FINAL YEAR PROJECT II

RAXS:
An Expert System for Rating Vulnerabilities

Jong Qianjun

15112

(Business Information System)

September 2013

Universiti Teknologi PETRONAS

Bandar Seri Iskandar

31750 Tronoh

Perak Darul Ridzuan

CERTIFICATION OF APPROVAL

RAXs:

An Expert System for Rating Vulnerabilities

by

Jong Qianjun

A project dissertation submitted to the

Business Information System Programme

Universiti Teknologi PETRONAS

in partial fulfillment of the requirement for the

BACHELOR OF TECHNOLOGY (Hons)

(BUSINESS INFORMATION SYSTEM)

Approved by,

____

(Mr. Khairul Shafee Kalid)

UNIVERSITI TEKNOLOGI PETRONAS

TRONOH, PERAK

September 2013

CERTIFICATION OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this project, that the original work is my own except as specified in the references and acknowledgements, and that the original work contained herein have not been undertaken or done by unspecified sources or persons.

(Jong Qianjun)

ABSTRACT

Over the past few years, there has been a worrying trend of increment in number of web application intrusions. Based on reports released by reliable sources, these incidents are due to the lack of experts in performing accurate risk assessment to mitigate the risk while performing web security testing. Risk assessment is the core process in providing appropriate recommendations when dealing with vulnerabilities discovered in a web application. Therefore this research paper will be highlighting the problem of insufficient experts to guide the less experienced information security analyst in conducting effective risk assessment. The objective of this research will be to design an expert system to aid the less experienced system analyst in conducting accurate risk assessment during the absence of experts. The expert system will cover all risk rating of vulnerabilities included in the OWASP Top 10 2013, and the target user will only be the less experienced information system analyst. The methodology used in the research would be based on the expert system development life cycle model. The main activity conducted is the construction of knowledge base of the proposed expert system. Based on the results of collected knowledge and information from the internet as well as interviewing experts, the knowledge developer will construct a decision tree which aids in the development of the expert system in later phase of the research.

ACKNOWLEDGEMENT

First and foremost, the author wishes to extend his deepest gratitude and appreciation to the supervisor of this project, Mr. Khairul Shafee Kalid. Without his support and guidance throughout the period, this project will not be possible.

Moreover, special thanks would also be dedicated to the various parties who have helped out in the development of the prototype. This is especially dedicated towards the experts and employees in the various firms who have willingly assisted in the project by giving valuable insights and ideas to the author. Their help in completing the prototype is also very much appreciated.

Last but not least, the author would like to express his utmost gratitude to his family and friends who have motivated him along the course of this project.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

1.1 Background of Study 1

1.2 Problem Statement

1.2.1 Problem Identification 4

1.2.2 Significance of Project 7

1.3 Objective and Scope of Study 8

1.4 Relevancy of the Project 9

1.5 Project Feasibility

1.5.1 Technical Feasibility 10

1.5.2 Organizational Feasibility 10

1.5.3 Economic Feasibility 11

1.5.4 Feasibility within Time Frame and Scope 11

CHAPTER 2: LITERATURE REVIEW

2.1 Expert System 13

2.2 Justification and Limitation of Expert System 16

2.3 Web Application Vulnerability Assessment and the Implementation of Expert System 18

2.4 Risk Assessment Phase 20

2.5 Related Work

2.5.1 IBM ISS X-Force 22

2.5.2 Vupen Security 23

2.5.3 RAMeX 23

2.5.4 KMS 24

2.5.5 IDES 24

2.5.6 GyMEs 25

2.5.7 Expert System for Boiler Fouling Assessment 25

CHAPTER 3: METHODOLOGY

3.1 Expert System Development Life Cycle 27

3.1.1 Problem Identification and Analysis 28

3.1.2 System Specify & Development Tool Selection 29

3.1.3 Tools 30

3.1.4 Knowledge Base 30

3.1.4.1 Knowledge Acquisition 31

3.1.4.2 Knowledge Representation 31

3.1.4.3 Computer Code 32

3.1.5 Prototype System 32

3.1.6 Testing and Validation 32

3.1.7 Implementation 34

3.2 System Architecture 35

3.3 Gantt Chart and Key Milestone 36

CHAPTER 4: RESULT AND DISCUSSION

4.1 Pilot Study 39

4.2 System Flowchart 43

4.3 Prototype 44

4.4 Prototype Testing

4.4.1 Assessment and Evaluation Testing 46

4.4.2 Verification and Validation Testing 48

CHAPTER 5: CONCLUSION

5.1 Conclusion 50

5.2 Future Work 51

6.0 References 52

7.0 Appendix 56

LIST OF FIGURES

FIGURE 2.1: Forward Chaining and Backward **15**

FIGURE 2.2: Operation of Expert System **16**

FIGURE 2.3: Life cycle of WAVA **18**

FIGURE 2.4: OWASP Top Ten comparison between year 2010 and 2013 **19**

FIGURE 2.5: Risk Assessment Life Cycle **21**

FIGURE 3.1: Expert System Development Approach **28**

FIGURE 3.2: System architecture of expert system **35**

FIGURE 4.1: Pilot study question 1 **40**

FIGURE 4.2: Pilot study question 2 **40**

FIGURE 4.3: Pilot study question 3 **41**

FIGURE 4.4: Pilot study question 4 **42**

FIGURE 4.5: Flowchart of expert system **43**

FIGURE 4.6: Sample decision tree to represent knowledge **44**

FIGURE 4.7: Homepage of expert system **45**

FIGURE 4.8: Interface of the expert system **45**

FIGURE 4.9: Prototype testing question 1 **46**

FIGURE 4.10: Prototype testing question 2 **47**

FIGURE 4.11: Prototype testing question 3 **47**

FIGURE 4.12: Prototype testing question 4 **48**

FIGURE 4.13: Prototype testing question 5 **49**

LIST OF TABLES

TABLE 2.1: Comparison between Human Expert and Expert System 17

TABLE 3.1: List of requirements to run Exsys Corvid 30

TABLE 3.2: FYP I Gantt Chart 36

TABLE 3.3: FYP II Gantt Chart 37

CHAPTER 1

INTRODUCTION

1.0 Introduction

This research is carried out to develop an expert system named “RAXS”, short for Risk Assessment Expert System, which will assist the less experienced information security analyst in the rating of risk level of vulnerabilities in web application. For example, during the web application security testing of an online fund transfer web application, an information security analyst, or ethical hacker, has discovered there are two vulnerabilities in the system which are an error in coding logic of the login field, and another backdoor that will lead to a compromised database. However the company only has available resources to mitigate one of the vulnerability. Therefore it is important to have an accurate rating of risk level of the two vulnerabilities to determine which requires a more immediate attention in order for the limited resources to be invested in remediating the more crucial vulnerability. The purpose of RAXS expert system will be to assist the less experienced information security analyst and recommend the risk level for each vulnerability and propose an appropriate solution to the vulnerability. For this section, the background of study, problem statements, objective and scope, relevancy, and feasibility of the project will be highlighted.

1.1 Background of Study

The risk assessment phase of web application vulnerability assessment, or in layman term, the security testing of web application, is especially important to ensure the accuracy and usefulness of a web application vulnerability assessment (Halley, 2011). By performing risk assessment, it will help in quantifying the risk associated with a vulnerability in web application, and the potential financial impact as well (Sykora, 2012). Moreover, an accurate risk assessment will also lead to optimal control recommendation which is in line with the priorities of stakeholders and executive management.

In the risk assessment phase, the information security analyst will determine which information asset will cause potential problems to the public, clients, organization, and application users if it is compromised (OWASP, 2013). The severity of the vulnerability associated with the breach of the information asset will then be qualitatively rated accordingly. After the potential risk levels and impacts are being calculated, the team responsible will be able to take appropriate actions to deal with the vulnerability that is most significant.

There exists a need for risk assessment due to the fact that perfect security is not feasible (Terry, 2013). This is mainly due to the fact that risk assessment is not required by the law, and there is always insufficient security budget. If there are laws requiring perfect security, and there is ample budget to ensure the web application is secure, the information security analyst will not need to perform risk assessment, instead he can recommend that all vulnerabilities be secured regardless of the business impact and investments needed. Therefore a risk assessment is required to ensure security investments are appropriate to the business process.

Based on a recent statement released by CyberSecurity Malaysia, formerly known as NISER in 2012, it is stated that there had been a rise of number of intrusions in Malaysia. The number of cyber-attacks had increased from 580 cases in 2007 to 766 cases in 2008, which is equivalent to an increase of 32.07%. Moreover a recent study by Ernst and Young in October 2013 has also discovered that for the past 12 months alone, the number of security incidents has increased by at least 5%. This resulted in a total of 62% of the organizations surveyed being compromised at the highest level, or in other words, the security is being completely compromised.

However, even by implementing web application vulnerability assessments, not many companies had achieved their desired outcome of a secure web system. This is due to inaccurate assessment of risk due to lack of understanding on the business which leads to wrong conclusions. In the case of Web application vulnerability assessment, the boutique firms will include all the small firms specializing in providing web application vulnerability assessment service to their respective clients or customers. In order to conduct a successful risk assessment, the security analyst must understand the business impact as well as the characteristic of the vulnerability. Since majority of security analyst are from Information Technology (IT) background, they had lesser experience to the business implications which will lead to inaccurate judgment.

Therefore to successfully conduct the assessment, less experienced information system security analyst will need to refer to the experts in their field who have more experiences. However due to the increase in demand for web application vulnerability assessment jobs, there will be a need to have an expert system to aid in the risk assessment phase, as less experienced analyst will need to depend on expert systems to make accurate decisions when the experts are not around. According to a statistic released by the Bureau of Labor in 2012, the estimated increment of information security analyst will only increase by a meager 22 percent from 2010 to 2020, indicating that the number of experts in the related field will be very limited for years to come, which justifies the need of an expert system to serve as a substitute for human expert in the domain. However in a report released by the same department in October 2013, it is seen that the workforce of IT security analyst has actually plummeted by 3.7% instead, albeit a rise in IT workforce. This has implied that although there may be a rise in number of IT workforce, there has been insufficient increment of IT personnel with security knowledge to complement the increment of personnel, which may lead to greater security compromises.

Therefore in this research, the researcher will be focusing on utilizing expert systems to support the risk assessment procedure. With this, the less experienced ethical hackers will be able to accurately determine the risk level of a specific vulnerability, and make accurate decisions in advising the client as to which vulnerability should be attended to first according to the risk level involved. This is to ensure more system can be adequately secured with the limited amount of resources.

1.2 Problem Statement

1.2.1 Problem Identification

1. *There are insufficient experts to guide less experienced information security analyst to conduct web application vulnerability assessment's risk assessment.*

   Due to the fact that the risk assessment would require the assessor's knowledge and experience in dealing with business operations as well as threat analysis skills, there are few experts who will be able to guide the less experienced to conduct risk assessment effectively.

   According to the information posted on world renowned firms providing training for Certified Ethical Hackers, it is seen that the course outline does not include any trainings for assessing the risk factor of the vulnerabilities. The training module only includes the penetration testing methods and trainings without any emphasis on the risk assessments methods. Thus the information security analyst will have insufficient training in dealing with risk assessment process.

   Based on a paper published by Satava in the article "26 things You Should Know Before Working for a National Accounting Firm", it is stated that the turnover rate of auditor in major auditing firms are as high as 23 percent as compare to local firms with only 9 percent. Due to the fact that most of the major web application vulnerability assessment jobs are conducted by the information security teams in auditing firms, a high turnover rate would mean that there would be lesser experts available who are able to conduct the assessment.

   Therefore without sufficient skills and experiences in conducting risk assessments, the information security analyst will not be able to accurately determine the risk level of a given threat. This may lead to wrong advice and suggestion to mitigate risk, which may lead to improper configuration of web application security. Due to that, the web application may be compromised by illegal third parties, causing significant reputational and operational risk.

2. *Unreliability of risk assessment resulting from expert under unfeasible condition.*

For a risk assessment to be accurate and precise, there are numerous factors that should be taken into consideration. Based on a 2013 paper released by an open source web application security project, OWASP, the factors that should be considered when performing a risk assessment includes both the technical and business impact factors. Moreover, it is crucial that the likelihood, criticality and severity of a threat agent or vulnerability be considered as well to increase the accuracy of assessing the risk involved.

Therefore in order to search for an accurate procedure or process to conduct a proper risk assessment, the time taken would be too long, as it is a complex procedure.

Since the same vulnerability, when placed under different conditions which may include different business system, it may behave differently and it will make the risk assessment process much more complex and unpredictable for the less experienced. Due to the complexity of the procedure, an experienced information security analyst may also make mistakes in the process.

Based on a research paper by Alexandra et.al (2009) on performance error due to work overload and other mental stressful events, it is stated that when performing complex processes, a human's decision may be unreliable even he is an expert due to fatigue and other factors. Thus to ensure the process of risk assessment will not be affected by human error, a more efficient tool will be needed.

Without an efficient system in place, the current decision making process for risk assessment is deemed to be too complex, and even an expert may conduct a wrong risk assessment. This may eventually lead to wastage of resources.

In short, due to the complex risk assessment process, the resources that are required to perform accurate risk assessment will be too huge if necessary steps are not taken.

3. *Difficulty to locate experts to aid the less experienced analysts in risk assessment.*

Even though there are a number of experts in risk assessments for hire throughout the world, there is still the problem of difficulty in locating experts. This problem is especially for major firms providing web application vulnerability assessment services as major firms will usually receive a high amount of workload which thins out the workforce of experts as each experts need to handle several jobs at once. Thus it is not possible for the experts to guide the less experienced analysts. Moreover it is not possible for the firms to hire outsiders to perform the job due to private and confidentiality matters. The web application vulnerability assessments' results are always kept within a limited number of people due to discretion reasons as it may affect the reputation of the company which is requesting for security inspections on their web application (Hiu, 2013). Therefore due to the several limitations, despite the number of experts available around the world, it is difficult to locate experts which can aid the less experienced analysts in the risk assessment phase on the job.

1.2.2 Significance of Project

This project will serve as an important milestone in the future development of a more secure web application for the corporate as well as individual usage. By having an expert system in place that is able to assist in providing recommendation and advice to the less experienced information security analyst during the risk assessment phase, a much accurate risk rating can be conducted even with the absence of an expert to guide them.

With an accurate risk assessment in place, it will ensure a more effective and efficient allocation of resources to secure the web applications. It will reduce the likelihood of investing valuable and limited resources towards remediating a vulnerability that would have minimal or no direct negative impact towards the web application, especially when there is another vulnerability that would have severe impact on the application. By implementing the system, the users will be able to propose suitable recommendations regarding the vulnerabilities that require fixing. Moreover, even when there is a lack of experts due to limitation in human resources, less experience analyst may refer to the expert system instead of waiting for an expert to guide them through the process of risk assessment.

In short with the expert system in place, issues relating to coming up with better risk assessment decisions for less experienced information security analysts can be avoided even with the absence of experts. Moreover, by having the expert system, web applications can also be more secure due to the accurate risk assessment, and this will reduce the operational risk, reputational risk as well as the business risk. With a secure web application, online business can be carried out without worrying their personal information may be compromised. Therefore this research is especially significant to ensure the future of business in the virtual world of internet can be carried out more efficient and effectively.

1.3 Objective and Scope of Study

The general aim of this research is to propose a design of a prototype expert system that will assist in the risk assessment phase of web application vulnerability assessment. The target user will be the less experienced information system analyst or the ethical hackers in case there is no expert to refer to during the risk assessment phase. By having this system, it will assist the users in effectively determining the risk rating of specific vulnerabilities. Therefore this expert system will only be employed after vulnerabilities had been uncovered and the risk of each vulnerability is to be determined. The nature of the assessment was such that it was meant to analyses an identified malicious threat to determine its severity in terms of business impact and ability to compromise the integrity of the web application. This will also help to identify possible future research opportunities as well as individual studies regarding web application security and risk assessment structures. The scope of the research will include the OWASP Top10 most significant vulnerabilities which will be discussed later in the literature review. The research will also focus on determining a specific threat's behavior and impact under different environment so that a more comprehensive risk assessment can be conducted.

