SEMARAK ILMU
PUBLISHING
202103268166(003316878-P)

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Web-Based Reporting Vulnerabilities System for Cyber Security Maintenance

Firkhan Ali Hamid Ali[1,*], Mohd Khairul Amin Mohd Sukri[1], Mohd Zalisham Jali[2], Muhammad Al-Fatih[1], Mohd Azhari Mohd Yusof[1]

[1] Fakulti Sains Komputer & Teknologi Maklumat, Universiti Tun Hussein Onn Malaysia, 86400 Parit Raja, Johor, Malaysia
[2] Fakulti Sains & Teknologi, Univerisiti Sains Islam Malaysia, Nilai, Malaysia

ARTICLE INFO

Article history:
Received 6 October 2022
Received in revised form 5 January 2023
Accepted 27 January 2023
Available online 18 February 2023

Keywords:
Cyber security maintenance; Web services; Vulnerability; Nessus

ABSTRACT

To maintain secure web services and IT infrastructure, this has proposed the prototype of a vulnerability reporting system. Among these reporting systems developed to deal with problems of maintenance and analysis report management system which not yet been implemented in the cyber security scanning tool, Nessus. The system, which was designed to manage and analyze cyber security maintenance by focusing on vulnerability reports, was based on web-based technology. To ensure that the prototyping system could be used quickly, the development process employed the prototyping-rapid application development technique. The administrator of this system may easily manage and keep track of the report following the activity of scanning the cyber security maintenance for vulnerabilities.

1. Introduction

Information technology is now used for a wider range of applications and with greater intelligence in society. Therefore, a lot of people utilize information technology as a tool to satisfy their interests and demands without considering the harm it may cause to other people or society [1]. The protection of information within computer networks continues to be addressed from a wide variety of inconsistent perspectives by uncoordinated groups often working at cross purposes [2].

Any organization must ensure the security of its web services and IT infrastructure to prevent further harm and unprofitable events [3]. Therefore, it must perform security testing and analysis on the organization's web services and IT infrastructure multiple times [4]. With the knowledge of the security condition in the web services and IT infrastructure, actions can be taken as soon as feasible [5].

Nessus is an open-source program that is the most reliable and effective for doing security analyses of web services and IT infrastructure [6]. After the scanning activity was done to the web

[*] *Corresponding author.*
E-mail address: firkhan1977@yahoo.com

https://doi.org/10.37934/araset.29.3.198205

services and IT infrastructure, a static report about the security level and available vulnerabilities was generated [7].

Vulnerability is the term used to describe the weak points in web services and IT infrastructure. It may turn into risks and vulnerabilities for the web services and IT infrastructure [8]. Examples include software defects, open ports that aren't required, and password system flaws.

2. Methodology

At the selected IT Lab, which is part of the faculty of Information Technology in the selected public university, a vulnerability report information system for web services and IT infrastructure was developed. The prototyping-rapid application development process was applied during the development, as can be seen in Figure 1.

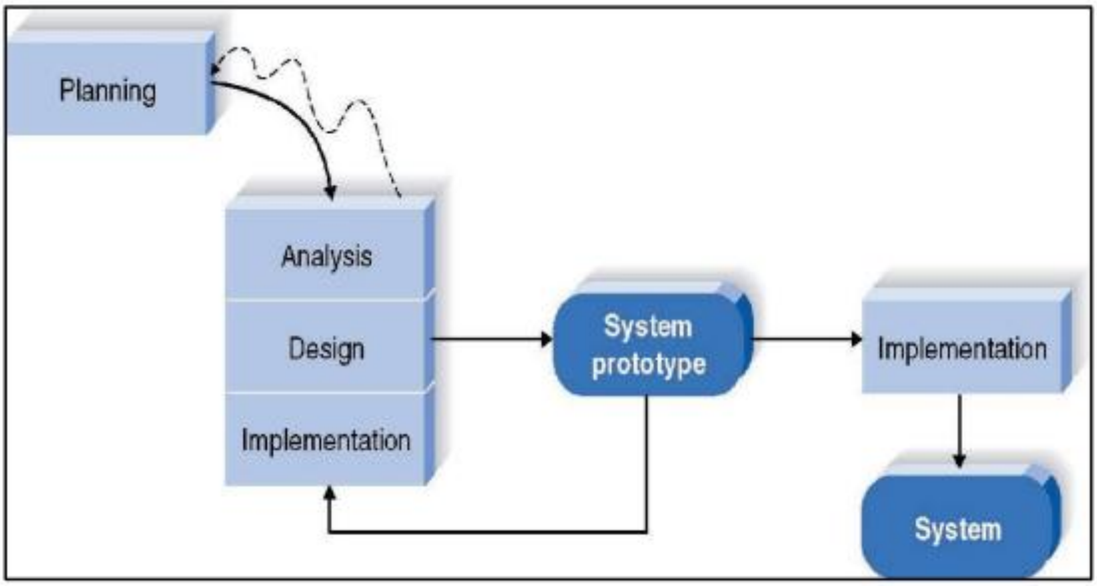


Fig. 1. Methodology of prototyping [9]

Before it could be completely implemented, the approach had to be completed in five steps to develop the prototype system. The steps are planning, analysis, design, system prototype, and implementation. In this system development, there existed the methodology range.

