This is why these vulnerabilities need to be reduced during the development stage which will cost the company less and still reduce the amount of vulnerabilities on the final system.

### Example of vulnerabilities being used in a business environment.

One example of vulnerabilities being taken advantage of in a business would be Dailymotion hack that took place December 2017. The incident involves millions of users emails and private information being leaked online due to a vulnerability on the website. This is one example of how a vulnerability can impact the company (I.E reputation) and impact the customer as well (I.E Private information).

## Social engineering

Social engineering is a method of seeking out a vulnerability in a system that require human error to create a vulnerability to then exploit. This may involves tricking employees at a company to allow outside users access to their systems through misleading emails, ads and messages. Once the outside users have gained access to their system they have created a vulnerability in the system for others to use to gain access as well. This vulnerability relies heavily on human fault and misjudgement in order to gain access to a system.

## What can be done to reduce vulnerabilities?

There are many different methods of reducing vulnerabilities, many are done during the development process of a system. One method of reducing vulnerability is to run tests on new functions that are implemented into the system to make sure that they work on their own and with the other function in the system. Other method of reducing vulnerability is to have different people working on different parts of the system so that the different parts of the system can be sixed by different people and different people can work on each part of the system while it is in development.

Another way of reducing vulnerabilities would be to reduce the gap between an employee’s personal life and their work life by giving them work emails and work equipment. These will only be used in the work environment. This will reduce the chance of misleading emails or infected hardware from being used in the workplace and infecting the system and creating vulnerabilities.

## Case studies

### Case study 1

The Dailymotion data breach is a good example for vulnerabilities that can be exploited in a system. The website Dailymotion which is a video-sharing technology platform, was hacked by an unknown group/individual. The breach was carried out on the 20th of October and was announced and made official in November. The damage was over 18.3 million private emails and password were leaked onto the web.

Dailymotion acted on this breach by informing all of it customers of the breach and advising them to take suitable measures to change information and details on their accounts.

(<http://www.zdnet.com/article/dailymotion-hack-exposes-millions-of-accounts/>)

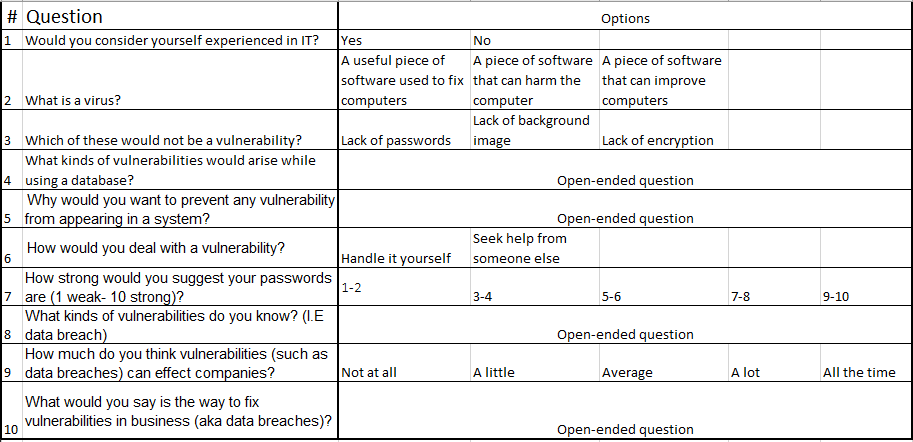
### Case study 2

# Primary research

Primary research involves gathering new data that has not been collected before. For example, surveys using questionnaires or interviews with groups of people in a focus group which has been done below.

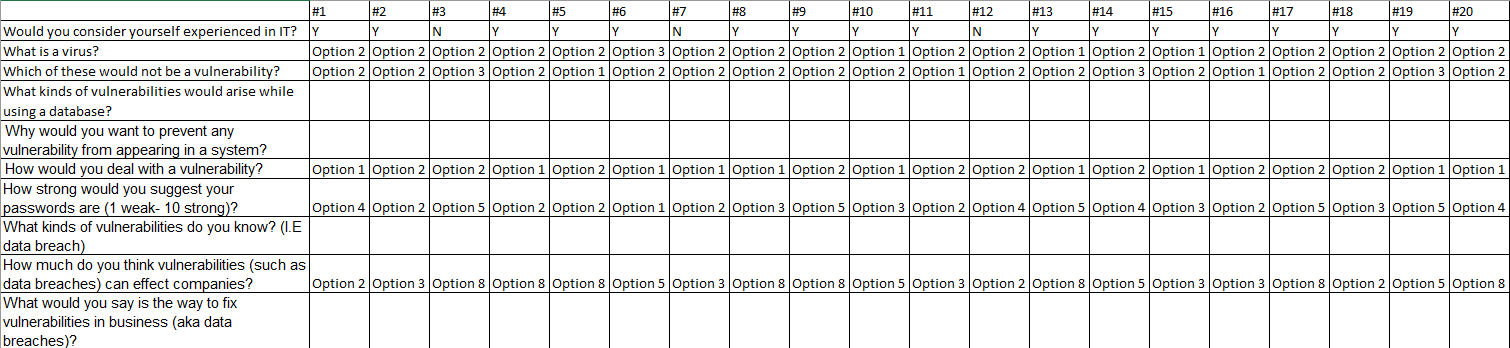
#### Questions

The image below is the list of questions that were answered on the questionnaire.



#### Answers

Below are the answers that were given to the questions that were on the questionnaire.



#### Bar chart

The chart below has some data on the choices that were made and the difference between them.