International Science and Technology Journal
المجلة الدولية للعلوم والتقنية

عدد خاص بالمؤتمر الليبي الدولي للعلوم التطبيقية و الهندسية دورته الثانية
LICASE -2
2024 / 10 / 30-29

المجلة الدولية للعلوم والتقنية
ISTJ

تم استلام الورقة بتاريخ: 2/ 10/2024م
وتم نشرها على الموقع بتاريخ: 30/ 10/2024م

Evaluating Security Criteria for Web-Based Applications

Higher Institute of Science and Technology, Ragdalin Portal as a case study

http://www.doi.org/10.62341/amam2053

Elshrif Ibrahim Elmurngi*[1], Abdulrauf Albaghdadi Alklabi[2]

[1,2]Higher Institute of Science and Technology, Ragdalin
Department of Computer Technology

*Email: elshrifelmurnagi@gmail.com

Abstract
The security of a system is a critical issue that cannot be overlooked, no matter how well-designed the system may initially appear. This is because security involves protecting an organization's assets, which can range from tangible items like web pages and customer databases to intangible aspects such as the company's reputation. Given that security is a fundamental requirement, it is essential for organizations to incorporate security elements into their systems. A common system within organizations is the web-based application, which not only offers reliable services to users—both potential and existing customers—but also helps safeguard the organization's reputation and ensures the continuity of future business engagements. Currently, evaluations of web-based applications primarily focus on aspects such as usability, user satisfaction, and user acceptance, often neglecting the security evaluation aspect. This paper will discuss the criteria needed to evaluate web-based applications from a security perspective. The proposed criteria will be applied in evaluating the Higher Institute of Science and Technology, Ragdalin Portal, as a case study in which a website designer was interviewed and asked questions related to the proposed criteria to identify the security vulnerabilities of web-based applications. This research paper will include an analysis based on this evaluation, with the hope that these evaluations can be used to develop better security practices for both the Higher Institute of Science and Technology Ragdalin portal and web applications in general in the future.
Keywords: Web-based application, Higher Institute of Science and Technology, Ragdalin Portal, Security evaluation.

International Science and Technology Journal
المجلة الدولية للعلوم والتقنية

عدد خاص بالمؤتمر الليبي الدولي للعلوم التطبيقية و الهندسية دورته الثانية
LICASE -2
2024 / 10 / 30-29

المجلة الدولية للعلوم والتقنية
ISTJ

تم استلام الورقة بتاريخ: 2/ 2024/10م وتم نشرها على الموقع بتاريخ: 30/ 2024/10م

تقييم معايير الأمان للتطبيقات المستندة إلى الويب: بوابة المعهد العالي للعلوم والتقنية، رقدالين كدراسة حالة

الشريف إبراهيم المرناقي، [1]* [2]عبدالرؤوف البغدادي الكلابي

[1,2]المعهد العالي للعلوم والتقنية ، رقدالين

قسم تقنية الحاسوب

*البريد الالكتروني:elshrifelmurnagi@gmail.com

الملخص

إن أمن النظام يشكل قضية بالغة الأهمية لا يمكن إغفالها، مهما بدت جودة تصميم النظام في البداية. وذلك لأن الأمن ينطوي على حماية أصول المنظمة، والتي قد تتراوح من العناصر الملموسة مثل صفحات الويب وقواعد بيانات العملاء إلى الجوانب غير الملموسة مثل سمعة الشركة. ونظرًا لأن الأمن متطلب أساسي، فمن الضروري أن تدمج المنظمات عناصر الأمن في أنظمتها. ومن بين الأنظمة الشائعة داخل المنظمات تطبيق قائم على الويب، والذي لا يقدم خدمات موثوقة للمستخدمين فحسب – سواء العملاء المحتملين أو الحاليين – بل يساعد أيضًا في حماية سمعة المنظمة ويضمن استمرارية المشاركات التجارية المستقبلية. حاليًا، تركز تقييمات التطبيقات القائمة على الويب بشكل أساسي على جوانب مثل قابلية الاستخدام ورضا المستخدم وقبوله، وغالبًا ما تهمل جانب تقييم الأمان. ستناقش هذه الورقة المعايير اللازمة لتقييم التطبيقات القائمة على الويب من منظور أمني. سيتم تطبيق المعايير المقترحة في تقييم بوابة المعهد العالي للعلوم والتكنولوجيا، رقدالين، كدراسة حالة تم فيها مقابلة مصمم موقع ويب وطرح أسئلة تتعلق بالمعايير المقترحة لتحديد نقاط الضعف الأمنية في التطبيقات المستندة إلى الويب. ستتضمن ورقة البحث هذه تحليلاً يعتمد على هذا التقييم، على أمل أن يتم استخدام هذه التقييمات لتطوير ممارسات أمنية أفضل لكل من بوابة المعهد العالي للعلوم والتكنولوجيا، رقدالين وتطبيقات الويب بشكل عام في المستقبل.