A feasibility analysis of the system was conducted during this planning phase to make sure it had realistic aims, a wide enough scope, and potential users [10]. All of the hardware and software requirements, as well as the location where the prototyping system study and implementation are to be done, have been specified [11].

The system requirements have been researched and determined for the prototyping system at this analysis phase. A study on the use of vulnerability scanning software in its reporting system was conducted.

To guarantee that the prototype system's output will match the study's purpose, the DFD (Data flow) and ERD (Entity-relationship) diagrams were created [12]. Additionally, it will make clear the crucial conditions for the data, database, module, and functioning of the prototype system. potential users. All of the hardware and software requirements, as well as the location where the prototyping system study and implementation are to be done, have been specified [13].

Before this design phase, all of the soft side requirements for the prototyping system itself had been completed conceptually in the form of DFD, ERD, tables, and diagrams. The design of the prototyping system, which comprised the interface design, database design, system connectivity, and installation and configuration of the software used in this development, was therefore completed during this phase [14].

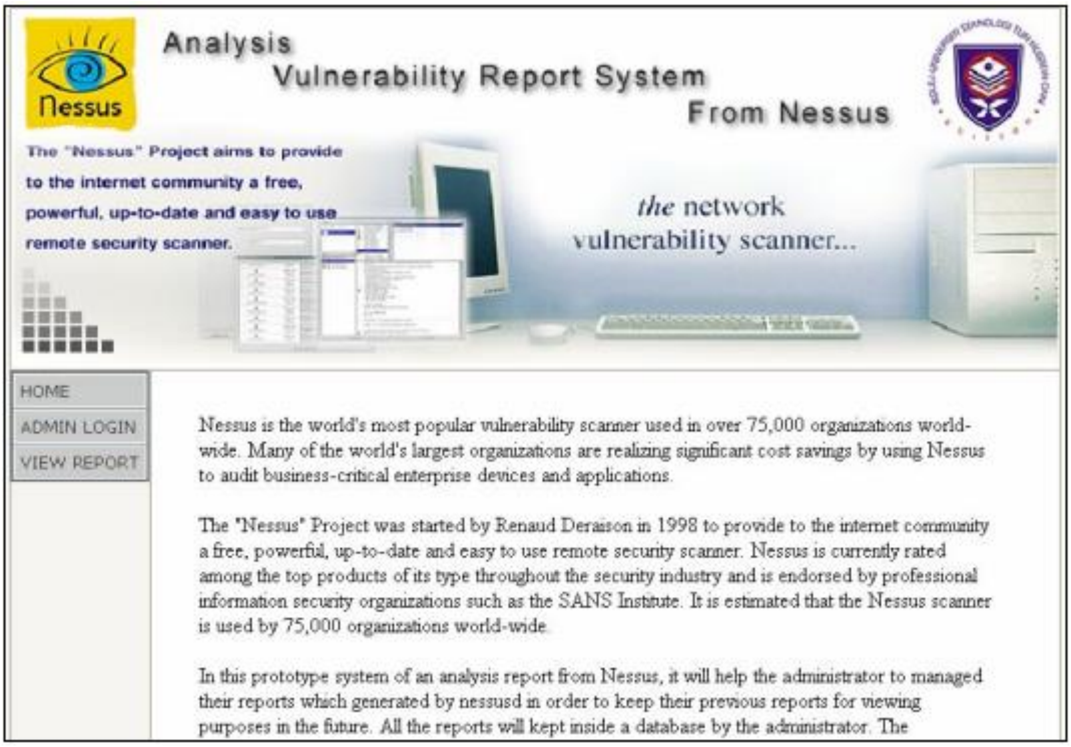
In the system prototyping phase, the design and analysis that went into this study were crucial for producing a working prototype of the system with the least amount of inaccuracy [15]. The system's source code will be generated in accordance with the findings of the previous phase, but it will undergo continuous review until it satisfies user needs with zero or fewer errors [16].

The system prototype was put into use during this implementation phase and was being used by the intended audience. To guarantee that users of the prototype system could use it quickly and efficiently, a user manual had been created [17].

In this stage, the prototyping system was tested and put to use to identify any flaws. Once everything has worked well and meets user criteria, it will then replicate all previous processes before moving on to the next ones.

3. Results

The prototype system has numerous features that have been built, such as login and password, upload and download of reports, viewing of reports, and report searching as the state in the following Figure 2.