In short the main objective of this project will be:

1. To study on how experience information security analysts conduct risk assessment. The knowledge obtained through the study will be utilized in the construction of the knowledge base of the expert system to ensure the expert system will duplicate the expert's decision making process during risk assessments.
2. To design and develop an expert system to aid the less experienced information security analyst in conducting accurate risk assessment during the absence of experts. The expert system will gather information from users and recommend a possible risk rating for a given vulnerability besides advising on the solution to the vulnerability.

1.4 Relevancy of the Project

The development of the expert system seeks to provide accurate and non-bias recommendation to its user regarding the risk ratings of vulnerabilities. The assessment will be conducted according to the document, OWASP Top Ten 2013 vulnerabilities to reduce the scope of the project due to resource constraints. Therefore it will not be able to provide absolutely correct recommendations for all possible vulnerabilities. However, it will also be an important milestone in making the online society a better place with less exploitation and security intrusions. With a safer online network, online business transactions can be carried out more efficiently leading to an improvement in economy to the community.

Moreover, it is worthwhile to note that web securities and the relevant technologies are subjected to constant changes which will introduce new exposures to existing web systems. Therefore the expert system will need to be constantly updated to provide a more complete risk assessment. Without updating, the expert system can only provide a "snapshot" of the security status at a specific given point of time. Without a carefully managed expert system, the introduction of new risks and vulnerabilities may not be properly addressed by the system.

In brief, for the relevancy of the project, the objective of developing an expert system to assist the less experienced system security analyst can definitely be achieved. However it is important to note that constant monitoring and management of the knowledge base is equally important to ensure its reliability in the field.

1.5 Project Feasibility

The three main feasibilities, namely the technical feasibility, organizational feasibility and economic feasibility will be analyzed in this section. This will be to determine whether the project is feasible within the scope of the project. Moreover, it will also be determined whether or not the project is feasible within the time frame of the project timeline.

1.5.1 Technical Feasibility

For this section, it will describe the extent to which the development of expert system to handle risk assessment is technically feasible to be conducted. Due to the fact that the development life cycle of expert system is different as compared to the conventional system development life cycle, there will be a moderate learning curve that needs to be addressed. This may include the stages of system development as well as the tools that will be needed to develop the expert system is different from that of conventional systems.

However, there are a lot of user friendly software and tools that are available online to develop expert system, which will reduce the steepness of the learning curve. Through the usage of those tools, even an amateur will be able to develop the system with particular ease. Moreover, there are also a lot of reference books and online resources that are readily available in the library as well as the World Wide Web. This will allow the required information and knowledge to be attained much easily.

1.5.2 Organizational Feasibility

For the organizational feasibility, it describes the willingness and acceptance rate of users in incorporating the system into the organization’s organizational process. The project will only be accepted if the people are supportive of it.

Due to the nature of the expert system which is to aid in determining the severity and criticality of a particular vulnerability in the system, it will help the less experienced in conducting successful web application vulnerability assessment. Since the user of the expert system, the less experience system security analyst, will be able to make use of the system to make a more accurate decision which increases their task performance, they will be accepting the implementation of the system.

As for the organization’s management team, by introducing this expert system to aid in their company’s system security analyst team, they will be able to achieve better performance at lesser cost. This is due to the fact that the less experienced members will be less dependent to the experts when performing security analysis while maintaining the same quality of work. Thus with the benefits weighing greater than the cost, the organization will be supportive of the implementation of the system.

1.5.3 Economic Feasibility

Economic feasibility is to determine whether the project is feasible financially. The project will only be considered as acceptable and practical only if the cost required to carry out the project will not exceed the benefit it will bring upon the implementation of the system. For the project, the main cost of the development of the expert system will be the transportation and communication cost involved in interviewing and searching for experts. The experts are approached to create the knowledge base required for the expert system.

As for the tools, since there are a lot of freeware available online that will aid in the development of expert system, the cost of software and tools will be minimal. However, in case the freeware are not as effective to develop the expert system, the cost needed to purchase genuine software will still be lower as compare to the benefit it will yield. For instance, in the case where the expert system has been implemented, it will be able to successfully perform risk assessment which will help the organization save a lot more cost in the remediation of the vulnerabilities.

Thus for the project, it will be economically feasible as the benefit yield will always be greater than the cost it will incur.

1.5.4 Feasibility within Time Frame and Scope

Before the commencement of the project, it has been scheduled that the project will only spanned for a limited amount of time which is approximately within the range of eight months. Since the time needed to develop the system will mainly depend on the knowledge required to be gathered for the knowledge base, the scope of the project will directly affects the total duration of the project.

Therefore in order to ensure the feasibility of the project in term of its time frame, the scope of the project has been readjusted to make it much more realistic and practical. The project will only cover the risk assessment section of the entire web application vulnerability assessment, which is a short but crucial section in the testing process. Moreover the project will focus mainly on the ten major vulnerabilities which are more prominent in nowadays society, to make the compilation of the related knowledge much convenient. Thus by adjusting the scope of the project to a smaller scale, the project is made much more feasible within the time frame of the system development life cycle.

CHAPTER 2

LITERATURE REVIEW

2.0 Introduction

This section will highlight all the information retrieved from various related literature sources. It will explain about the expert system, web application vulnerability assessment, risk assessment phase as well as the related works that has been done in the past that is similar to the current project. Comparisons and researches will be made to enhance the value of this project.

2.1 Expert System

The idea of expert system can be traced back to as far as the 1970s. The first major advancement in expert system dated back to 1972, whereby the first ever French Prolog computer language which aids to develop expert system much more efficiently is designed. Based on a paper written by Michie in 1979, an expert system is defined as an "intelligent information system which is able to behave as a human expert in a specific domain". Another more recent paper published in 2009 by Duan however, defines expert system as a "system which utilized the captured human knowledge in a computer to solve complex questions that will usually require human experts". From the two definitions, it can be clearly seen that expert system is meant as a substitute for human experts in solving complex problems for a specific domain.

Since the advent of expert system, it is widely recognized that an expert system is composed of three main parts, which is first, the knowledge base, secondly an inference machine and thirdly the user interface. According to a paper entitled "An Expert System for Decision Making" by Bohanec et al (1983), the knowledge base is a repository of knowledge about a specific domain. Based on the definition of Bohanec (1983), the knowledge base is a collection of knowledge about a particular problem domain, and it will be utilized by the inference engine to solve user stated problems by generating user oriented explanation of solutions. It includes the required knowledge to solve problems related to a single domain. The knowledge is usually stored as facts and rules (Awad, 1996). In nowadays society, rule-based knowledge base which employs the IF…THEN rules are more commonly used as compared to other methods such as frame-based.

As for the inference machine, it is the engine which coordinates reasoning and inferencing based on the rules being stored in knowledge base and provides suggestion of solutions of the problem stated by users, and able to generate user oriented explanations. Apart from the common use of prolog programming language or using software such as exsys corvid for expert system's inference engine development, there are a number of projects which implements other type of programming language to develop the inference engine. For instance, javascript is also a commonly used language for the development of inference engine. It is more commonly known as javascript-based rule engine which utilizes javascript for the programming of inference engine (Pascalau & Giurca, 2013). Moreover there are also expert system shells such as "expertise2Go" which implements javascript as inference engine. However it is seen that most of the rules engine or inference engine which is developed using javascripts are web-enabled only.

Certain Common inferencing rules include forward chaining and backward chaining, whereby the first focus on gathering information to deduce the goal, and the later focuses on the goal first and work out to determine its authenticity by gathering additional information (Awad, 1996). Based on Ignizio (1991), rule based representation of knowledge is the most commonly used mode to represent knowledge captured from experts. It uses the IF…THEN statements to represent the knowledge captured from the experts. An example of rule based expert system's representation is shown below:

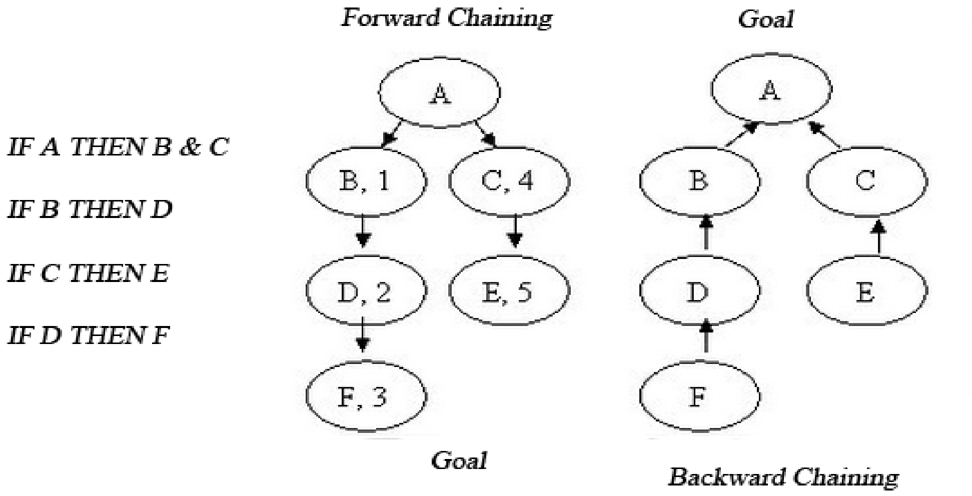


FIGURE 2.1 Forward Chaining and Backward Chaining (Watson, 1997)

Lastly there is the user interface which is normally a graphical interface that allows user to operate the expert system easily. Through the user interface, the expert system will be able to gather required information from the user by either multiple choice menu or asking direct questions. The information is then passed on for the inference engine to be processed to provide recommendation to the user. Therefore by utilizing both the knowledge base gathered from experts of a specific domain and also the inference machine, the users will be able to solve their problems without the need to refer to a human expert. A clear diagram which summarizes the operation of expert system can be seen below:

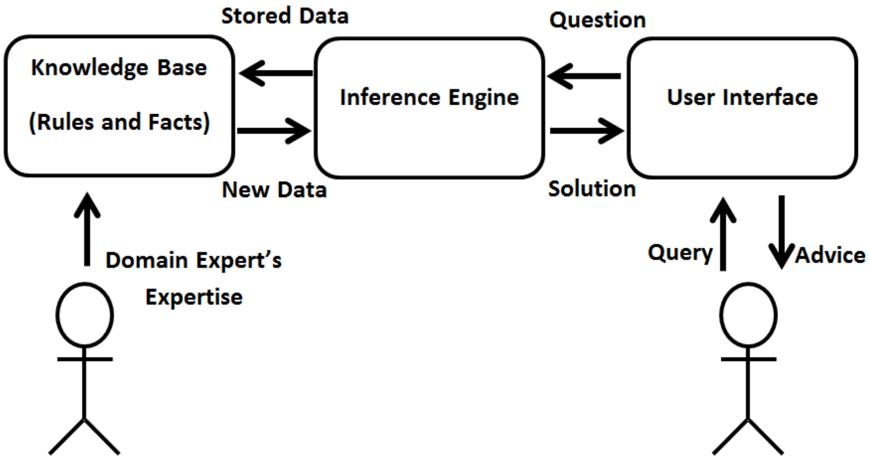


FIGURE 2.2 Operation of Expert System (IGCSE ICT, 2012)

2.2 Justification and Limitation of Expert System

As stated by Ashrafi et al (1995) in their research, with the aid of expert systems, reliable decisions can be made as expert systems, unlike humans, are not prone towards errors and biases which is due to fatigue, lack of attentions, emotions and much more. Since human errors are the most prominent factor that will disrupt the accuracy and precision of the decision made, if the human error is being removed from the decision making process by implementing expert system, the result will be much more reliable. Moreover, expert systems are able to hold a large knowledge base of a specific domain. As compared to human, expert systems will take lesser time in organizing the solutions, and there will be less possibility of forgetting important knowledge due to aging or illness. Therefore by utilizing expert system, the risk of human error in making decisions can be minimized, and a more accurate decision can be made by the expert system regardless of the physical and mental condition of the user.

Moreover, another more prominent reason that justifies the need for expert system is that expert systems will be able to release the users from performing repetitive, routine task which is complex and requires a lot of process to get the decision done. From past researches, it is discovered that through implementing expert systems, it is able to increase the user's job satisfaction and cultivates positive attitude towards their task at hand (Guimaraes et al, 1996). For instance, expert system can support non expert users in reaching a more accurate decision by simplifying the decision making process and reach a conclusion without referring to an expert. Besides, experts can also utilize expert systems to reach a decision much easily without going through complex processes. With a comprehensive expert system, the users will be able to avoid the steep learning curve required and get to the decision immediately. Through this advantage, significant amount of time and resources can be invested elsewhere, as the number of trainings required for the user to perform optimally and make the right decisions can be reduced.

In short, the need to implement expert system is mainly to tackle the problems present in human expert. The table below summarized the comparison between human expert and expert system:

TABLE 2.1 Comparison between Human Expert and Expert System

Factor	Human Expert	Expert System
Time (can be obtained)	Working days only	Anytime
Geography	Local	Anywhere
Safety	Cannot be replaced	Can be replaced
Damages	Yes	No
Speed and Efficiency	Changes	Consistent
Cost	High	Intermediate

However, with the numerous advantages of expert system, it will not be economically feasible to implement the system in every situation. As stated by Guimaraes, the success of expert systems is measured by their cost saving and benefits, which includes also the intangible benefits. Thus in order for expert system to be implemented, the tasks to be handled by the system must have a high payoff, and especially crucial to the operation of the business.

Moreover, expert systems have also migrated from academically oriented efforts in the past few decades and moving towards a more complex managerial-oriented role (Ashrafi et al. 1995). Due to the changing trend, expert systems have shifted to accommodate situations which are much more complex and the problems are badly structured. In those situations, the expert system will be utilized to come up with a sound decision in handling those problems quickly by imitating the decisions of an expert. In short, expert systems will only be implemented in the situation whereby the payoff is high and is crucial to the business operations, as well as the problem to be solved must be complex. If those conditions are not fulfilled, there will be no need for an expert system.

