



UNIVERSITY OF INFORMATION TECHNOLOGY
AND SCIENCES (UITs)

DEPARTMENT OF INFORMATION TECHNOLOGY

PAPER : 1

IT 464 : COMPUTER DATA NETWORK SECURITY LAB

Information security risks management framework

Submitted To:

Shubham Saha
Lecturer,
Department of IT, UITs

Submitted By:

Name: Md.Tanvir Khan
Fahim
Student ID: 2014755005
Name:Thimur Rahman
Topu
Student ID: 2014755019
Name:Most.Jarin Sarker
Student ID: 2014755036
Department of IT, UITs

November 15, 2022

Department of IT, UITS © All rights reserved.

Contents

1	Abstract	2
2	Introduction	2
3	Related Work	2
3.1	Risk Before and After Controls University Of Greenwich	3
4	University campus network setup	3
5	Proposed quantitative information security risk assessment model	4
5.1	Assets Identification	4
5.2	Understanding security requirements	4
5.3	Vulnerabilities identification	5
5.4	Quantitative risk measurement	5
5.5	Find and apply countermeasures	5
5.6	Possible Remediate	5
5.7	Mitigate Vulnerabilities	5
5.8	Reporting	5
6	Evaluation of proposed quantitative information security risk assessment model	7
6.1	Vulnerability identification and assessment	7
6.2	Quantitative risk level measurement	9
6.3	Upgrade recommendations	10
7	Evaluation of proposed information security risksmanagement framework	10
8	Conclusion:	11
9	Reference:	11

1 Abstract

The purpose of this policy is to provide a security framework that will ensure the protection of University Information from unauthorized access, loss, or damage while supporting the open, information-sharing needs of our academic culture. All University Information is classified into one of four levels based on its sensitivity and the risks associated with disclosure. The classification level determines the security protections that must be used for the information. Here if we want to propose a framework, we will want to reduce the risk of security. We can't ensure that it will be safe 100% but we can make it more secure. Our ongoing process is at first, we scan the website and want to find the threats and vulnerabilities. We will find low, medium, and High vulnerabilities. We will work on that high vulnerabilities and then my main work begins and that is how to reduce high vulnerabilities and make them more secure than it's before. The proposed framework is applied on ucam of uits scanning the website security vulnerabilities.

2 Introduction

Ucam is University of information technology and sciences (uits) Information that may be verbal, digital, and/or hard copy, individually controlled or shared, stand-alone or networked, used for administration, research, teaching, or other purposes. Standards and procedures related to this Information Security Policy will be developed and published separately. Every University website has some classification levels. Restricted level: Bank account number, credit card number, Mobile banking(bKash, Upay), Net banking's (mtb,ipay) password. The restricted level is one of the most valuable things of a university network's data. If anyone can Hack the restricted data he can get any ones personal bank statement transaction access by this. Confidential level: It's about personal files(Students' or teachers' personal information like their certificate, National Id no. etc), internal data, and education records(Courses attempt, CGPa). If anyone gets access to this level he can modify anyone's past or running cgpa and he can use their certificate and National Id no. In any terrorist attack or anything. So, we have to find the vulnerabilities and reduce the threats to Security.

3 Related Work

The process for risk assessment will be the same at each level: the impact and likelihood for each risk, before and after controls, will be considered and a 1 to 5 scoring mechanism used to give a position on a 5 X 5 matrix. This will result in scores ranging from 1 to 25, with 25 being the highest score. Recently University Of Greenwich works on network's risk before and after controls. Here We highlighted

some points of there works.

3.1 Risk Before and After Controls University Of Greenwich

In order to assess the effectiveness of controls, risk will first be scored before considering the operation of the University's controls – this is termed the 'Raw Risk Score'. For each risk, the controls and actions in place will then be identified and assessed and the risk score generally reduced to arrive at the 'Residual Risk Score'. 25. The control and actions should either reduce the likelihood that a risk will occur or the impact of that risk were it to occur (an example of the latter would be purchasing insurance to insure against a risk). The difference between controls and actions is that while controls will normally run continuously until changed, actions to reduce risks will be time-limited and should be SMART (specific, measurable, achievable, realistic and timebound). An action may evolve into a control. Residual risk is what is left after considering 7 controls and actions. Where the score after controls is still at an unacceptably high level, additional controls and actions may be required in order to reduce the risk level further. The University's objective is to optimise its controls and actions, i.e. to ensure the most cost-effective controls and actions are in place for each risk and the cost versus the benefit of the control is considered. This may mean that certain risks have a high residual score because the cost of reducing the risk still further may be higher than the potential cost if the risk actually happens – the level of residual risk will, however, need to be considered for compliance with this policy.