Nessus
Analysis
Vulnerability Report System
From Nessus
The "Nessus" Project aims to provide to the internet community a free, powerful, up-to-date and easy to use remote security scanner.
the network vulnerability scanner...
HOME
ADMIN LOGIN
VIEW REPORT

Nessus is the world's most popular vulnerability scanner used in over 75,000 organizations world-wide. Many of the world's largest organizations are realizing significant cost savings by using Nessus to audit business-critical enterprise devices and applications.

The "Nessus" Project was started by Renaud Deraison in 1998 to provide to the internet community a free, powerful, up-to-date and easy to use remote security scanner. Nessus is currently rated among the top products of its type throughout the security industry and is endorsed by professional information security organizations such as the SANS Institute. It is estimated that the Nessus scanner is used by 75,000 organizations world-wide.

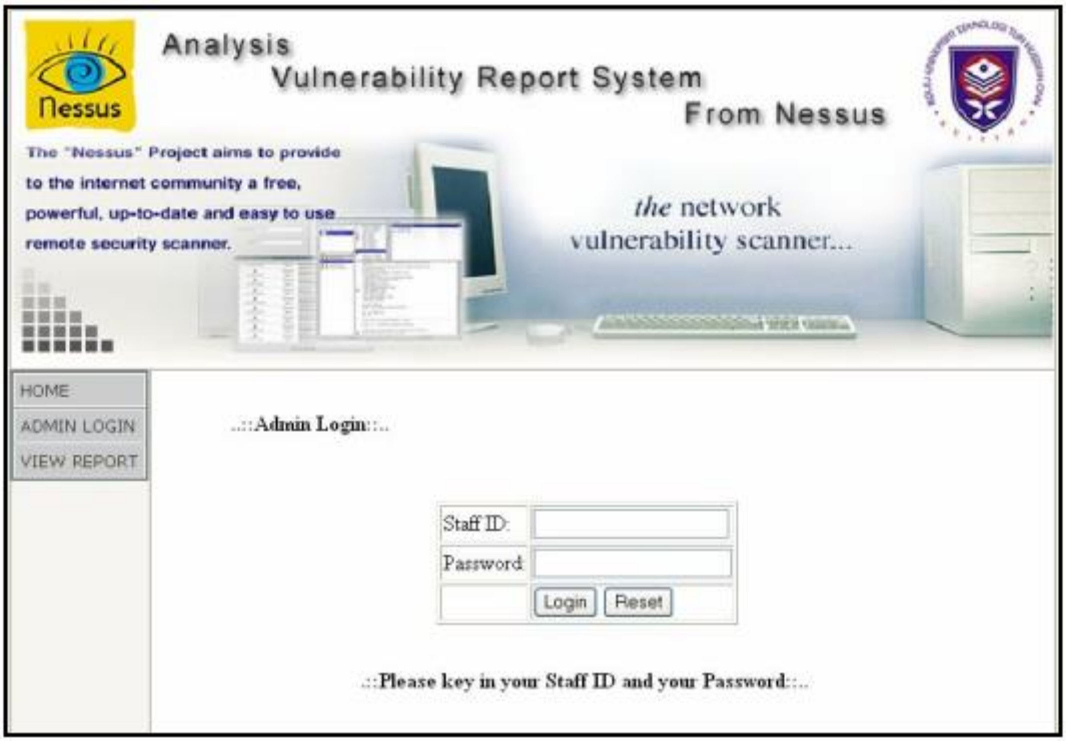
In this prototype system of an analysis report from Nessus, it will help the administrator to managed their reports which generated by nessusd in order to keep their previous reports for viewing purposes in the future. All the reports will kept inside a database by the administrator. The

Fig. 2. Main page of the prototyping system

The prototype system has two different user types: administrative users and regular users. Users must double-click the View Report button for regular users and the Admin Login button for administrative users in order to log in.

For administrative users, there are various functions that they can perform in accordance with keeping reports in the system. It has the ability to upload, remove, print, and rename report files that have been saved in the system. The files of overall reports can only be viewed, downloaded, and printed by regular users.

The login and password function for the administrative user in the system is shown in Figure 3 below. A login and password function for typical use in the system is shown in Figure 4.