الكلمات المفتاحية: تطبيق مستند إلى الويب، بوابة المعهد العالي للعلوم والتكنولوجيا رقدالين، تقييم الأمان.

1. Introduction

Currently, there are thousands of hosts providing applications and web services, with hundreds of thousands of web locations and custom-built web applications available on the Internet. Many of these were developed initially without considering application-level attacks, making them susceptible and difficult to secure. Despite ongoing efforts to enhance the security of these web applications and tools, new vulnerabilities are discovered and publicized each month, which can often be addressed. However, most of these tools highlight known vulnerabilities, focusing on specific severe issues without guaranteeing complete security.

تم استلام الورقة بتاريخ: 2/ 2024/10م
وتم نشرها على الموقع بتاريخ: 30/ 2024/10م

Fortunately, combining application security scanning tools with firewall devices can offer high-level protection for online commercial transactions involving web applications. A security model addresses the theoretical need to model information security, focusing on maintaining three critical information characteristics: privacy, integrity, and availability. Privacy ensures that information is shared only with authorized individuals or organizations, while integrity ensures that information remains accurate and complete, as explained by [1]. The evaluation criteria are standardized to specify what the evaluation sponsor (the person or organization requesting the evaluation) must provide and what the evaluator (the independent person or organization conducting the evaluation) must do. This standardization aims to ensure consistency and uniformity in evaluation results. For each evaluation area, the required documentation from the sponsor is identified, followed by criteria for each relevant aspect or phase of the evaluation.

There is a lack of research focused on evaluating web-based applications from a security perspective. Therefore, this research aims to establish criteria for evaluating web-based applications with a focus on security.

The rest of this paper is organized as follows. Section 2 presents the related works. Section 3 shows the methodology. Section 4 analysis and results, Section 5 presents the conclusion and future works.

1.1. Problem Statement

The significance of web-based applications is indisputable, as users rely on them to deliver their intended services effectively. These users, including both potential and current customers, represent valuable assets to a company. Therefore, web-based applications must maintain not only usability but also robust security. However, current evaluations of these applications predominantly emphasize usability, user satisfaction, and user acceptance, with insufficient focus on security assessment. This research seeks to address this gap by establishing criteria for evaluating the security of web-based applications.

1.2. Research Objectives

This research aims to accomplish the following objectives:

1- Propose criteria specifically designed to evaluate the security of web-based applications.

2- Apply the proposed security evaluation criteria to the Higher Institute of Science and Technology's Ragdalin Portal as a case study.

3- To provide some analysis based on the security evaluation performed in the case study.

2. Related Work

The primary goal of the related work section is to update you and the readers on the current knowledge and ideas in the field, including diverse perspectives and viewpoints. Additionally, the literature review provides a foundation for defining and defending your research topic. It helps explain how your research fits into the broader context and justifies your approach to the topic. The related work involves the following steps:

تم استلام الورقة بتاريخ: 2/ 10/2024م وتم نشرها على الموقع بتاريخ: 30/ 10/2024م

2.1 Web-based application

Non-browser-based applications are relatively uncommon but can be useful in specific scenarios. Some desktop applications, such as download managers like DAM [2], support HTTP and can be considered non-browser-based applications. While web browsers themselves are desktop applications that communicate with web servers via HTTP, similar desktop applications can act as client components to access web servers and utilize web services. The advantage of native desktop applications over browser-based ones is that they can offer rich and complex GUIs and can be developed with less effort compared to browser-based web applications.