2.3 Web application vulnerability assessment and the Implementation of Expert System

Web application vulnerability assessment (WAVA) is conducted to identify security loopholes which are introduced during the design, implementation or deployment of a web application (Kearns, 2010). The four main process of conducting a WAVA is shown below:

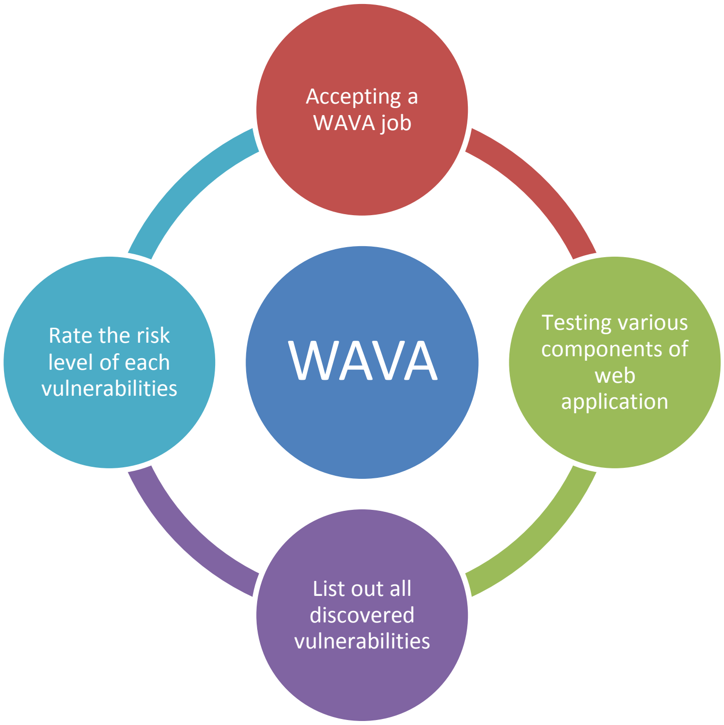
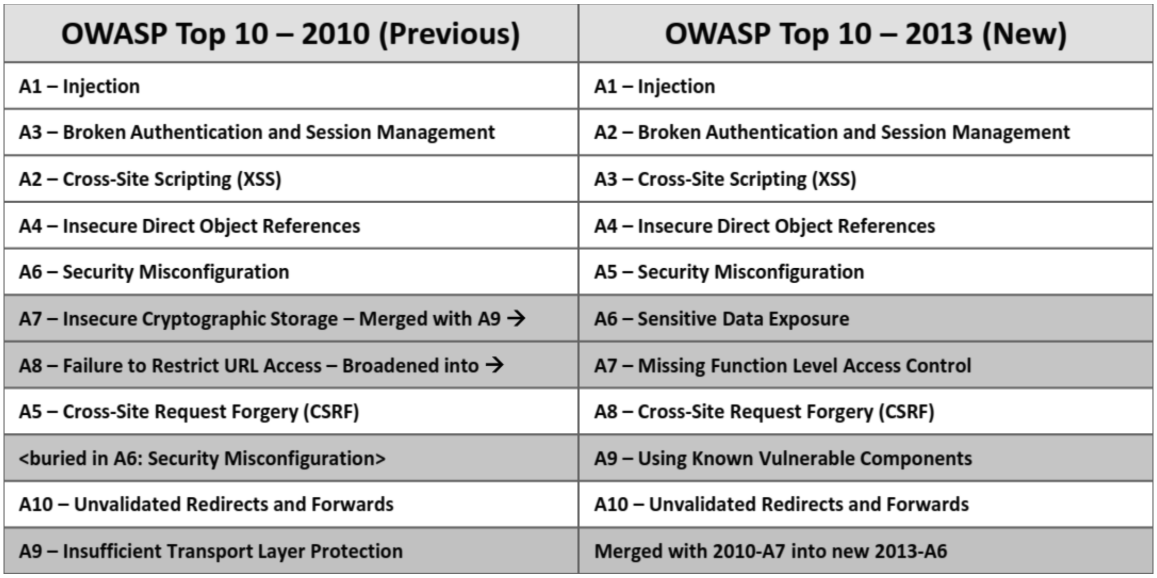

Accepting a WAVA job
Testing various components of web application
List out all discovered vulnerabilities
Rate the risk level of each vulnerabilities
WAVA

FIGURE 2.3 Life cycle of WAVA (Cheng, 2013)

The first step in conducting WAVA is to accept a job from a client which is concerned about the security of their firm. After getting the job, it will then proceed to the second phase which is to test the various components that are present in the web application.

The process requires that an information security analyst to identify functions which are critical to security and functionality of the web application, and test those functions to ensure it is functioning correctly. When all the vulnerabilities or flaws in the web application are identified, the information security analyst will need to list out all the discovered vulnerabilities. After that, the last step will be the risk assessment phase whereby all the discovered vulnerabilities will be rated a risk level based on the potential impact and severity. The cycle repeats after the risk assessment phase (Cheng, 2013).

Due to the wide scale of possible vulnerabilities in web systems, various communities had taken initiatives to research and update the most critical and prevalent security issues faced by nowadays society. The most significant initiative would be the OWASP Top Ten which depicts the most critical security issues of web systems. The figure below shows the summary of the Top Ten vulnerabilities for year 2013 as compared to year 2010.



OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Storage – Merged with A9 →	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access – Broadened into →	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6

FIGURE 2.4 OWASP Top Ten comparisons between year 2010 and 2013(OWASP, 2013)

Since Web application vulnerability assessment is a crucial aspect in any business operations as it handles the confidentiality and privacy of the operations, and the procedures to assessing risk requires experiences due to its complexity, an expert system is needed. According to Dieter Gollmann (2007) in his research paper entitled “Securing Web Applications”, it is stated that the World Wide Web had been the major and most favored platform for a wide range of services, but there had been little awareness in secure coding, which has led to increasing number of exposed vulnerabilities and attacks. Moreover due to the increasing amount of potential profit that can be gained through web applications, the number of intrusion had increased significantly.

Apart from smaller scale cyber-attacks which are aimed towards stealing of monetary resources and confidential customer information, there is also a recent state sponsored espionage happening in the Middle East Banks. According to an article published on CNN by David Goldman, the attack is conducted using a virus codenamed “Gauss” which appears to be used for tracking flow of funds. Kaspersky Lab had also identified that the virus had been capturing online bank account login credentials since September 2011. Furthermore, a more comprehensive analyze had also shown that “Gauss” had the exact same architecture as “Flame” and “Stuxnet”, which are all suspected state sponsored virus for the purpose of reconnaissance. Therefore from these cases, the importance of Web application vulnerability assessment is being highlighted to reduce the risk of unauthorized access and cyber-attacks.

2.4 Risk Assessment Phase

However, the main problem with performing a successful web application vulnerability assessment would be to accurately assess the risk level of the vulnerabilities, or in short the risk assessment phase. Risk assessment, or risk rating is a process of judging the risk levels of discovered security issues to allow a more efficient mitigation of risk (Hally, 2011). Since the level of impact and criticality level of the same vulnerability or threat may differ from one web application to the other, the process to determine the risk level would be complex and requires experiences.

Based on a paper released by OWASP in 2013, it is stated that the crucial aspects in risk assessment would be to determine the prevalence, detectability, and ease of exploit, and also to determine the technical and business impact. However, the hardest part to consider in risk assessment would be to decide on how much security risk a vulnerability or threat will present to a company. This is due to the fact that for different companies, there will be different conditions and operational process which will directly influence the risk level of the vulnerability. For the same vulnerability, the risk level may vary due to different threat agents existing in different companies, and also due to the different system setup.

The steps involved in conducting risk assessment would revolved in a cycle starting with identifying vulnerability, estimating likelihood, estimating impact, determine risk severity, and lastly deciding what to fix (OWASP, 2013). The first step of identifying vulnerability will be to determine how many and what types of vulnerabilities are present in the tested system. The second and third step will focus on determining the possible impact of risk each vulnerability will present to the system and its implication on business operation, which is the severity. The last step will be to rate each vulnerability to its respective risk level, and determine which vulnerability to be remediated first from the most critical to less critical depending on the available resources. The steps are shown below:

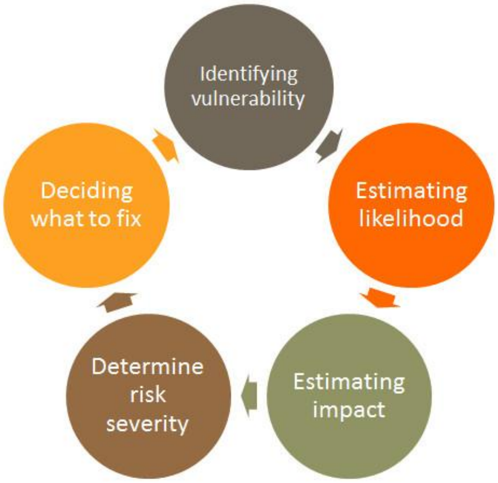


FIGURE 2.5 Risk Assessment Life Cycle (OWASP, 2013)

Therefore, to minimize the loss incurred to an organization due to vulnerabilities, which may include bugs, flaw, weaknesses that will directly leads towards a breach in confidentiality and integrity of the web system, prioritization of vulnerabilities is especially important (Zhang and Liu, 2010). Due to the huge amount of vulnerabilities and different risk scoring scales, there present a need for a standardized system that is able to recommend risk ratings based on a set of predetermined criteria and rules.

Besides, researches had also been done which substantiates the importance of having a mechanism or system to quantify risk levels to better predict the impact of vulnerabilities. Only through having a tool to quantitatively estimate risk level, an efficient and effective risk management can be carried out (Houmb et. al, 2009). However based on the research paper, it is stated that in order to quantify and estimate risk, experience-based data is especially important. This is due to the task of risk rating is a decision intensive operation, and any slight errors in the process may lead to inaccurate results. However the requirements such as experience-based data are not readily available due to the difficulty in extracting it. Therefore from this statement, it is seen that it is crucial to have a knowledge developer to extract the valuable experience-based data from the experts to enable a more comprehensive system which will aid in performing the risk rating phase in risk assessment.

Moreover, another factor which lead to a lack in experience-based data is due to the fact that the number of experts in web application vulnerability assessment is limited as the expert will need to have knowledge in both business and information technology skills, and there have been insufficient training modules provided by conventional training firms. The less experienced information system analyst will need to have alternative method to make accurate decisions in risk assessment. Therefore from this problem, expert system will come into the picture as it is able to substitute an expert in providing solution to complex problems such as risk assessment procedures.

2.5 Related Work

This section presents all the researches that had been done by previous researchers which are similar to the proposed system. Comparisons will be made to have a clearer idea on the existing proposed system so that further improvements can be done.

2.5.1 IBM ISS X-Force

The IBM ISS X-Force, or in short the X-Force database is a collection of threats and vulnerabilities that is prevalent throughout the world (Liu and Zhang, 2010). After being bought over by IBM in the late 2006, it has published over 40,000 unique vulnerabilities and threats (Frei and May, 2007). The vulnerabilities information had been collected collectively from various sources including the internet, former X-force and IBM’s own ISS software. To date, it is one of the most significant threat and vulnerabilities database available online. It employs vulnerability rating method in which each threat or vulnerability will be assigned a risk level with certain level of description of possible extent of damage.

However, due to its nature as a database, it will not be able to provide recommendation to users regarding the risk level of an uncovered vulnerability based on the systems it resides in. It will not be able to provide a risk rating based on how the vulnerability will interact with other components in the system environment. Moreover, IBM ISS X-Force is also unable to provide recommendation of remediation on how to mitigate the risk. Therefore there is still room for improvement on the current X-force system.

2.5.2 Vupen Security

Vupen Company aimed towards actively tackling system vulnerabilities by providing threat protection program to its clients who may include government bodies and enterprises. It is a security research company providing solutions to mitigate vulnerabilities risk, preventing exploitation and ensuring security policy compliance. Due to the nature of the company, it has also come out with a vulnerability rating method similar to IBM ISS X-Force.

As compared to X-Force risk rating methodology, it is more comprehensive as it divides risk into more levels, allowing a more accurate decision in choosing which vulnerability to be mitigated first. However, similar to X-Force, it also employs a qualitative method of measuring risk. Therefore, in terms of the effectiveness, it is not able to provide risk rating based on the vulnerability’s interaction with the other components in the system as well. It will require the experts working in the company to manually look into the target system and come up with their own recommendation based on their observations.

2.5.3 RAMeX (Risk Analysis and Management Xpert System)

Based on a research done by Kailay and Jarratt, they had produced a prototype expert system codenamed RAMeX, or Risk Analysis and Management Xpert system, which is meant for computer security risk analysis and management. Through the implementation of this expert system, it is hoped to be able to handle intentional threats, producing solutions and countermeasures, and to rapidly conduct informal analyses.

It implements a RAM methodology, which is the short for Risk Analysis and Management to perform a structured and logical risk analysis procedure. There will be 7 steps in the methodology, namely:

Step 1: Identification of Asset
Step 2: Identification of Threat
Step 3: Identification of Vulnerabilities
Step 4: Identification of Existing Security Countermeasures
Step 5: Business Impact Assessment
Step 6: Assessment of Security Countermeasures
Step 7: Report Generation

By using the methodology, it is attempting to perform risk analysis of computer security systems through a more logical method. However, this system will only analyze the possible risks of computer systems, and not web applications. Since nowadays most business operations are carried out online, it is important to take into account of web application security as well.

2.5.4 KMS (Knowledge Based Monitoring System)

Tseng and Wu (2007) had utilized expert system to improve stability and reliability of web services. The system being developed is named as KMS. The KMS had been implemented to predict, handle, and assess malfunctions or anomalies in web service systems. By using the expert system, anomalies such as CPU overloading or suspicious network flow can be discovered and managed properly. The expert system utilized a revised method of repertory grid test, which is the fuzzy table approach with fuzzy variables. The author implements the approach into constructing a monitoring expert system which is proven possible.

2.5.5 IDES (Intrusion Detection Expert System)

Based on a research paper entitled “A Real-Time Intrusion Detection Expert System (IDES) by Teresa F. Lunt et al., the research team had developed an expert system to observe user behavior in a monitored computer system. It will assess the activities of individuals or groups activities and flags suspicious events. The expert system is also able to observe and determine individual’s behavior pattern and discover deviation from normal pattern.

It is operated by a rule based engine which will record all known system vulnerabilities and possible intrusion scenarios, which makes IDES capable in handling exploitation by illegal third parties as well as violation of rules within the network.

2.5.6 GyMEs (Gypsy Moth Expert System)

According to a study conducted by Potter et al. (2000), the team had developed an expert system based on the rule-based knowledge representation to assess the risk of infestation of the gypsy moth in North America’s exotic forest. The risk assessment will consider the composition, structure and management objectives of the forest. The expert system will be used to determine the vulnerability of a particular forest towards infestation of Gypsy Moth.

2.5.7 Expert System for Boiler Fouling Assessment

An early research in 1995 by Afghan, Carvalho and Coelho had presented a concept of expert system to handle boiler fouling assessment. The expert system is developed to assess the formation of deposits on the boiler’s heat transfer surface. It uses a rule based system with specific criteria for the fouling assessment. The diagnostic variables being used in the expert system includes the rate of change of radiation heat flux ratio, the efficiency of the boiler’s heat transfer surface, deposit thickness and so on. This expert system will contribute to the mitigating of the deposit formation on the boiler.

In short, from the previous researches contributed by various researchers, it can be seen that expert system can help in the decision making and problem solving of complex domains. Moreover there have been several researches that had been done to prove that expert system is able to assist in assessment of computer and web systems. Therefore in order to rectify the issue of the steep learning curve of risk assessment process in Web application vulnerability assessment, there will be a need to further research on the usage of expert system in the field of assessing risk level of vulnerabilities and threats in web applications.

CHAPTER 3

METHODOLOGY

3.0 Introduction

This section will highlight on the system design model used in this research. A specific model which is meant for expert system, the expert system development life cycle will be described in detail together with the project activities that has been carried out throughout this project. Apart from the system design, the system architecture of the proposed expert system will also be mentioned in this section together with the Gantt chart and its key milestones.