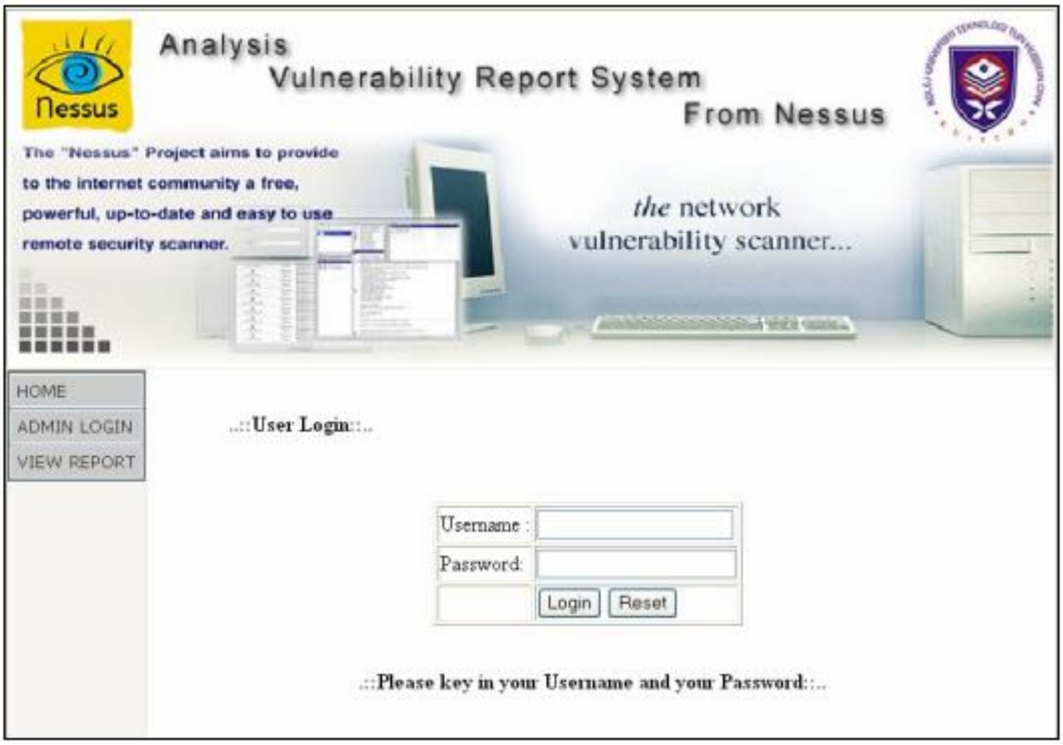

Nessus
Analysis
Vulnerability Report System
From Nessus
The "Nessus" Project aims to provide to the internet community a free, powerful, up-to-date and easy to use remote security scanner.
the network vulnerability scanner...
HOME
ADMIN LOGIN
VIEW REPORT
Login
Reset

..::Admin Login::..

Staff ID:
Password:

..::Please key in your Staff ID and your Password::..

Fig. 3. Login page for administrator


Nessus
Analysis
Vulnerability Report System
From Nessus
The "Nessus" Project aims to provide to the internet community a free, powerful, up-to-date and easy to use remote security scanner.
the network vulnerability scanner...
HOME
ADMIN LOGIN
VIEW REPORT
Login
Reset

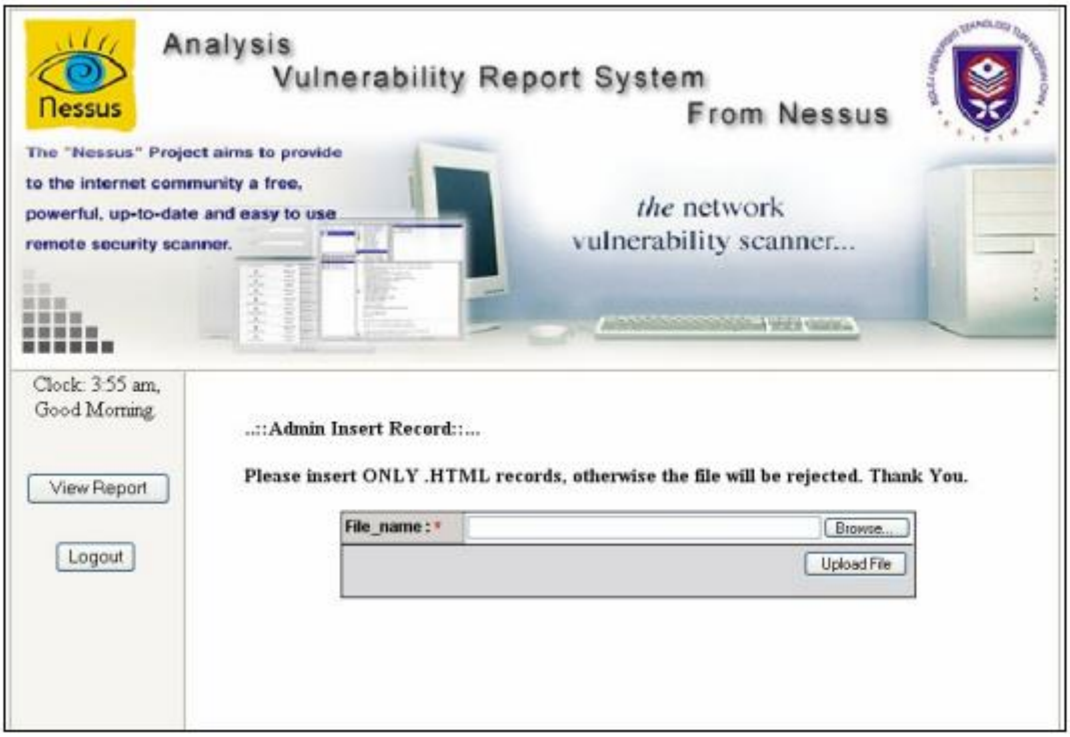
..::User Login::..