4 University campus network setup

Usually, a University uses a campus network which is a proprietary local area network. This University also uses it. The standard topology for the University campus networks is mesh topology, which is best for this kind of situation. But in this case, units use a Hybrid topology

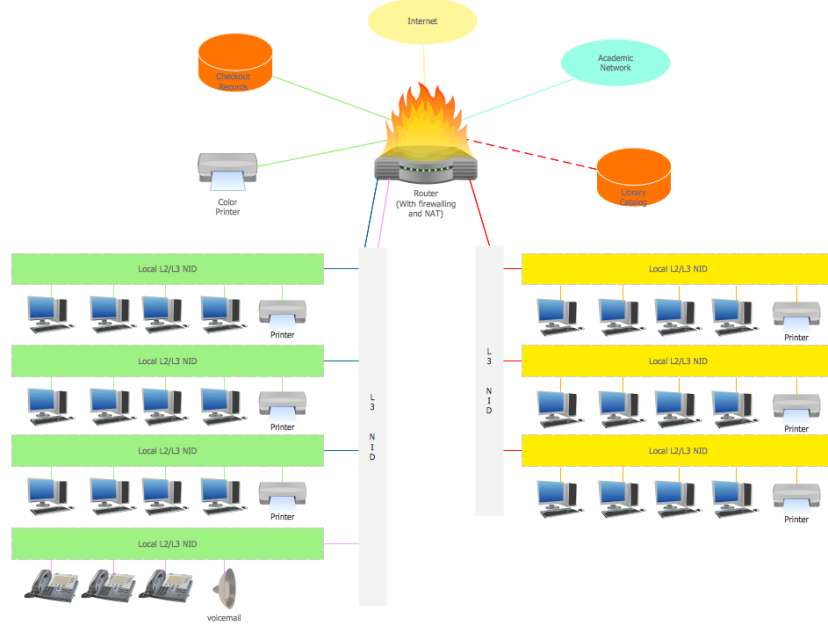


Figure 1: Network Setup For university

5 Proposed quantitative information security risk assessment model

Here our Proposed quantitative information security risk assessment model will design on the data of vulnerabilities that we find by scanning the website. We find one high and some medium vulnerabilities. We will work on that one high and two specific medium vulnerabilities. Our target is to reduce the risk of high and medium vulnerabilities.

5.1 Assets Identification

The use of attributes and methods to uniquely identify an asset, allows for correlation of data across multiple sources, reporting of asset information across different organizations and databases. here our risk assessment will specifying assets.our framework will taken here as an Asset.

5.2 Understanding security requirements

Organizations without dedicated security personnel and with lenient security policies are increasingly exposed to threats, even if they have basic security infrastructure in place. Once discovered, these threats may have already spread to many computing

resources, taking considerable time and effort to eliminate completely. Unforeseen costs related to threat elimination can also be staggering.

5.3 Vulnerabilities identification

The vulnerability identification process enables you to identify and understand weaknesses in your system, underlying infrastructure, support systems, and major applications. It allows you to analyze the potential exposures generated by your supply chain and your business partners.

5.4 Quantitative risk measurement

By the convergence of frequency and impact of exploit, quantitative security risk level can be measured. With the calculated risk magnitude the qualitative risk level can be determined in the range low to high.

5.5 Find and apply countermeasures

Countermeasures Found in Each Layer Security countermeasures are the controls used to protect the confidentiality, integrity, and availability of data and information systems. There is a wide array of security controls available at every layer of the stack. Overall security can be greatly enhanced by adding additional security measures, removing unneeded services, hardening systems, and limiting access.