The role-based access control (RBAC) model for web-based applications extends traditional RBAC from a single enterprise domain to web implementations. In the context of the Internet, establishing trust is crucial for users engaging in sensitive transactions without pre-established trust, which is vital for e-commerce. The RBAC model and XML-based ORBAC security policy can be applied to define security policies for web-based applications, as outlined by [1].

Web-based applications present unique testing challenges compared to traditional applications due to their heterogeneous components, which arise from various technologies and programming models, and the diverse environments in which they operate, including different host platforms and browsers. Additionally, the global and distributed nature of web application users and the capability to generate software components at runtime add complexity to testing. Many research projects, including those by [3] have focused on defining test models, typically using object models and state machine models, to address these challenges.

2 .2 Current evaluation methods for web-based application

Students are notified about the web-based course evaluation process through their university-assigned email addresses. However, this method poses a challenge since it cannot be guaranteed that students regularly check their university emails. To address this issue, advertisements are placed in the campus newspaper, and posters are displayed in the engineering buildings' hallways to announce the commencement of the web-based evaluation process. Additionally, faculty members are encouraged to inform their classes about the online course evaluation. The primary advantages of web-based course evaluations include the flexibility and consistency of evaluation items, the immediate availability of evaluation data to aid faculty and departments in course planning, and the storage of data for trend analysis, as noted by [6].

[4] conducted a comprehensive analysis of usability evaluation methods in the Web domain. Their findings revealed significant gaps in the currently utilized evaluation methods. Due to the complexity of web artifacts, no single method was deemed universally applicable for all situations. Consequently, usability evaluation methods are

continuously revised to address all aspects of usability across various categories of software applications.

2.3 Importance of evaluating web-based application

[7] Emphasize that the extent to which a web-based evaluation instructional system can be automated and tailored to meet the specific needs of a particular library is crucial in its development. The EMIS approach, characterized by its descriptive and unidirectional nature, guides users through a set of pre-developed instructional modules. These modules, being general in nature, may not fully address the unique needs of a specific library and its evaluation requirements. On the other hand, according to [8] evaluating the quality of websites is essential for effectively browsing interesting sites. A website is often viewed as a scientific showcase when considering an institution. The most common strategy adopted by some approaches is to understand the type of website to propose relevant criteria. For instance, a website facilitating payment transactions [12] will not be evaluated with the same characteristics as an academic site [10].[8] provides a literature review to identify the purposes of recent research, determine the affected categories, and propose a process for extracting criteria for evaluating websites based on a review of existing studies.

2.4 Security for Web-Based application

Some papers address security issues but do not thoroughly examine web application security tools. Security in web applications is a critical issue that requires careful attention.

Various solutions can be implemented to enhance security services in web applications. Although no solution is entirely perfect, these measures act as preventive steps against potential threats. One effective solution is the implementation of a Web Application Firewall (WAF). A WAF helps monitor and filter traffic between a web application and the internet, providing insights into packet data traffic and blocking various attacks. According to the OWASP Top Ten list, the most prevalent attacks include Injection, Cross-Site Scripting (XSS), and Broken Authentication and Session Management [9] These attacks typically target web servers, making the role of WAFs crucial in mitigating such threats.

Many verification tools have successfully discovered previously unknown vulnerabilities in legacy C programs, suggesting that similar success could be achieved with web applications. A key difference is that vulnerabilities in C or Java often result from improper control flow, whereas web application vulnerabilities typically arise from insecure information flow, which encryption or traditional web access control models cannot adequately address [7]. Securing web services involves considering five fundamental areas: message-level protection, message privacy, parameter checking, authentication, and authorization. It is important to evaluate these aspects within the context of network services rather than network security itself, as network security pertains to a different layer of the ISO model. Some solutions employ similar

technologies, which were initially developed for network services and have been in use for many years [5].

2.5 Evaluate security criteria for web-based applications

To assess security criteria for web-based applications using a portal as a case study, we can examine various dimensions such as authentication, authorization, data protection, secure communication, and vulnerability management.