Username :
Password:

..::Please key in your Username and your Password::..

Fig. 4. Login page for user

Users with administrative privileges have the ability to upload report files into the database as the stated in Figure 5. Only files produced by the Nessus program with an HTML format are accepted by the system. Figure 6 shows an example of a user selecting the report's file name, PC7-192.268.0.113.html. In order to locate the file, it will click the Browse button on the system.



Analysis
Vulnerability Report System
From Nessus

The "Nessus" Project aims to provide to the internet community a free, powerful, up-to-date and easy to use remote security scanner.

the network vulnerability scanner...

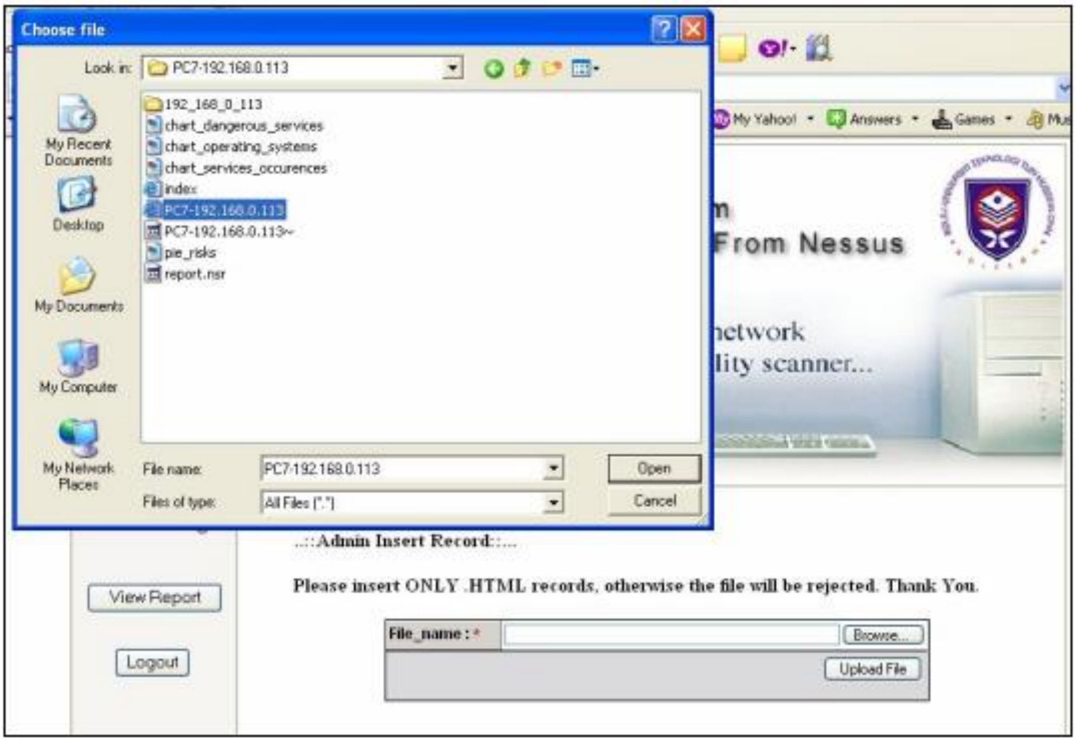
Clock: 3:55 am, Good Morning

..::Admin Insert Record::...

Please insert ONLY .HTML records, otherwise the file will be rejected. Thank You.

File_name : *

Fig. 5. Insert the report’s file



Choose file

Look in: PC7-192.168.0.113

192_168_0_113
chart_dangerous_services
chart_operating_systems
chart_services_occurences
index
PC7-192.168.0.113
PC7-192.168.0.113~
pie_risks
report.nsr

File name: PC7-192.168.0.113
Files of type: All Files (*.*)

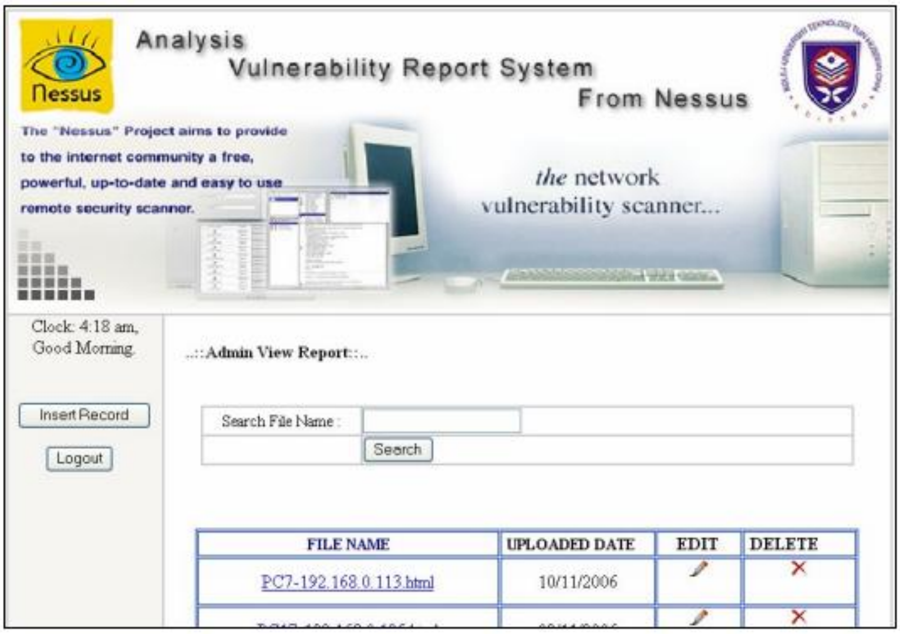
..::Admin Insert Record::...