3.1 Expert System Development Life Cycle

The methodology that has been utilized to design and develop the expert system to support the risk assessment phase is the expert system development life cycle (ESDLC). There are seven steps in the ESDLC, which includes problem identification and analysis, determining system specification, selection of development tool, building the knowledge base, developing prototype system, testing and validation, and lastly implementation. The summary of the seven steps is being shown in the diagram below:

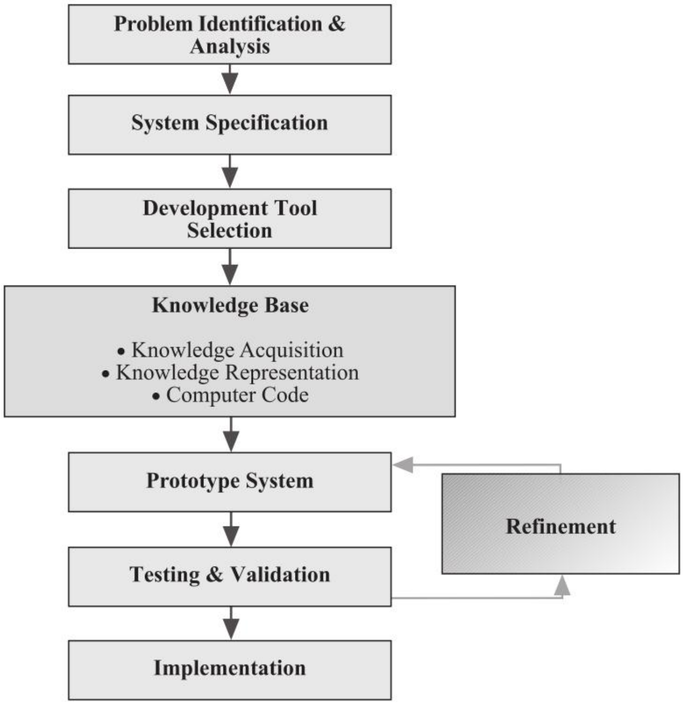


FIGURE 3.1 Expert System Development Approach (Kostas, John and Dimitris, 2002)

3.1.1 Problem Identification and Analysis

For the first step in building an expert system, the knowledge developer had first identified the possible scenarios and problems that the expert system will handle. The impact of the problem with and without expert system had also been analyzed to determine the need for the development of expert system. Together with problem identification, the requirement analysis is completed by the knowledge developer. The output for this step is the identified problem and the requirements gathered.

In the requirement analysis procedure, the knowledge developer had interviewed various information security analysts to have a clearer picture of the current process of performing risk assessment. The results of the interviews are being highlighted in the next section of the report. By having a clearer understanding, the developer will be able to gather and analyze the specifics of the target users, the various functions of the system as well as the limitations of the system. After performing the analysis, it is determined that the target user should be the less experienced information security analyst, and the functions of the expert system will only be to provide recommendations on the risk assessment phase of WAVA which is limited to vulnerabilities stated in OWASP Top 10 2013. This is to ensure the scope of the project can be achieved within the time frame provided.

As for the second achievable in this step, it would be the identification and confirmation of problem. Therefore to conduct this step, interviews has been conducted with information security analysts. The knowledge developer has determined the eligibility of the problem and objectives through the interactions with the information security analyst. In this step, another method which is literature survey has also been conducted as well to find past related research papers to determine the various researches that had been done previously which relates to building expert system to tackle the problem of risk assessment in web application vulnerability assessment. The research papers are retrieved from online repositories such as Scopus, Google Scholar, and Science Direct.

Moreover, a small scale pilot study had also been conducted with a small group of experts to determine the problem. The use of questionnaires had been chosen as the method of communication to gather the required information and knowledge from the experts regarding the eligibility of the proposed problem. Due to the nature for distributing the questionnaires which is aimed towards only the expert information security analyst, the number of respondent will be limited.

3.1.2 System Specification and Development Tool Selection

After identifying the problems, the following step would be to select the system of choice as well as the tools that will be most appropriate to handle the development phase. In this step, the hardware and software that will be used in the development phase will be chosen. The knowledge developer has selected Notepad++ as the software of choice due to its capability and simplicity. As for the hardware or system specification, it will need to be able to handle the software’s requirement.

3.1.3 Tools

As mentioned in the previous step, the software tool that will be used is Notepad++. This is mainly due to the software's capability in handling programming of the required rule engine or inferencing engine. It has a cleaner but much efficient coding interface as compared to other software and tools such as the normal notepad which is the conventional tool used for javascript and rule programming. Since the expert system will be implemented in a web-based html environment, this software allows a much simple interface to work on the building of website using html scripts and php coding language.

Based on the Notepad++ website's official system requirement release, in order to run the software efficiently, the minimum requirement for the system specification will be:

TABLE 3.1 List of requirements to run Exsys Corvid

System	Requirement
Operating System	Windows XP/Vista/7/8
Internet Browser	Internet Explorer 6 or higher
Hard Disk	11MB free space
Screen Resolution	As long as the software is able to run on the stated operating system

3.1.4 Knowledge Base

After the software and hardware tools for developing the expert system were selected, the knowledge developer proceeded to the next step which is the construction of knowledge base. In this research, the knowledge base will comprised of the related knowledge relating to determining the risk rating and risk assessment of vulnerabilities.

This step will be divided into three main parts, which is first the knowledge acquisition, followed by knowledge representation, and lastly computer code. Through this step, the expert's knowledge will be captured and represented in the knowledge base.

3.1.4.1 Knowledge Acquisition

To acquire related knowledge in the problem domain, experts in the related field have been chosen. In order to gather the required knowledge from the experts regarding the risk assessment procedures, interviews were conducted with several information security analysts from professional audit firms such as PricewaterhouseCoopers and Deiloitte who have their own technical vulnerability management teams. The experts were contacted via phone calls and e-mails to schedule a meeting to discuss on the risk assessment procedures.

Related information regarding risk assessment is also acquired from the internet through the Open Web Application Security Project's documents on risk assessment. This is due to the fact that the open source community is the most prominent figure in web application vulnerability assessment, which has served as a guide for many information security firms.

By acquiring the related knowledge, the expert system will be able to perform a much accurate risk rating as more facts and rules can be added. This is because a more comprehensive risk assessment can only be done with enough knowledge, and the inference engine utilizing the knowledge base can make a more relevant and accurate decision.

3.1.4.2 Knowledge Representation

After the knowledge is acquired from the experts, the captured knowledge will then be represented through the system. The knowledge developer has chosen the more commonly used forward reasoning algorithm to construct the expert system. This is to ensure user friendliness of the system as well as to ease the construction of expert system using a more commonly used approach. The expert system will collect information from the users to be inferred by the inference engine using the rules and facts and come up with the goal, which is the risk level of the respective vulnerabilities.

3.1.4.3 Computer Code

In the final step of the construction of knowledge base, the rules derived from knowledge representation were coded as computer codes. The “IF…THEN” statement were codified as a form of code in the software used, which leads to the possibility of getting results and goals from the “IF…THEN” rules. This is due to the fact that rule is a formal way of specifying a recommendation, directive, or strategy, expressed as a premise and conclusion.

By having the rules being coded in place, the expert system developed will be able to provide recommendation to the users regarding the risk ratings of vulnerabilities after collecting required information from the users.

3.1.5 Prototype System

After the completion of the knowledge base, it is being incorporated into the expert system to allow it to communicate with users. Through the user interface of the prototype, the end user will be able to communicate with the prototype and obtain recommendations derived from the knowledge base using the inference engine. The user will obtain the solution from the expert system which aids the user in his decision making process.

3.1.6 Testing and Validation

The testing and validation phase has been conducted by a selected group of information security analyst who had been participating in the questionnaires and interviews. To ensure the system works correctly, the prototype are to be tested, verified, validated and evaluated.

The testing phase is divided into two phases, whereby the first phase will be the assessment and evaluation phase, and the second will be verification and validation phase. For assessment and evaluation phase, the main aim for the testing is to ensure the user-friendliness of the system as well as the system's response time. Three criteria that are being taken into account is the user friendliness in terms of font used and user interface, ease of navigation, and smoothness of the system. The first phase is carried out to test the usability of the system which is considered as a simpler and surface testing. A total of twenty users are participating in this phase, including seven experts from PricewaterhouseCoopers and Deiloitte, as well as thirteen less experienced information security analysts comprised of interns and fresh employees.

As for the second phase of the testing, it is further divided into three categories, which is the accuracy of knowledge base, completeness of knowledge base, and condition-decision matches testing.

Accuracy of knowledge base is verified by allowing the experts to go through the more important rules which the ones are involving vulnerabilities which are more common place and have the greatest impact if deemed inaccurate. This includes the top five vulnerabilities in the list which are SQL injection, broken authentication and session management, cross –site scripting, insecure direct object reference, and security misconfiguration. The decision tree used for the construction of the expert system is shown to the experts, and they will determine the percentage of decisions which is acceptable in their perspective. The experts who are involved in developing the rules are exempted from determining the accuracy of the rules they participated in developing. All experts will be participating in determining the accuracy of rules developed by knowledge gathered from internet sources.

As for completeness of knowledge base, it is aimed towards determining whether all the conditions and consequences are being included in the expert system. The experts had gone through the questions stated in the expert system to determine whether all possible scenarios faced during web application vulnerability assessment has been included into the system. The experts then rated the completeness of possible scenarios for each of the top ten vulnerabilities. The ratings from each expert are then total up and divided accordingly to obtain the average rating for this category of testing. This is to ensure the system is able to guide the less experienced information security analyst to determine the risk rating in whichever scenario.

Lastly, condition-decision match testing is to decide whether the results of the expert system are correct when put under real life situation. The experts had been invited to test on this matter by comparing the decisions generated by the expert system to the decisions made by the experts on the risk ratings, by providing the same information and conditions. The testing result depends on the similarity between the decisions made by the experts and the expert system. For this test, the less experienced information security analyst utilized the prototype while the experts determine the risk rating decisions through their experience. A total of 30 real life vulnerabilities are being tested during the validation process.

After the testing is completed, the expert system is deemed fit to be used by the end users.

3.1.7 Implementation

In this final step, the expert system being developed will be implemented and made available to the end users. During implementation, the process of organizing knowledge and integrating with existing procedures will be conducted.

Therefore the expert system will be deployed for use of risk assessment in web application vulnerability assessment.

3.2 System Architecture

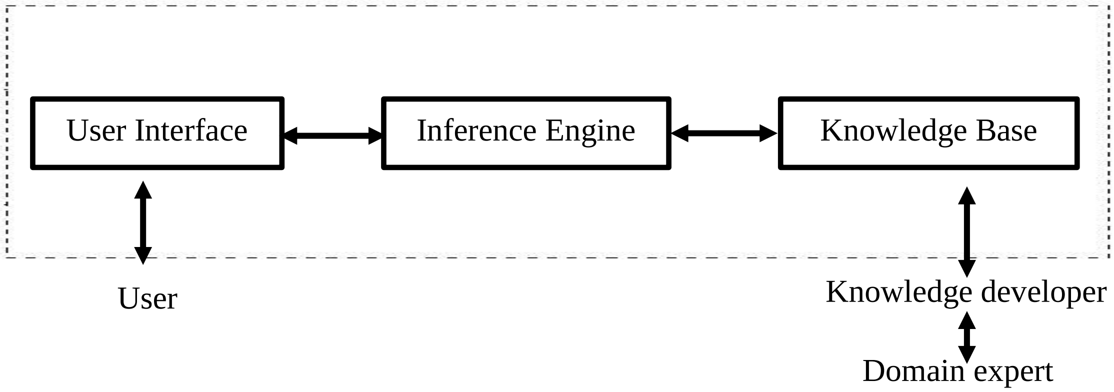


FIGURE 3.2System architecture of expert system

The diagram above shows the system architecture of the proposed expert system. The expert system consists of three main parts which is the knowledge base, inference engine and the user interface. The knowledge base is the repository of rules and facts obtained from the expert information security analysts. The knowledge developer which is the author of this research paper will be extracting the knowledge and codify it as rules into the knowledge base for the expert system.

During the actual runtime of the expert system, the system users which are the less experienced information security analysts will be interacting with the user interface residing in a client computer which has access to the expert system. The interface will obtain the needed information to provide a recommendation of the risk rating by asking the users in the form of multiple choice questions or subjective questions. The information obtained will then be passed to the inference engine to produce appropriate recommendations based on the knowledge base. After the information is processed by the inference engine, the recommendation will be passed back to the users in the user interface.

During the runtime of the system, there will be no involvement of the knowledge developer and the domain expert. The ones involved will only be the users of the system, knowledge base, inference engine, and the user interface. The knowledge developer and domain expert will only be involved during the maintenance or upgrading of the expert system.

3.3 Gantt Chart and Key Milestone

Project Activities	Date													
	20/5	27/5	3/6	10/6	17/6	24/6	1/7	8/7	15/7	22/7	29/7	5/8	12/8	19/8
Brainstorming ideas	▨	▨												
Literature Survey			▨	▲										
System specification and development tool selection			▨	▲										
Questionnaire creation and distribution			▨	▨	▨	▲								
Interview experts				▨	▨	▨	▨	▨	▨	▲				
Collection and analyzing of knowledge, information acquired							▨	▨	▨	▨	▨	▨	▲	
Interim report submission														▲

TABLE 3.2 FYP I Gantt Chart

The above diagram shows the Gantt chart of the respective activities done and the important dates. Each triangle in the Gantt chart represents the completion of each activity and also serves as a key milestone of the project. Since the Gantt chart above is only representing the schedule of FYP 1, it will not be showing the date of completion of the prototype development as it is expected to be completed only during FYP 2. Besides, as for the interviewing expert's activity, it is only an estimated date of completion as the expert system development life cycle requires the knowledge developer to continuously approach the experts to clarify regarding the accuracy of the knowledge base. Therefore the interview date may span longer than expected.

Project Activities	Date													
	23/9	30/9	7/10	14/10	21/10	28/10	4/11	11/11	18/11	25/11	2/12	9/12	16/12	23/12
Literature survey	▨	▨	▨	▨	▨	▲								
Interview experts		▨	▨	▨	▨	▲								
Construction of knowledge base	▨	▨	▨	▨	▨	▲								
Prototype development	▨	▨	▨	▨	▨	▨	▨	▨	▨	▲				
Testing and validating prototype	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▲	
Final report submission														▲

TABLE 3.3 FYP II Gantt Chart

The Gantt chart above shows the activities that will be conducted during FYP 2. It is the continuation of the activities conducted during FYP 1. The summary of the project activities, its methods and deliverables are summarized as followed:

Project Activities	Methods	Deliverables
Literature survey	• Online search • Journal readings	• Background studies on expert system, web application vulnerability assessment, and use of expert systems in web security assessment.
Interview experts	• Interview • Questionnaires	• Knowledge regarding the proper way to conduct risk assessment on web application vulnerability assessment in order to construct the knowledge base.

Construction of knowledge base	• Use of software	• A knowledge base covering the knowledge regarding risk assessment of vulnerabilities listed under OWASP Top 10 2013.
Prototype development	• Use of software	• A complete prototype which fulfills the objectives stated earlier in this paper.
Testing and validating prototype	• Alpha testing by developer and beta testing by related experts	• A comprehensive testing on the prototype including testing of the knowledge base, as well as the testing on the performance of the system.

CHAPTER 4

RESULTS AND DISCUSSION

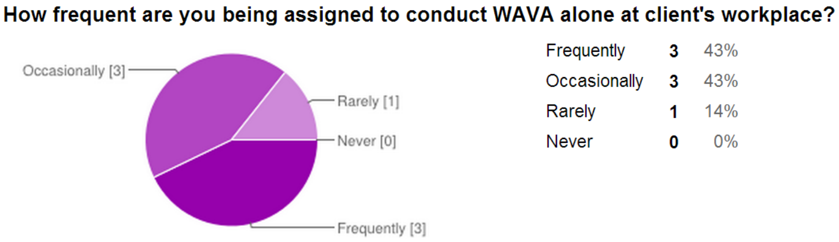
4.0 Introduction

This section of the report will be discussing about the results obtained from the various phases in the research. It includes all results from the pilot study, the interviews, results of collected knowledge in the form of decision tree, and prototype design.

4.1 Pilot Study

Due to the nature of the research, the pilot study will involve distributing questionnaires to the expert information security analyst to determine the eligibility of the problem, as well as some background information on the information security analyst. However since the number of experts are limited, the number of respondents will be limited to only seven experts from different firms which had specialized teams working on web application vulnerability assessment. This pilot study only serves to understand the problem, and due to the small number of experts, interviews will also be carried out with some of the analysts individually. However, the result of the individual interviews will not be included in the pilot study as it will be shown in the actual research result which is used for the construction of knowledge base of the expert system.