5.6 Possible Remediate

The vulnerability remediation process is a workflow that fixes or neutralizes detected weaknesses. It includes 4 steps: finding vulnerabilities through scanning and testing, prioritising, fixing and monitoring vulnerabilities.

5.7 Mitigate Vulnerabilities

Mitigating vulnerabilities involves taking steps to implement internal controls that reduce the attack surface of your systems. Examples of vulnerability mitigation include threat intelligence, entity behavior analytic, and intrusion detection with prevention.

5.8 Reporting

Vulnerability management solutions often include features such as policy management, application scanning/testing, vulnerability remediation, network and vulnerability monitoring, and reporting (vulnerabilities, compliance issues, etc).

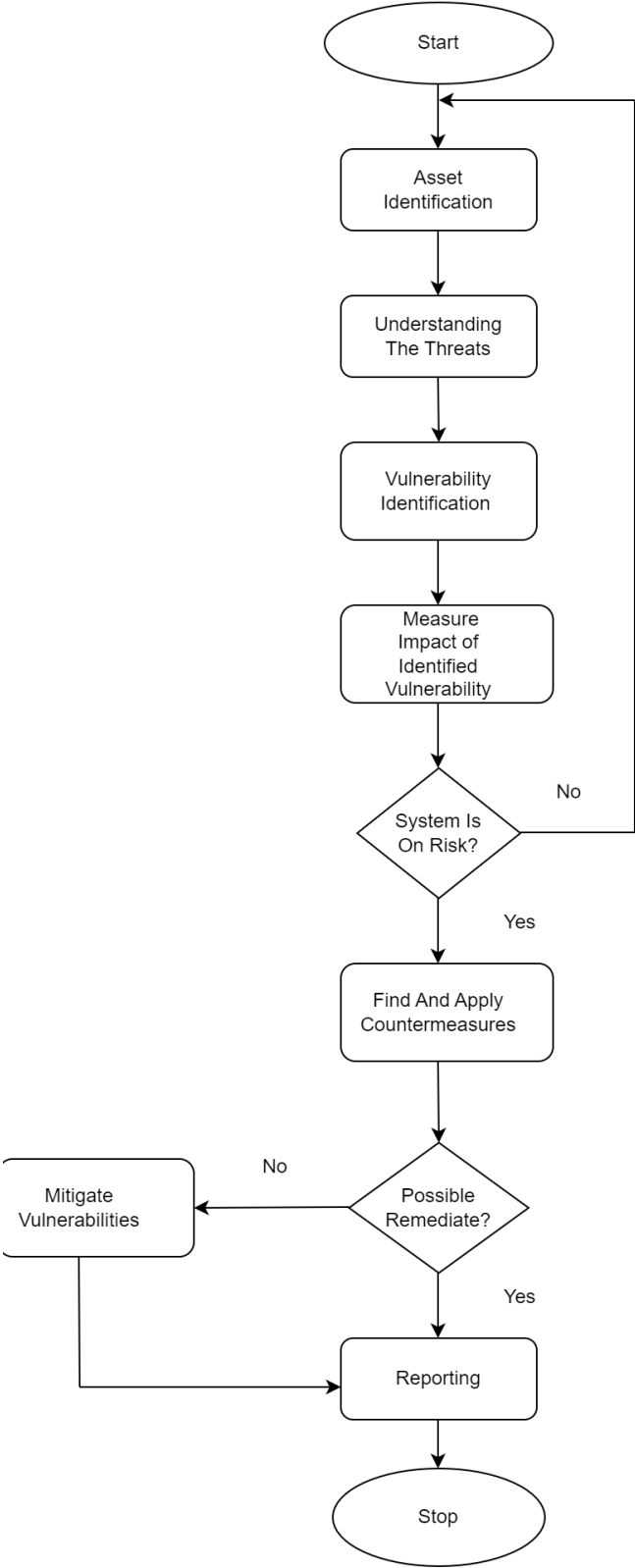
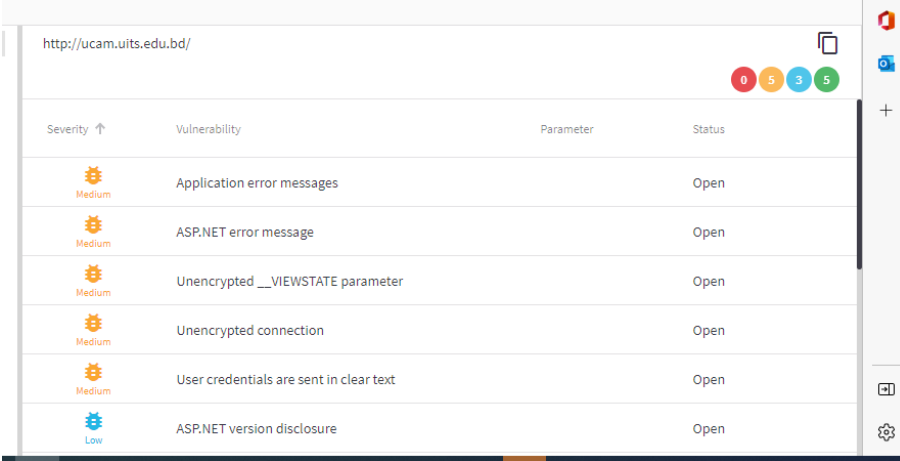