Please insert ONLY .HTML records, otherwise the file will be rejected. Thank You.

File_name : *

Fig. 6. Selecting report’s file

The file had to then be uploaded by pressing the Upload File button on the prototype system. The report's file that had already been uploaded into the prototype system is shown in the next figure, Figure 7.


Nessus
Analysis
Vulnerability Report System
From Nessus
The "Nessus" Project aims to provide to the internet community a free, powerful, up-to-date and easy to use remote security scanner.
the network vulnerability scanner...
Insert Record
Logout
Search
✎
✕

Clock: 4:18 am,
Good Morning

..::Admin View Report::..

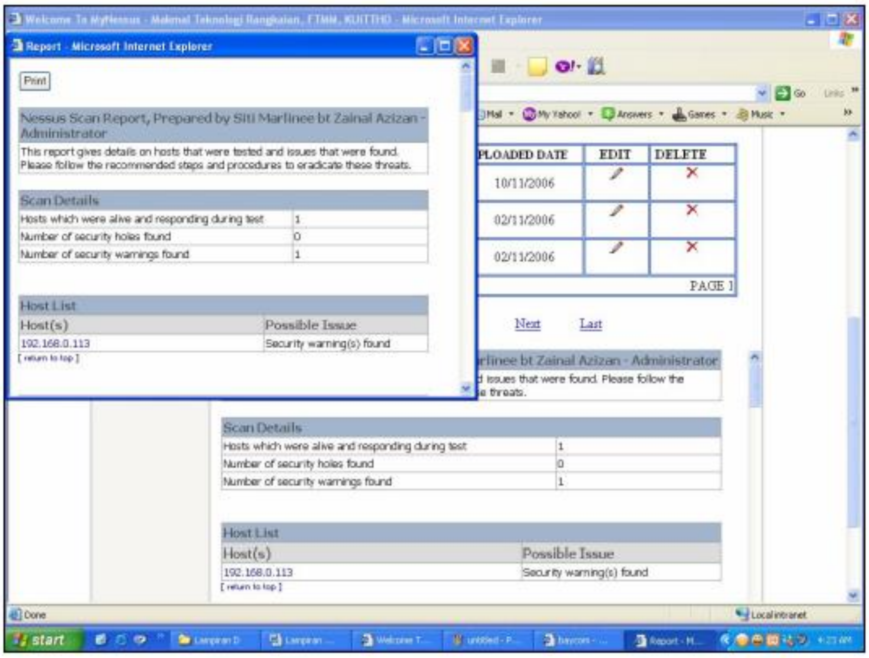
Search File Name :

FILE NAME	UPLOADED DATE	EDIT	DELETE
PC7-192.168.0.113.html	10/11/2006	✎	✕

Fig. 7. Available report file

It is possible to delete and edit each reporting file that was present in the prototype system. By using the Edit function, the file's name can be changed. The prototype system also has a feature that allows users to conduct database searches on reports by selecting the Search button. All this menu had represented in Figure 7.

Figure 8 depicts the report view in the prototype system. It can display in a pop-up or a frame format. The user can print the report from this reporting function by selecting the Print button.



Nessus Scan Report, Prepared by Siti Marlinee bt Zainal Azizan - Administrator
This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

Scan Details	
Hosts which were alive and responding during test	1
Number of security holes found	0
Number of security warnings found	1