The pilot study is being conducted with a group of seven experts from PricewaterhouseCoopers and Deloitte, whose position ranged from associate to manager. Questionnaires are being distributed to the seven of them which all of them had responded Their age group is from 20-25 until 30-40 years old, but the majority of the respondents are between ages 20 to 30, with more than three years of experience performing web application vulnerability assessment. Moreover from their responds in the questionnaire, most of them are comfortable with performing the risk assessment phase alone, which makes them suitable candidates of being the expert in the field as they are not the ones referring to others, but others are referring to them for answers. The results of the rest of the questionnaire of the pilot study are highlighted below:

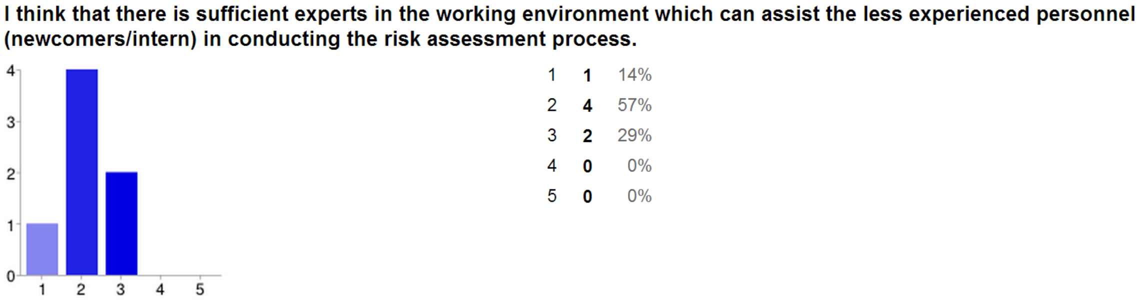


How frequent are you being assigned to conduct WAVA alone at client's workplace?

Frequently	3	43%
Occasionally	3	43%
Rarely	1	14%
Never	0	0%

FIGURE 4.1 Pilot study question 1

The above question asked about the frequency of the information security analyst being out stationed alone at the client's workplace to perform WAVA. From the result above, it can be seen that majority of them have been frequently assigned alone at the client's workplace. According to the interview with the experts, most of the information system analyst will be stationed at the client's place at well, regardless if they are experienced or less experienced due to lack of manpower. As for the other 3 person who answered occasionally, those are the ones who have been promoted to managerial or assistant manager positions, which reduce the need for them to personally performed WAVA instead of conducting managerial role. From this result, it can be seen that there is indeed a lack of experts to be refer to if a less experienced information security analyst is to be assigned alone at the client's workplace due to lack of human resource. Therefore, there is definitely a need for an expert system to assist the less experienced analyst to perform a much accurate risk assessment.

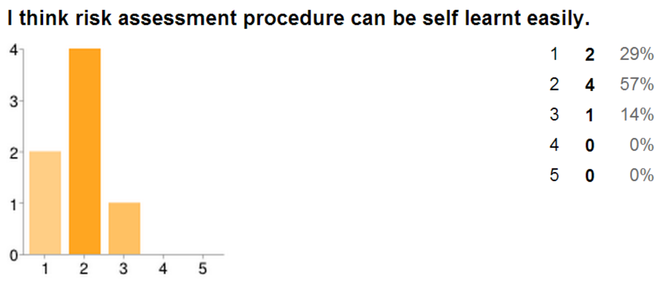


I think that there is sufficient experts in the working environment which can assist the less experienced personnel (newcomers/intern) in conducting the risk assessment process.

1	1	14%
2	4	57%
3	2	29%
4	0	0%
5	0	0%

FIGURE 4.2 Pilot study question 2

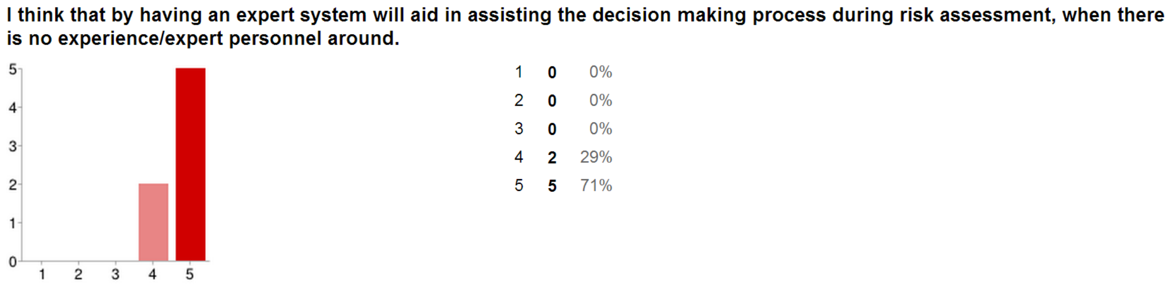
The above question enquires about the expert’s opinion on the availability of experts in the field that may assist the less experienced analyst. The scale is rated as 1 being strongly disagrees and 5 being strongly agree. From the results obtained, it is seen that most of the experts disagrees that there are sufficient experts that can aid the less experienced personnel. This further substantiates the previous question whereby most personnel are being assigned individually to the client’s workplace. Due to the lack of experts, the less experienced analyst may face difficulty in performing accurate risk assessment as the process requires experiences as mentioned before. Therefore from this result, it is seen that there is a need of having an expert system that will assist and recommend the less experienced analyst to perform risk assessment accurately.


I think risk assessment procedure can be self learnt easily.

1	**2**	29%
2	**4**	57%
3	**1**	14%
4	**0**	0%
5	**0**	0%

FIGURE 4.3 Pilot study question 3

The above question clarifies with the experts regarding their opinions on whether risk assessment can be self learnt easily, with 1 being strongly disagree and 5 strongly agrees. From the results obtained, it can be seen that majority of the respondents have simultaneously disagrees that risk assessment procedure is something that can be self learnt easily. This is mainly due to the fact that risk assessment is a process that needs to be based on an individual’s experience to be able to judge accurately. Therefore if a less experienced information security analyst is being assigned individually to a project without having any experts to assist him due to resource restriction, the accuracy and reliability of the testing result may not be satisfactory. From this situation, it is safe to say that an expert system is needed to substitute an expert who have years of experience in performing risk assessment to ensure the less experienced analyst can obtain proper recommendations and be able to learn to do it the correct way.



I think that by having an expert system will aid in assisting the decision making process during risk assessment, when there is no experience/expert personnel around.

1	**0**	0%
2	**0**	0%
3	**0**	0%
4	**2**	29%
5	**5**	71%

FIGURE 4.4 Pilot study question 4

The last question as shown above enquires about the expert's opinion on whether or not it is a good idea to have a system that will assist the less experienced analyst. The results obtained from the experts are mostly positive as they think that by having an expert system, it will be able to solve the problem of insufficient experts. Since expert systems are able to mimic an expert's stream of thoughts when solving a particular problem, the less experienced analyst will be able to refer to the system instead of an expert. This will in turn solve the problem of having insufficient experts and be able to make a sound decision in rating the risk of each vulnerabilities discovered.

In short, based on the pilot study conducted towards a group of experts, it can be summarized that there is indeed a problem of insufficient experts in the field that will hinder the success of WAVA. Moreover it is also stated that by having an expert system that is able to mimic the thoughts of an expert, it can be useful in assisting the less experienced information security analyst. Therefore from the pilot study, it has proven that there is a need for an expert system that is able to aid the less experienced analyst so that a more accurate WAVA can be conducted, which in turn provides a more secure web application to any given organization.

4.2 System Flowchart

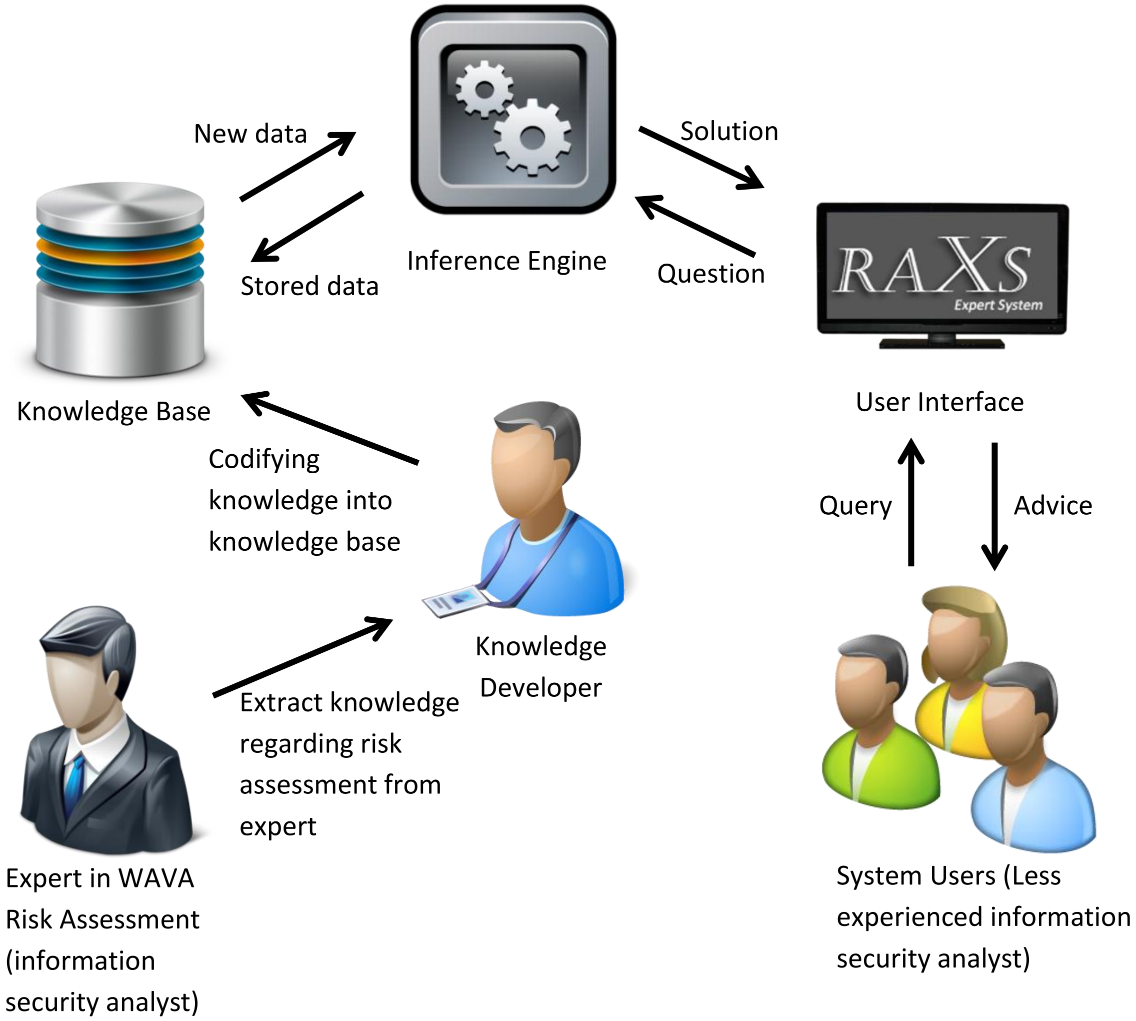


FIGURE 4.5 Flowchart of expert system

The system flow chart above shows how the expert system is being operated. During system runtime, the users will input information as requested by the expert system, and the expert system will generate the risk rating by utilizing the inference engine as well as the knowledge base.

As for the knowledge itself, the knowledge developer will update the knowledge base's rules and facts through the knowledge developer's assistance. Thus the knowledge in the expert system can be updated.

4.3 Prototype

The prototype of the research project will focus on developing an expert system. Therefore the main parts in the prototype will be the knowledge base, user interface and the inference engine. In this research paper however, the knowledge retrieved from the experts will be displayed in decision trees for easier reference.

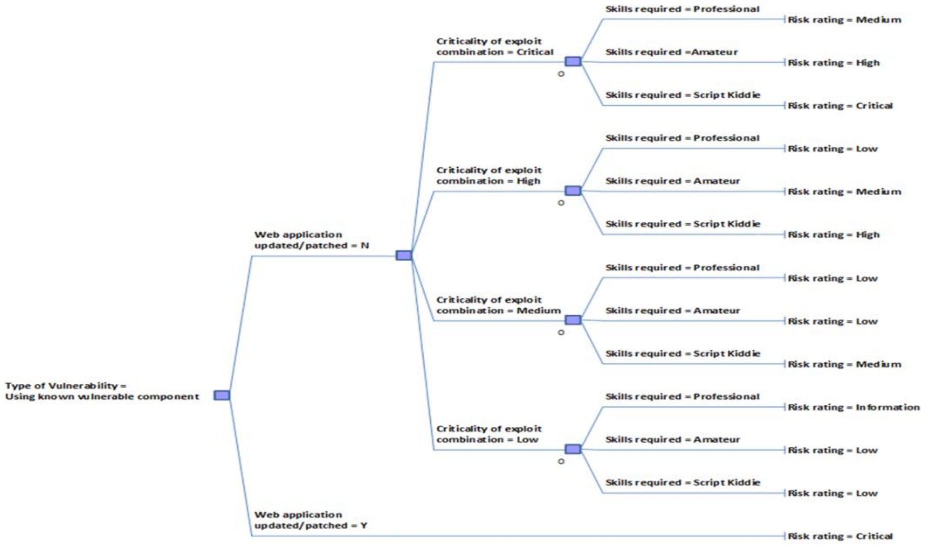
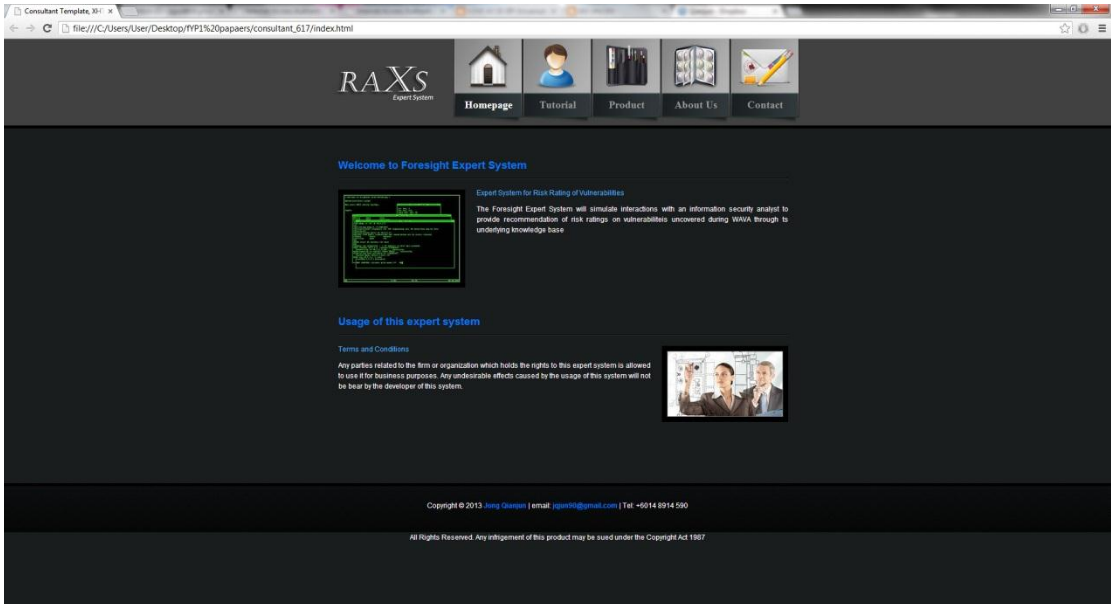

Type of Vulnerability = Using known vulnerable component
Web application updated/patched = N
Web application updated/patched = Y
Criticality of exploit combination = Critical
Criticality of exploit combination = High
Criticality of exploit combination = Medium
Criticality of exploit combination = Low
Skills required = Professional
Risk rating = Medium
Skills required =Amateur
Risk rating = High
Skills required = Script Kiddie
Risk rating = Critical
Skills required = Professional
Risk rating = Low
Skills required = Amateur
Risk rating = Medium
Skills required = Script Kiddie
Risk rating = High
Skills required = Professional
Risk rating = Low
Skills required = Amateur
Risk rating = Low
Skills required = Script Kiddie
Risk rating = Medium
Skills required = Professional
Risk rating = Information
Skills required = Amateur
Risk rating = Low
Skills required = Script Kiddie
Risk rating = Low
Risk rating = Critical

FIGURE 4.6 Sample decision tree to represent knowledge

Additional decision trees used for the expert system are being recorded at the appendix section of this research paper. The decision tree is separated into ten different trees for easier reference and each tree will represent one type of vulnerabilities out of the top ten vulnerabilities.