Figure 2: Control Panel

6 Evaluation of proposed quantitative information security risk assessment model

6.1 Vulnerability identification and assessment

A vulnerability assessment provides university with details on any security weaknesses in its environment. It also provides direction on how to assess the risks associated with those weaknesses. This process offers the organization a better understanding of its assets, security flaws and overall risk, reducing the likelihood that a cybercriminal will breach its systems and catch the business off guard. For vulnerability assessment in Uits ucam we use some web scanning tools like Invicti and Acunetix and found some risks and vulnerability in the web application of ucam.



The screenshot displays the Acunetix web scan results for the URL <http://ucam.uits.edu.bd/>. The interface includes a summary bar at the top with colored circles representing the count of vulnerabilities by severity: 0 Critical, 5 High, 3 Medium, and 5 Low. Below this is a table listing the identified vulnerabilities.

Severity	Vulnerability	Parameter	Status
Medium	Application error messages		Open
Medium	ASP.NET error message		Open
Medium	Unencrypted __VIEWSTATE parameter		Open
Medium	Unencrypted connection		Open
Medium	User credentials are sent in clear text		Open
Low	ASP.NET version disclosure		Open

Figure 3: Acunetix Web Scan result





Total alerts found	13
 High	0
 Medium	5
 Low	3
 Informational	5

Figure 4: Acunetix Web Scan result

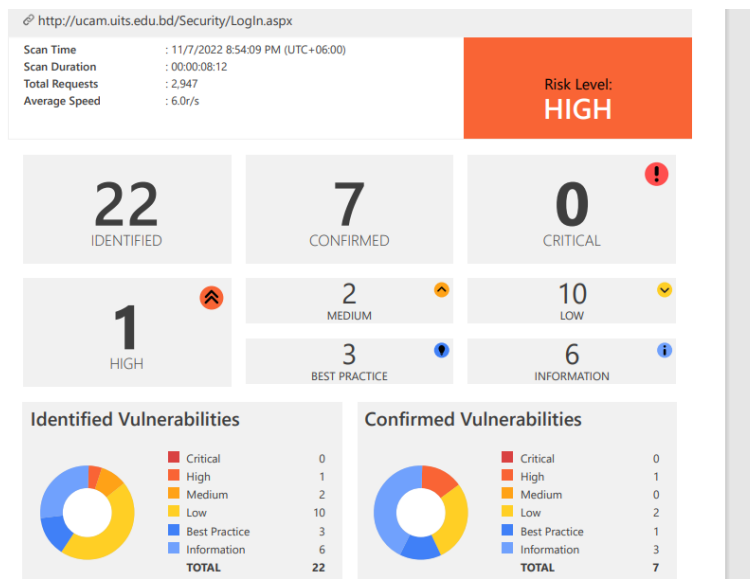


Figure 5: Invicti Web Scan result

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER	PARAMETER TYPES
	Password Transmitted over HTTP	GET	http://ucam.uits.edu.bd/Security/Login.aspx	No Parameters	No Parameter Types
	Out-of-date Version (jQuery)	GET	http://ucam.uits.edu.bd/Security/Login.aspx	No Parameters	No Parameter Types
	SSL/TLS Not Implemented	GET	https://ucam.uits.edu.bd/Security/Login.aspx	No Parameters	No Parameter Types
	(Possible) Backup File Disclosure	GET	http://ucam.uits.edu.bd/Security/Login.aspx/PasswordRecovery.aspx~	No Parameters	No Parameter Types
	(Possible) Cross-site Request Forgery in Login Form	GET	http://ucam.uits.edu.bd/Security/Login.aspx	No Parameters	No Parameter Types
	Missing X-Frame-Options Header	GET	http://ucam.uits.edu.bd/Security/Login.aspx	No Parameters	No Parameter Types
	Programming Error Message	GET	http://ucam.uits.edu.bd/Security/trace.axd	No Parameters	No Parameter Types

Figure 6: Invicti Web Scan result

6.2 Quantitative risk level measurement

In Invicti Where we identified 22 vulnerabilities. Where confirmed are 7, critical 0, High 1, medium 2, low 10. Here we have also best practice 3 and information 6 site, that's not necessary for our documentation. We will work for that 1 high and 2 medium vulnerabilities. Here in Acuntix security audit find 13 vulnerabilities. Here high 0, medium 5, low 3, and informational 5. Here we also work on that medium vulnerabilities. At first we will choose our vulnerabilities and work on it.

- 1. Password Transmitted over HTTP: Impact If an attacker can intercept network traffic, he/she can steal users' credentials. The software transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors. Many communication channels can be "sniffed" by attackers during data transmission.