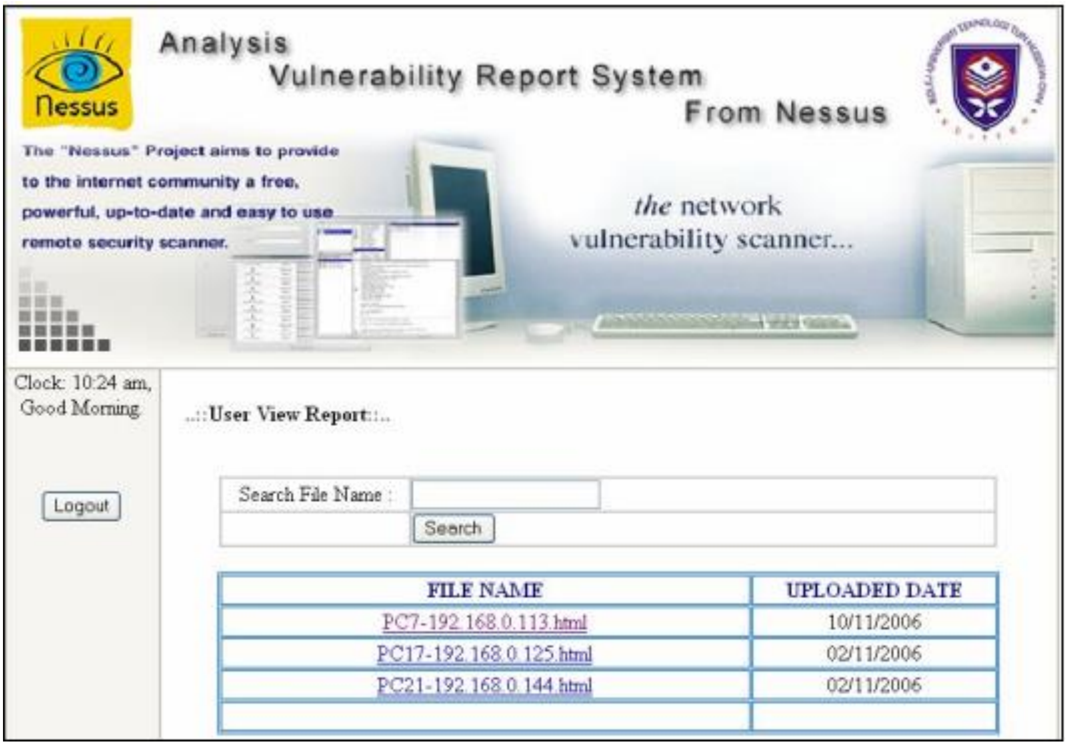
Host List	
Host(s)	Possible Issue
192.168.0.113	Security warning(s) found

[return to top]

PLOADED DATE	EDIT	DELETE
10/11/2006	✎	✕
02/11/2006	✎	✕
02/11/2006	✎	✕
		PAGE 1

Fig. 8. Management of report’s file

The prototype system will provide an interface similar to that in Figure 9 once a regular user has logged on using their login information and password. The average user has access to the files that were stored on the system and can read, search for, and print reports from them [18].



Analysis
Vulnerability Report System
From Nessus

The "Nessus" Project aims to provide to the internet community a free, powerful, up-to-date and easy to use remote security scanner.

the network
vulnerability scanner...

Clock: 10:24 am,
Good Morning

..::User View Report::..

Search File Name :

FILE NAME	UPLOADED DATE
PC7-192.168.0.113.html	10/11/2006
PC17-192.168.0.125.html	02/11/2006
PC21-192.168.0.144.html	02/11/2006

Fig. 9. Main menu

4. Conclusions

The reports of the results of the vulnerability scan in the cyber security maintenance of web services and IT infrastructure must be kept in the correct system after completion. Better management of the reports that must be analysed or viewed in the present or in the future will result from this [19].

In this case, it is possible to handle the vulnerability scanning activity's outcomes and report effectively. The lone prototype system, however, is the focus of this investigation [20]. Future work on this prototype will involve improving the technique so that it can be implemented more effectively and function as a usable system to do the cyber security maintenance of web services and IT infrastructure [21]. It indicates that the system may be used with all necessary functionality and zero or fewer errors.

Acknowledgment

This research was supported by Universiti Tun Hussein Onn Malaysia (UTHM) through TIER 1 (vot Q152)

References

[1] Amoroso, Edward G. *Fundamentals of computer security technology*. Prentice-Hall, Inc., 1994. https://doi.org/10.1016/0142-0496(94)90187-2

[2] Wang, Dan, Terh Jing Khoo, and Zhangfei Kan. "Exploring the Application of Digital Data Management Approach for Facility Management in Shanghai's High-rise Buildings." *Progress in Energy and Environment* 13 (2020): 1-15.

[3] Zalisham, Firkhan Ali Bin Hamid Ali1Mohd, and Mohd Norazmi bin Nordin Jali. "Preliminary Study On It Security Maintenance Management In Malaysia Organizations." *PalArch's Journal of Archaeology of Egypt/Egyptology* 18, no. 1 (2021): 4061-4073.