As for the interface of the expert system, the completed user interface for the RAXS expert system will be as followed:



Welcome to Foresight Expert System

Expert System for Risk Rating of Vulnerabilities

The Foresight Expert System will simulate interactions with an information security analyst to provide recommendation of risk ratings on vulnerabiliteis uncovered during WAVA through ts underlying knowledge base

Usage of this expert system

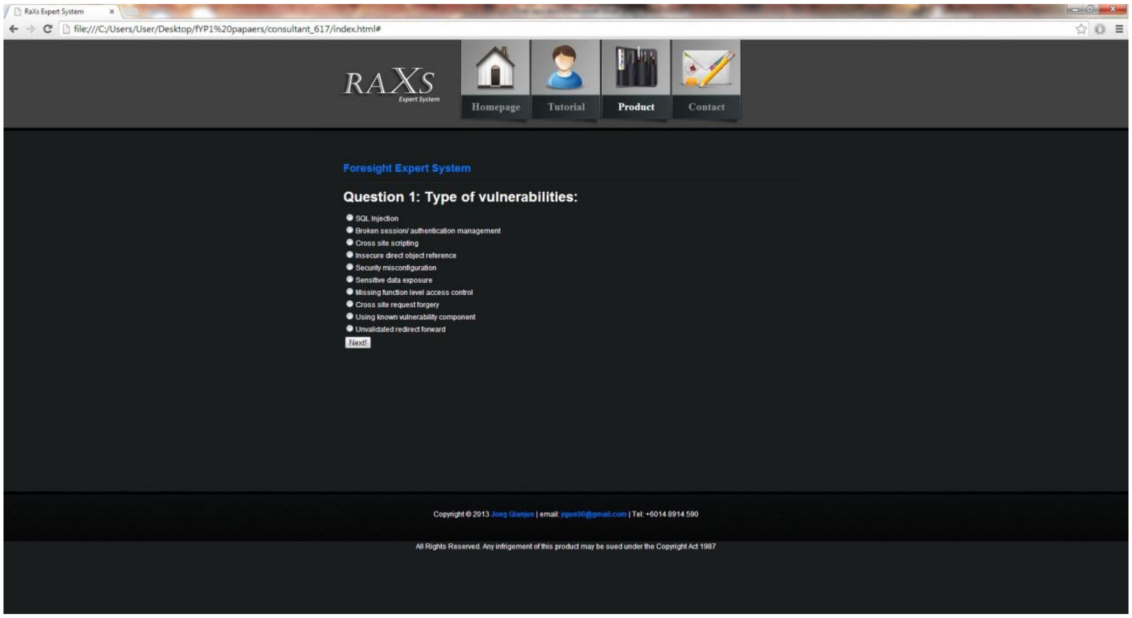
Terms and Conditions

Any parties related to the firm or organization which holds the rights to this expert system is allowed to use it for business purposes. Any undesirable effects caused by the usage of this system will not be bear by the developer of this system.

Copyright © 2013 Jong Qianjun | email: jqjun90@gmail.com | Tel: +6014 8914 590

All Rights Reserved. Any infrigement of this product may be sued under the Copyright Act 1987

FIGURE 4.7 Homepage of expert system


RaXs Expert System
file:///C:/Users/User/Desktop/fYP1%20papaers/consultant_617/index.html#
RAXS
Expert System
Homepage
Tutorial
Product
Contact

Foresight Expert System

Question 1: Type of vulnerabilities:

○ SQL Injection
○ Broken session/ authentication management
○ Cross site scripting
○ Insecure direct object reference
○ Security misconfiguration
○ Sensitive data exposure
○ Missing function level access control
○ Cross site request forgery
○ Using known vulnerability component
○ Unvalidated redirect forward

Next!

Copyright © 2013 Jong Qianjun | email: jqjun90@gmail.com | Tel: +6014 8914 590

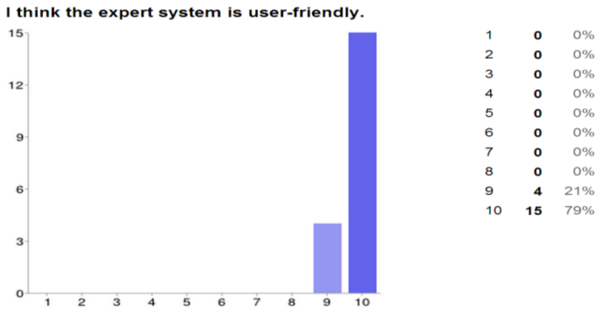
All Rights Reserved. Any infrigement of this product may be sued under the Copyright Act 1987

FIGURE 4.8 Interface of the expert system

4.4 Prototype Testing

The prototype testing phase is being divided into two phases, which is assessment and evaluation phase as well as verification and validation phase. For the first phase of testing it will be carried out by seven experts from PricewaterhouseCoopers, Deiloitte, and thirteen of the less experienced information security analysts which are consisted of either interns or fresh employees who have limited experiences in risk assessment. As for the second phase of testing, it will only be carried out by the experts as they are the ones having the knowledge to assist in verifying and validating the effectiveness of the knowledge base.

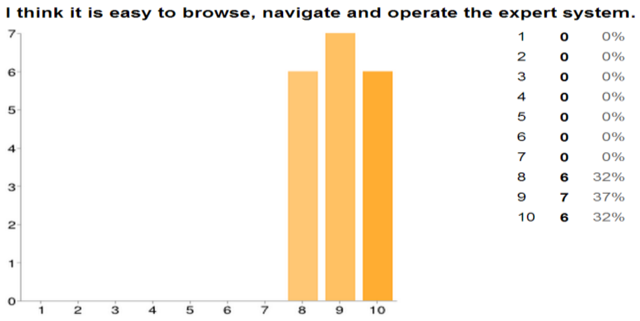
4.4.1 Assessment and Evaluation Testing



1	0	0%
2	0	0%
3	0	0%
4	0	0%
5	0	0%
6	0	0%
7	0	0%
8	0	0%
9	4	21%
10	15	79%

FIGURE 4.9 Prototype testing question 1

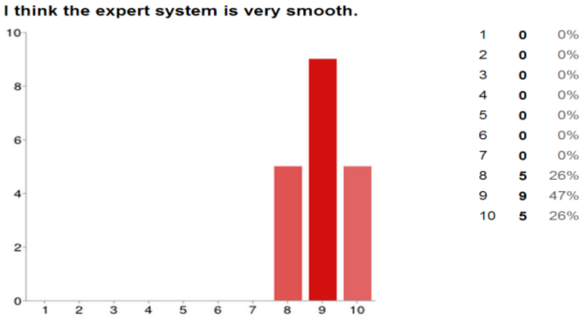
The first question requires the respondent to express their opinion regarding the user-friendliness of the expert system whereby one means not user-friendly at all and ten represents very user-friendly. Based on the responses acquired from the respondents, it is seen that a majority of them accounting to 79% agrees that the expert system is user friendly. This is due to the fact that during the design of expert system, effort is being made to take into account the learning curve of using the expert system. It is made to be as simple as possible using all the buttons and symbols which is familiar to the users, and the color scheme used has also been taken into consideration.



1	0	0%
2	0	0%
3	0	0%
4	0	0%
5	0	0%
6	0	0%
7	0	0%
8	6	32%
9	7	37%
10	6	32%

FIGURE 4.10 Prototype testing question 2

The second question is regarding the ease of navigation of the expert system where one is rated as hard to navigate and ten for easy to navigate. For this testing, it is aimed at understanding whether or not it is easy to browse through the system to get the required information or to operate the expert system as intended. Due to the existence of tutorial, guideline to let the users understand how the expert system operates in the tutorial tab of the system, most of the users find it easy to navigate around the expert system. Thus from the result, it can be seen that majority of the users find the expert system easy to navigate as all of the users choose between eight to ten on the likert scale.

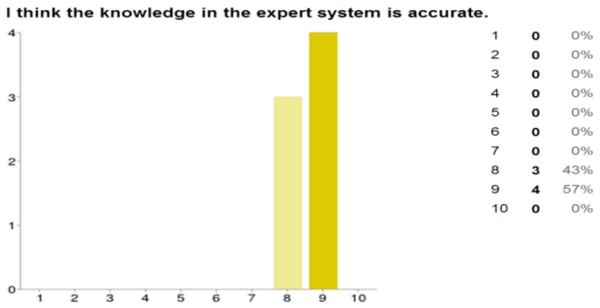


1	0	0%
2	0	0%
3	0	0%
4	0	0%
5	0	0%
6	0	0%
7	0	0%
8	5	26%
9	9	47%
10	5	26%

FIGURE 4.11 Prototype testing question 3

For the third question, it is regarding the performance of the expert system where one is regarded as not smooth while ten is very smooth. For any system, the smoothness of the system is a given, and if a system’s performance is bad and lags a lot, no matter how well the functionality is, the system is deemed a failure. Thus for the prototype testing, the performance of the system is being tested as well by allowing the users to test the response time and smoothness of the system. From the result, it can be seen that most of the users find that the system is acceptable in terms of performance. However there have been few comments regarding the use of fading transitions between tabs and questions which makes the usage of the system less convenient thus giving a slightly lower rating of eight. However there are also those which states that the usage of fades and transitions actually makes good eye candies for the users. Therefore the developer had taken into consideration the ideas but remain the design of the system as majority of the users find the system performance acceptable (74%) compare to the ones who does not (26%).

4.4.2 Verification and Validation Testing



1	0	0%
2	0	0%
3	0	0%
4	0	0%
5	0	0%
6	0	0%
7	0	0%
8	3	43%
9	4	57%
10	0	0%

FIGURE 4.12 Prototype testing question 4

The fourth question of the prototype testing is conducted with only the experts to determine the accuracy of the expert system. In the question, rating one is rated as least accurate whereas rating ten is most accurate. The results obtained are based on the ratings given by experts after going through the decision process of the expert system of the top five most impactful and common vulnerabilities in the expert system. From the result, it can be seen that most of the experts have given ratings higher or equal to eight. This is mainly due to the fact that the rules are constructed based on the expert’s recommendations with modifications after performing researches online to suit a wider range of users working in different environment, as some of the rules are more applicable to the expert firm’s requirement on a stricter rating.

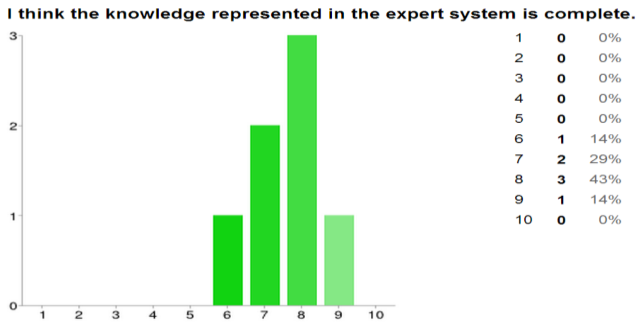


FIGURE 4.13 Prototype testing question 5

The fifth question of the prototype testing focuses on the completeness of the expert system whereby one represents incomplete and ten as completed. Based on the result obtained, it is seen that the ratings given are more spreaded as compared to the other questions. This is due to some experts thinking that the expert system should address the interactions between vulnerabilities instead of just focusing on individual vulnerabilities. For a web application, there may be a possibility of different vulnerabilities which seems unrelated, actually compromises the security of the system even further when putting them together in a single system. Although the point stated by the experts is valid, it is not included in the current project’s scope. However it is a good starting point for future works related to this field.

For the last part of the testing, it is the condition-decision testing whereby both experts and the less experienced information security analysts work together. In this testing, the experts have been generous in providing assistance in the testing by providing real-life risk assessment testing. The experts have provided thirty real-life situation involving risk assessment for the testing process whereby the experts will determine the risk ratings of the vulnerabilities using their experience while the less experienced ones were provided with the expert system. From this testing, it is seen that 76% of the decisions made by the experts and the less experience analysts actually matches. Therefore it can be seen that the expert system is quite reliable as the success rate is within the acceptable range.

CHAPTER 5

CONCLUSION AND RECOMMENDATION

5.1 Conclusion

The recent incidents that had happened around the world has delivered a crystal clear message to the world, that is no organization can be safe from illegal parties without putting extra efforts in securing their web applications. The world has evolved to a new generation whereby business and the society have moved to the online network. However this advancement does not come without a price as the risk of compromisation of web security has also increased. This is due to the fact that whenever there is profit, there will be crime. Therefore it is crucial to have a better risk assessment system to aid the less experienced information system analyst in the web application vulnerability assessment to ensure its completeness and accuracy.

However, as for the research itself, it has definitely achieved its objective of developing an expert system that will aid the less experienced information system analyst to perform risk assessment during the absence of the experts. With the help of the experts in the field, the system will be able to cover the risk assessment for the latest Top 10 vulnerabilities prevalent in the world. Nevertheless, the expert system being developed will only be effective for the current period and will require constant updating as new vulnerabilities may be discovered every day and sooner or later, the knowledge contained in the expert system may become obsolete.

In short, to ensure a better future for mankind where everyone is able to trade freely and communicate without worries in the online virtual world, it will be crucial for web application vulnerability assessment to be carried out effectively, which requires an efficient risk assessment process. Only with a much secure system, only then the nation is able to become a developed state where economy knows no boundaries and trading can be conducted much freely.

5.2 Future Work

As mentioned in earlier sections, the risk assessment of a web application's security is a continuous process which requires constant checkup. Due to new vulnerabilities being exposed constantly, the knowledge base of the expert system will also need to be updated to ensure its accuracy and reliability. Even though for this project, the expert system is developed based on the latest document regarding web application vulnerabilities, which is the OWASP Top Ten 2013, due to the advancement of technology and ever evolving creativity of mankind, the knowledge will definitely become obsolete in a few years' time. Moreover, to more effectively address the possible threats towards the web application, the scope of the expert system should definitely be increased to cover more possibilities of attack.

Therefore to ensure the reliability of the expert system, there will be much more to be done in the future as researchers will need to be constantly aware of the updated vulnerability documents through experts, and update the knowledge base accordingly. In the future, more vulnerabilities and solutions need to be added into the system to ensure the system is able to detect the newer vulnerabilities and able to perform the appropriate risk ratings. Thus for the future work, it would be much more effective if the expert system will allow new rules to be added more conveniently to ensure the expert system is constantly updated.

Only by constantly monitoring the dependability and reliability of the system, only then the expert system can be functioning optimally and effectively.

REFERENCES

Afghan, N., Carvalho, M. G. & Coelho, P. (1995). Concept of Expert System for Boiler Fouling Assessment. *Applied Thermal Engineering.* Vol.16 No.10.