- 2. Out-of-date Version (jQuery): Since this is an old version of the software, it may be vulnerable to attacks. Most of the time this happens for two reasons: A theme or plugin has replaced the version of jQuery that WordPress uses with an older version.
- 3. SSL/TLS Not Implemented:

An attacker who is able to intercept your - or your users' - network traffic can read and modify any messages that are exchanged with your server. That means that an attacker can see passwords in clear text, modify the appearance of your website, redirect the user to other web pages or steal session

information. Therefore no message you send to the server remains confidential

- 4. User credentials are sent in clear text: User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

6.3 Upgrade recommendations

- 1. Password Transmitted over HTTP Remediation All sensitive data should be transferred over HTTPS rather than HTTP. Forms should be served over HTTPS. All aspects of the application that accept user input, starting from the login process, should only be served over HTTPS.
- 2. Out-of-date Version (jQuery) Update latest version.
- 3. SSL/TLS Not Implemented implement SSL/TLS properly, for example by using the Certbot tool provided by the Let's Encrypt certificate authority. It can automatically configure most modern web servers, e.g. Apache and Nginx to use SSL/TLS. Both the tool and the certificates are free and are usually installed within minutes.
- 4. User credentials are sent in clear text Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

7 Evaluation of proposed information security risks-management framework

When we scan our website we identified many vulnerabilities. But in the framework we said we gonna work on measure or impactful vulnerabilities. We select for from them. First one is Password Transmitted over HTTP Impact. what really transfer plaintext that's why we chose it and discuss how harmful and danger it is and we give a remediation for it. Secoyome is Out-of-date Version (jQuery) what was running the old version now we have to update it or Install it latest version. The third one is SSL/TLS Not Implemented what is also provide plaintext. And the last one is User credentials, what is unencrypted channel. That's mean confidential data will processing on unencrypted way, that's is so much danger for the website security. So, the main thing is by following the remediation we can reduce the security risk and solve the vulnerabilities. if we can make it 100 % secure It's not the problem we just make our website more secure than it was before.

8 Conclusion:

This paper proposed Quantitative Information Security Risk Assessment framework for University's Computing Environment. The goal of proposed model is to reduce risks of security breach, this means understanding the cause that makes University's campus network vulnerable. Applying the proposed framework onto the uits ucam web server, it is clear that the current approaches of securing the network are ineffective in University environment's concern.

9 Reference:

- <https://www.gre.ac.uk/about-us/governance/risk-management>
- <https://www.techtarget.com/searchsecurity/definition/vulnerability-assessment-vulnerability-analysis>