[4] Zhang, Qisheng, Jin-Hee Cho, Terrence J. Moore, and Ray Chen. "Vulnerability-aware resilient networks: Software diversity-based network adaptation." *IEEE Transactions on Network and Service Management* 18, no. 3 (2020): 3154-3169. https://doi.org/10.1109/TNSM.2020.3047649

[5] Fritz, Willy. "Numerical simulation of the peculiar subsonic flow-field about the VFE-2 delta wing with rounded leading edge." *Aerospace Science and Technology* 24, no. 1 (2013): 45-55. https://doi.org/10.1016/j.ast.2012.02.006

[6] Bozkus Kahyaoglu, Sezer, and Kiymet Caliyurt. "Cyber security assurance process from the internal audit perspective." *Managerial Auditing Journal* 33, no. 4 (2018): 360-376. https://doi.org/10.1108/MAJ-02-2018-1804

[7] Konrath, Robert, Christian Klein, and Andreas Schröder. "PSP and PIV investigations on the VFE-2 configuration in sub-and transonic flow." *Aerospace Science and Technology* 24, no. 1 (2013): 22-31. https://doi.org/10.1016/j.ast.2012.09.003

[8] Ilham, Zul, and Nur Aida Izzaty Saad. "Wan Abd Al Qadr Imad Wan, and Adi Ainurzaman Jamaludin." Multi-criteria decision analysis for evaluation of potential renewable energy resources in Malaysia."." *Progress in Energy and Environment* 21 (2022): 8-18. https://doi.org/10.37934/progee.21.1.818

[9] Dennis, Alan, Barbara Haley Wixom, and Roberta M. Roth. *Systems analysis and design*. John wiley & sons, 2008.

[10] Chu, Julio. *Experimental surface pressure data obtained on 65 delta wing across Reynolds number and Mach number ranges*. Vol. 3. National Aeronautics and Space Administration, Langley Rearch Center, 1996.

[11] Khattak, Muhammad Adil, Jun Keat Lee, Khairul Anwar Bapujee, Xin Hui Tan, Amirul Syafiq Othman, Afiq Danial Abd Rasid, Lailatul Fitriyah Ahmad Shafii, and Suhail Kazi. "Global energy security and Malaysian perspective: A review." *Progress in Energy and Environment* 6 (2018): 1-18.

[12] Zaman, Nur Badriyah Kamarul, Wan Nur Aisyah Abdul Raof, Abdul Rahman Saili, Nur Nabila Aziz, Fazleen Abdul Fatah, and Selvakkumar KN Vaiappuri. "Adoption of Smart Farming Technology Among Rice Farmers." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 29, no. 2 (2023): 268-275. https://doi.org/10.37934/araset.29.2.268275

[13] Tey, Wah Yen, and Kiat Moon Lee. "Computational one-factor investigation on the effect of sonication parameters in biomass pretreatment." *Progress in Energy and Environment* 16 (2021): 18-35..

[14] Ibrahim, Fazdliel Aswad, Nurfadzillah Ishak, Jacqueline Kueh Yee Woon, Wong Boying, Mohd Wira Mohd Shafiei, Radzi Ismail, and Rafiza Abdul Razak. "Virtual Technology (VR) Attractiveness Attributes in Influencing House Buyers' Intention to Purchase." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 29, no. 2 (2023): 126-134. https://doi.org/10.37934/araset.29.2.126134

[15] Nathan, Shelena Soosay, Kuan Jung Ying, Lim Hui Wen, and Lim Xin Weoi. "Design of Smart Walking Shoe for Visually Impaired People." *Journal of Advanced Research in Applied Mechanics* 101, no. 1 (2023): 53-61. https://doi.org/10.37934/aram.101.1.5361

[16] Iqbal, Muhammad Saqib, Zulhasni Abdul Rahim, and Syed Aamer Hussain. "Digital Disruption and COVID-19: A Review on the Paradigm Shift in Pakistan." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 24, no. 1 (2021): 28-36. https://doi.org/10.37934/araset.24.1.2836

[17] Ali, Firkhan Ali Bin Hamid, and Mohd Zalisham Jali. "Human-technology centric in cyber security maintenance for digital transformation era." In *Journal of Physics: Conference Series*, vol. 1018, no. 1, p. 012012. IOP Publishing, 2018. https://doi.org/10.1088/1742-6596/1018/1/012012

[18] Khattak, Muhammad Adil, Muhammad Khairy Harmaini Shaharuddin, Muhammad Saiful Islam Haris, Muhammad Zuhaili Mohammad Aminuddin, Nik Mohamad Amirul Nik Azhar, and Nik Muhammad Hakimi Nik Ahmad. "Review of cyber security applications in nuclear power plants." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 7, no. 1 (2017): 43-54.

[19] Firkhan Ali, H. A., Maziah Na'aman, "Vulnerability Assessment on the Network Security" in *NCSTIE 2006: Proceedings of the International Conference on Science and Technology 2006. PWTC, UiTM Pulau Pinang* (2006).

[20] Ali, Firkhan. "H. A etl.,"Development Of Dual-Factor Authentication For Web Based Application Using SMS"." *Proceedings of the ICITS* (2008).

[21] Ali, Firkhan Ali Bin Hamid, and Yee Yong Len. "Development of host based intrusion detection system for log files." In *2011 IEEE Symposium on Business, Engineering and Industrial Applications (ISBEIA)*, pp. 281-285. IEEE, 2011. https://doi.org/10.1109/ISBEIA.2011.6088821