Award, Elias M., I. (1995). Building expert system: principle, procedures, and application. *MN, United State of America: West Publishing Company.*

Bohanec, M. et al. (1983). An Expert System for Decision Making. *Processes and Tools for Decision Support.*

Chabrow, E. (2013, October). Analyzing IT Security Employment Stats. Retrieved November 1st, 2013 from http://www.bankinfosecurity.com/blogs/analyzing-security-employment-stats-p-1570

Choi, J. (2002). A Rule -Based Expert System Using an Interactive Question-and-Answer Sequence. Retrieved June 19, 2013 from http://www.ucgis.org/summer2002/choi/choi.htm

Delaney, J. & Forsyth, G. (2000). *Using XML and Other Techniques to Enhance Supportability of Diagnostic Expert Systems.* Pp. 380-390.

Duan, Y. (2009). Web-Based Expert System. *IGI Global, Web Technologies.*

Ethical Hacking and Countermeasures (CEH). Retrieved June 19, 2013 from http://www.eccouncilacademy. org

Exsys Corvid System Requirement. Retrieved June 25, 2013 from http://www.exsys.com/pdf/Corvid_ITOverview.pdf

Frei, S. & May, M. (2007). Putting Private and Government CERT's to the Test. *ZISC Information Security Colloquium.*

Garner, R. (2013, April). Hack to the future: Corporations, military recruit ethical hackers to fend off Cyberattacks. Retrieved June 19, 2013 from http://www.schools.com/articles/ethical-hackers-recruited-corporations-military.html

Giurca, A. & Pascalau, E. (2009). *A Lightweight Architecture of an ECA Rule Engine for Web Browsers.*

Goldman, D. (2012, August). *Cyberweapon targets Middle East bank accounts*. Retrieved June 19, 2013 from http://money.cnn.com/2012/08/09/technology/gauss-cyberweapon-bank-accounts/index.html

Gollmann, D. (2008). Securing Web Application. *Information Security Technical Report 13.*

Halley, J. (2011). Web Application Security Assessment Policy. *SANS Institute.*

Houmb, S. H., Franqueira, N. L. & Engum, E. A. (2009). Quantifying Security Risk Level from CVSS Estimates of Frequency and Impact. *The Journal of Systems and Software.*

How are Expert System Corvid Knowledge Automation System Fielded. Retrieved June 25, 2013 from http://www.exsys.com/faq.html

Industrial Management & Data Systems Journal. Retrieved June 25, 2013 from http://www.emeraldinsight.com/journals.htm?articleid=850085&show=html

InfoSecurity. (2013, October). Cyber-attacks Are No. 1 Threat to Existence, UK Firms Say. Retrieved November 1st, 2013 from http://www.infosecurity-magazine.com/view/35335/cyberattacks-are-no-1-threat-to-existence-uk-firms-say/

Kailay, P. & Jaratt, P. (1995). RAMeX: A Prototype Expert System For Computer Security Risk Analysis and Management. *Computers and Security, 14.*

Kearns, T. (2010). IT Security StandardL Web Application Security Vulnerabilities. *Provost Information Technology Company.*

Kostas S. M, John E. P, Dimitris T. A, (2002). GENESYS: an Expert System for Production Scheduling. *Industrial Management & Data Systems*. Vol. 102 Iss: 6. Pp.309 – 317.

Liu, Q. & Zhang, Y. (2010). VRSS: A New System for Rating and Scoring Vulnerabilities. *Computer Communications.*

Lunt, T. et al. (1992). A Real-Time Intrusion Detection Expert System (IDES). *SRI Project 6784.*

Potter, W.D. et al. (2000). A Web-Based Expert System for Gypsy Moth Risk Assessment. *Computers and Electronics in Agriculture.*

Satava, D. (1999). 26 Things You Should Know Before Working for a National Accounting Firm. *New Accountant Magazine.*

Sharif, M. N. (n.d.). Topic 8 Expert System. Retrieved from http://www.slideshare.net/norelianamdsharif/topic-8-expert-system

Shiau, W. (2011). A Profile Of Information Systems Research Published In Expert Systems With Applications From 1995 To 2008. *Expert Systems with Application.*

Shukor, A. (2012, October). Internet security threat in Malaysia. Retrieved June 19, 2013 from MOSTI.

Sykora, N. (2012). Importance of Doing Risk Assessment. Retrieved June 25, 2013 from http://www.halock.com/blog/importance-risk-assessment/

Terry, K. (2013). Unlimited Security Budget and Perfect Security. Retrieved June 25, 2013 from http://www.halock.com/blog/unlimited-security-budgets-perfect-security/

Tseng, C. R. & Wu, C. (2007). An Expert System Approach to Improving Stability and Reliability of Web Service. *Expert Systems with Application.*

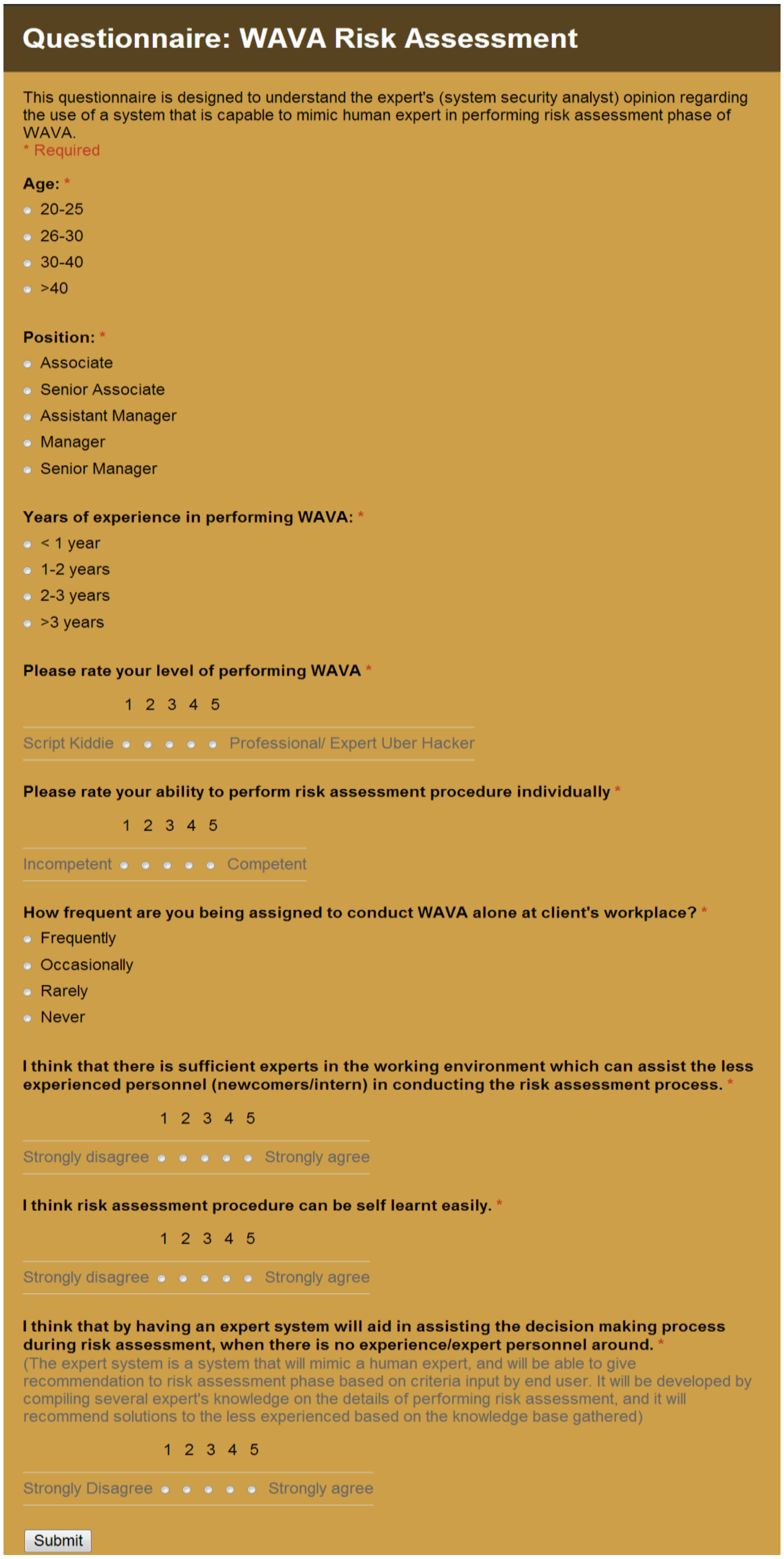
Watson, L. (1997). *Applying Case-Based Reasoning.* Morgan Kaufmann Publisher, Inc.

Whitemire, A. M. (2009). Risk of Performance Error due to Sleep Loss, Circadian Desynchronization, Fatigue, and Work Overload. *Human Research Program Requirements.*

William, J. & Wichers, D. (2013). OWASP Top 10 – 2013. Retrieved June 19, 2013 from http://www.owasp.org

Yoon, Y. & Guimaraes, T. (1993). Selecting Expert System Development Techniques. *Information and Management*, North-Holland. Vol. 24. pp. 209-223.

APPENDIX



Questionnaire: WAVA Risk Assessment

This questionnaire is designed to understand the expert's (system security analyst) opinion regarding the use of a system that is capable to mimic human expert in performing risk assessment phase of WAVA.

* Required

Age: *

- ○ 20-25
- ○ 26-30
- ○ 30-40
- ○ >40

Position: *

- ○ Associate
- ○ Senior Associate
- ○ Assistant Manager
- ○ Manager
- ○ Senior Manager

Years of experience in performing WAVA: *

- ○ < 1 year
- ○ 1-2 years
- ○ 2-3 years
- ○ >3 years

Please rate your level of performing WAVA *

	1	2	3	4	5	
Script Kiddie	○	○	○	○	○	Professional/ Expert Uber Hacker

Please rate your ability to perform risk assessment procedure individually *

	1	2	3	4	5	
Incompetent	○	○	○	○	○	Competent

How frequent are you being assigned to conduct WAVA alone at client's workplace? *

- ○ Frequently
- ○ Occasionally
- ○ Rarely
- ○ Never

I think that there is sufficient experts in the working environment which can assist the less experienced personnel (newcomers/intern) in conducting the risk assessment process. *

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I think risk assessment procedure can be self learnt easily. *

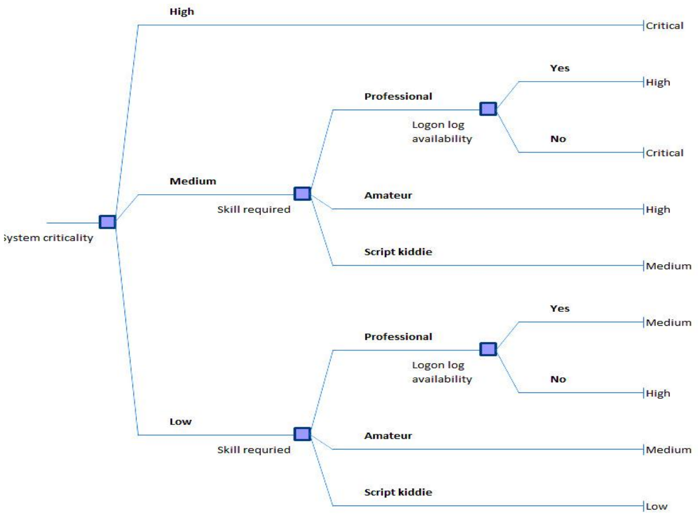
	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

I think that by having an expert system will aid in assisting the decision making process during risk assessment, when there is no experience/expert personnel around. *

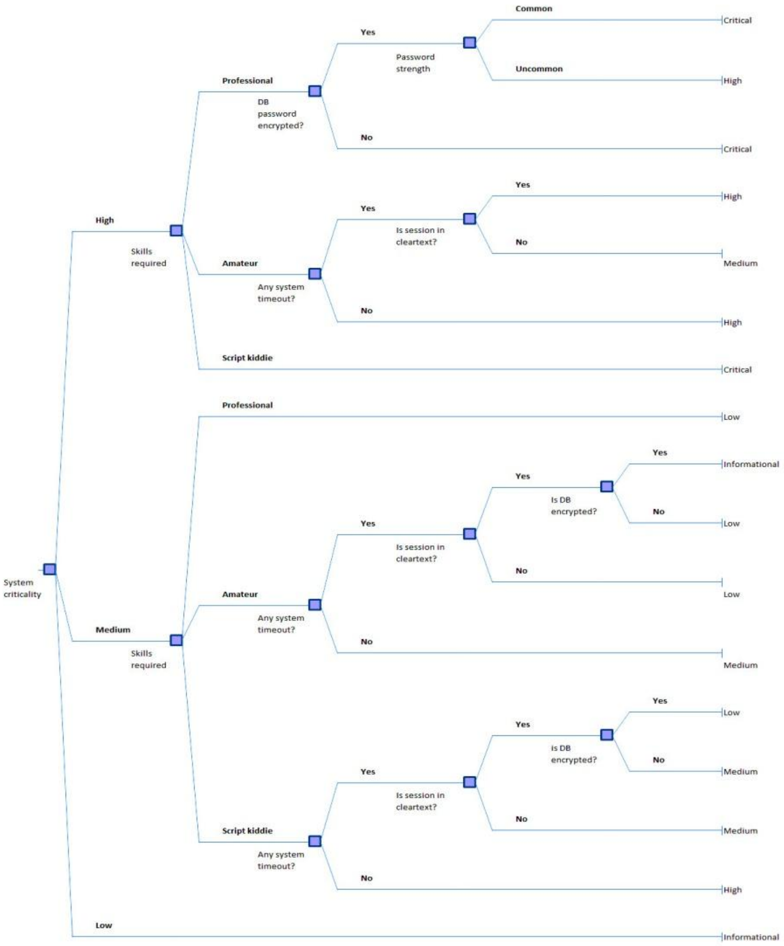
(The expert system is a system that will mimic a human expert, and will be able to give recommendation to risk assessment phase based on criteria input by end user. It will be developed by compiling several expert's knowledge on the details of performing risk assessment, and it will recommend solutions to the less experienced based on the knowledge base gathered)

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly agree

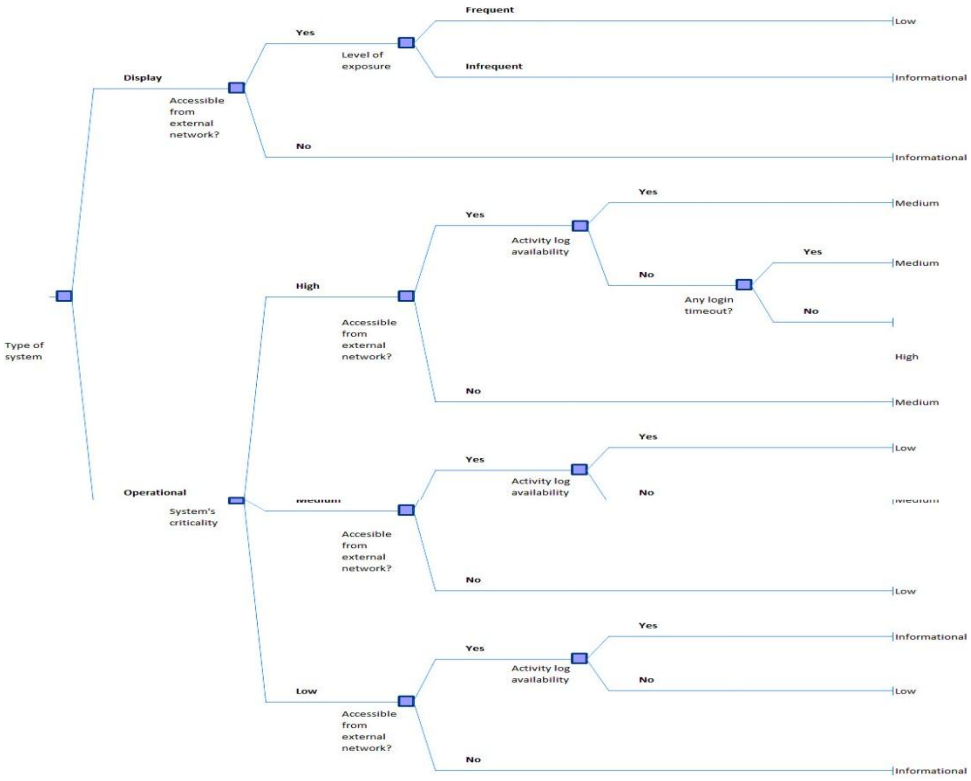
APPENDIX 1: Screenshot of survey questionnaire



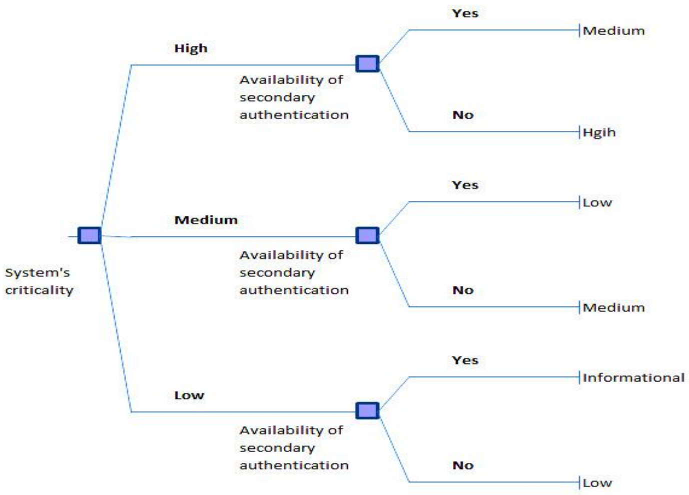
APPENDIX 2: Decision tree for vulnerability #1



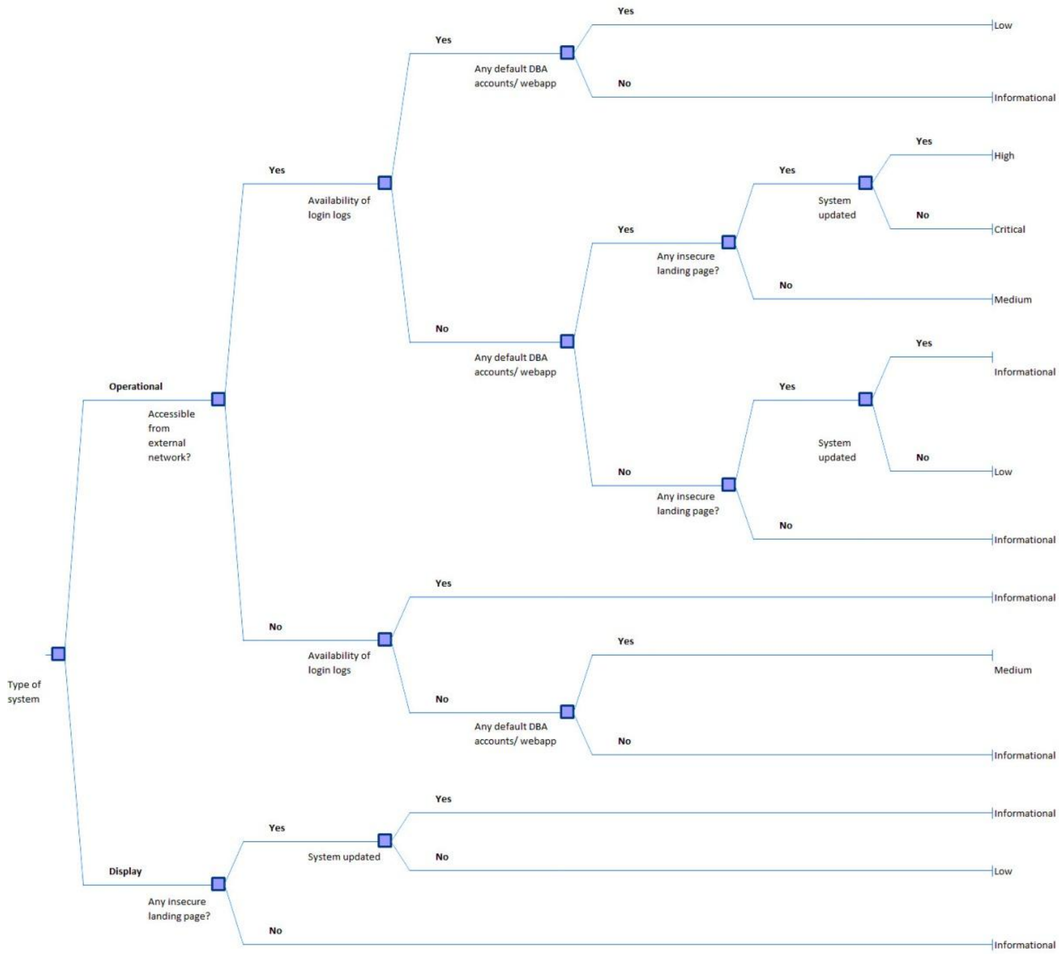
APPENDIX 3: Decision tree for vulnerability #2



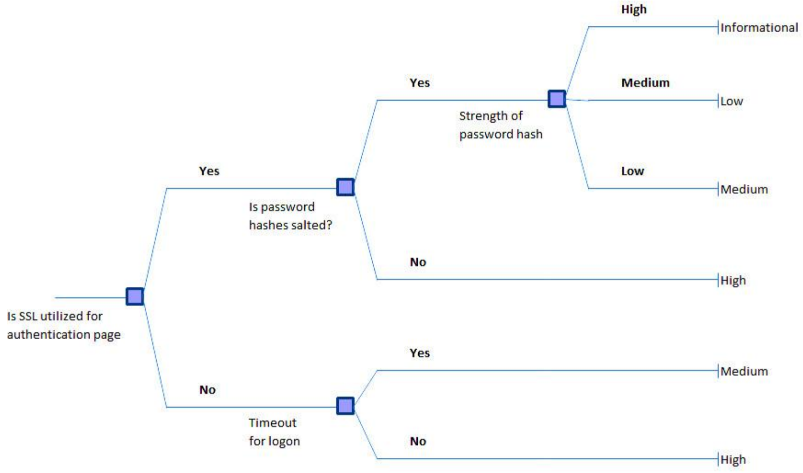
APPENDIX 4: Decision tree for vulnerability #3


System's criticality
High
Availability of secondary authentication
Yes
Medium
No
Hgih
Medium
Availability of secondary authentication
Yes
Low
No
Medium
Low
Availability of secondary authentication
Yes
Informational
No
Low

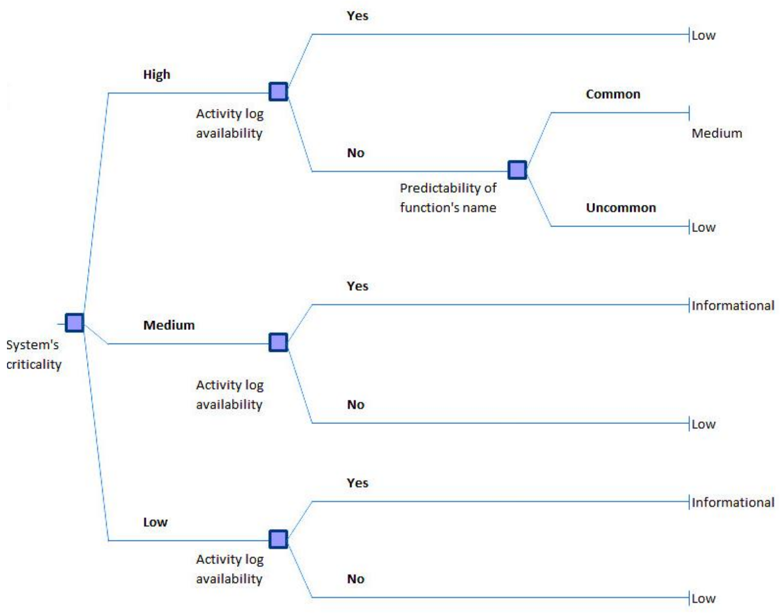
APPENDIX 5: Decision tree for vulnerability #4


Type of system
Operational
Accessible from external network?
Yes
Availability of login logs
Yes
Any default DBA accounts/ webapp
Yes
Low
No
Informational
No
Any default DBA accounts/ webapp
Yes
Any insecure landing page?
Yes
System updated
Yes
High
No
Critical
No
Medium
No
Any insecure landing page?
Yes
System updated
Yes
Informational
No
Low
No
Informational
No
Availability of login logs
Yes
Informational
No
Any default DBA accounts/ webapp
Yes
Medium
No
Informational
Display
Any insecure landing page?
Yes
System updated
Yes
Informational
No
Low
No
Informational

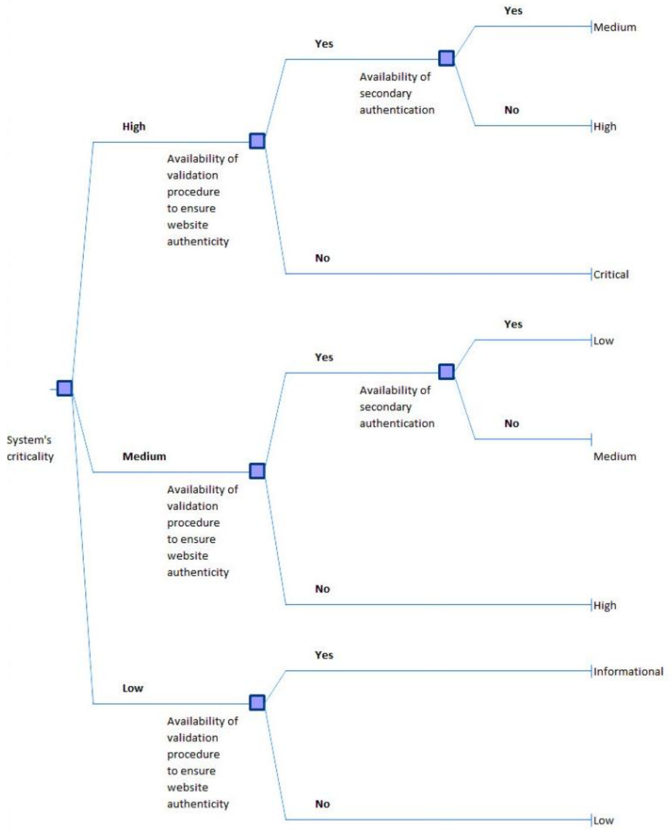
APPENDIX 6: Decision tree for vulnerability #5


Is SSL utilized for authentication page
Yes
Is password hashes salted?
Yes
Strength of password hash
High
Informational
Medium
Low
Low
Medium
No
High
No
Timeout for logon
Yes
Medium
No
High

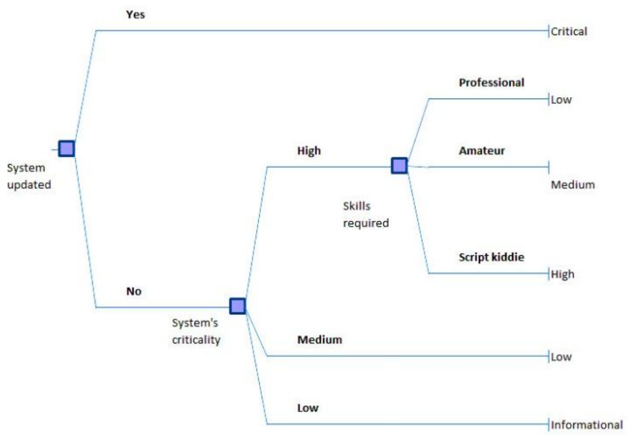
APPENDIX 7: Decision tree for vulnerability #6



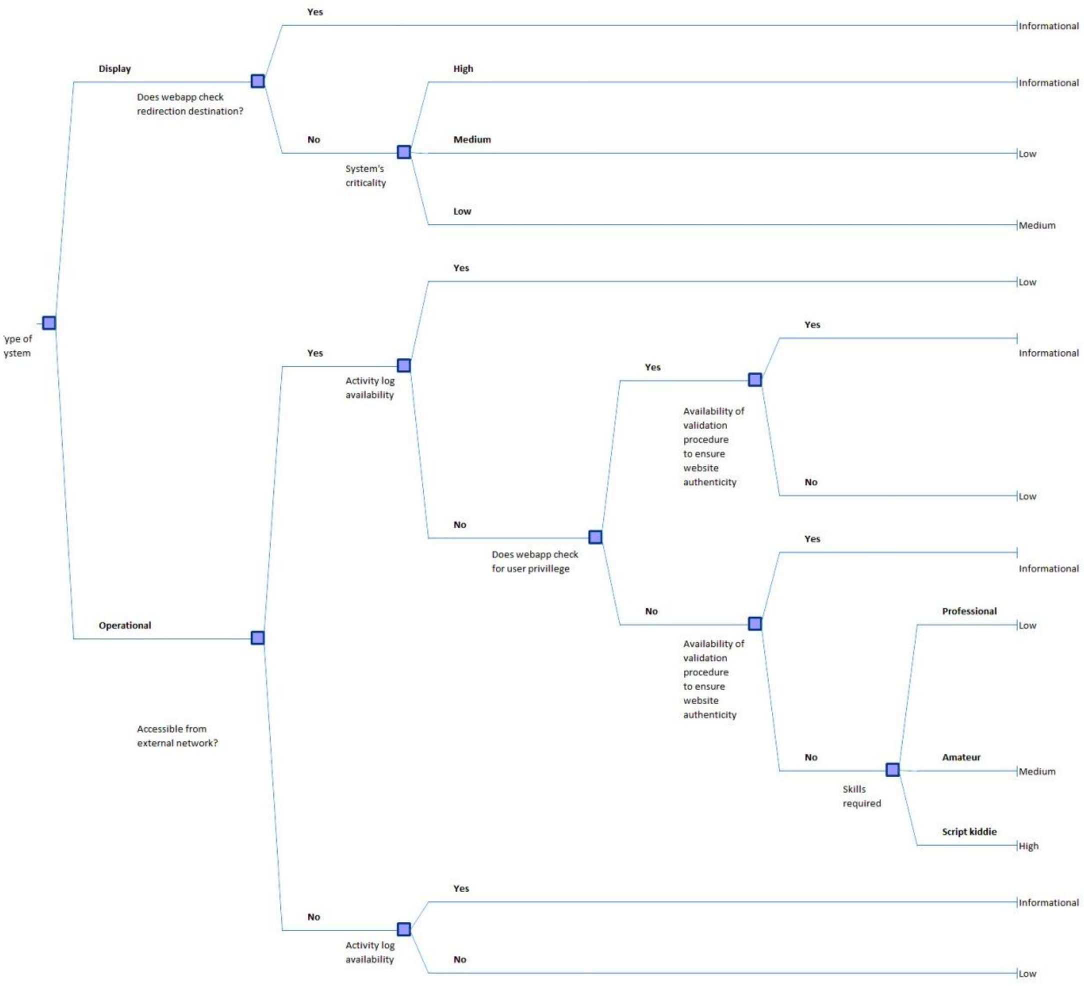
APPENDIX 8: Decision tree for vulnerability #7



APPENDIX 9: Decision tree for vulnerability #8



APPENDIX 10: Decision tree for vulnerability #9



APPENDIX 11: Decision tree for vulnerability #10