[13] conducted a comprehensive survey of recent research in web application security. They outlined the unique characteristics of web application development, identified key security properties that should be preserved, and categorized existing works into three major classes. Additionally, they highlighted several open issues that still need to be addressed.

Although numerous research studies have been conducted on web application security evaluation, few attempts have been made to establish a systematic approach that quantifies the results. Below are several papers that discuss this research area:

[14] introduced a security evaluation framework for web-portal security assessment, which integrates ISO/IEC 15408 [15] and the OWASP evaluation model Common Criteria Web Application Security Scoring (CCWAPSS) [16] This framework uses a scoring system to assess the significance of each factor within the criteria, facilitating numerical rankings. As a result, it provides practical security evaluations that web portal developers can quickly understand and implement.

[17] proposed a quantitative security evaluation approach for software systems from the vendor's perspective, focusing on the analysis of collectible vulnerability data. They applied a stochastic model using a non-homogeneous Poisson process to explain this data and used numerical examples to evaluate the security measures relative to the content management system of an open-source project.

[18] developed a method for computing the security qualities of software architectures using security patterns. The core metric in this evaluation was threat coverage, and they proposed an algorithm to aggregate low-level measures associated with these patterns into a single high-level indicator.

[19] presented a hierarchical structure for web service security, complete with a model that evaluates various aspects of security from an analytical perspective. They used the Analytical Hierarchy Process (AHP) theory to prioritize and weight critical security properties, such as authorization, confidentiality, and availability, allowing for greater customization according to provider/consumer needs.

Currently, evaluations of web-based applications are primarily focused on usability, user satisfaction, and user acceptance. There is a lack of research that concentrates on evaluating web-based applications from a security perspective. Therefore, this research aims to develop criteria to support the evaluation of web-based applications from a security perspective and provide an analysis based on the security evaluation conducted in the case study.

3. Methodology

The methodology consists of four distinct phases: planning, information gathering, implementation, and analysis, each interconnected to ensure a comprehensive evaluation. This research focuses on assessing web-based applications from a security perspective, with the analysis of the case study serving as a key output for this research (Refer to Figure 1).

3.1 Planning

This section will discuss the findings and analysis conducted during the study. The study's objectives were to propose criteria for the security evaluation of web-based applications and validate these criteria through a case study. The Higher Institute of Science and Technology's Ragdalin Portal was selected as the web-based application for this case study. Interviews were conducted with staff at the institute's Computer Center to gather information on the evaluation of the web-based application. Subsequently, the analysis summarizing the case study findings from the interviews will be presented.

3.2 Information Gathering

The second phase was information gathering, aimed at obtaining a comprehensive understanding of the project. This involved reviewing academic papers, theses from previous researchers, and various case studies to support the literature review. The information gathered provided valuable insights and raised pertinent questions that guided the researcher in successfully conducting the study. After collecting the necessary information, the researcher conducted content analysis, a technique used to analyze the collected data. This content analysis formed a crucial foundation for the implementation phase.

3.3 Implementation

The third phase is the implementation phase. Based on the content analysis, the researcher identified several criteria for evaluating web-based applications. These criteria will be detailed and thoroughly explained in the analysis and findings section. Using these criteria, the researcher conducted interview sessions with staff at the Higher Institute of Science and Technology's Ragdalin Computer Center to gather information about the Ragdalin Portal, a specific example of a web-based application. The output from these interviews was analyzed, and the results are discussed in the analysis and findings section.

3.4 Analysis

The final phase of this study involved analyzing the case study conducted on the Higher Institute of Science and Technology's Ragdalin Portal, serving as an example of a web-based application. This analysis was based on the information gathered during the interview sessions with a website designer at the omputer Center of the Higher Institute of Science and Technology's Ragdalin. The interview material was adapted from the framework of vulnerability categories suggested by [7] With the analysis included in the next section, the researcher is considered to have successfully achieved the three objectives established in the planning phase.

4. Finding and analysis

This section will discuss the findings and analysis conducted during the study. The study's objectives were to propose criteria for the security evaluation of web-based applications and validate these criteria through a case study. The Higher Institute of Science and Technology's Ragdalin Portal was selected as the web-based application for this case study. Interviews were conducted with a website designer at the Computer Center of the Higher Institute of Science and Technology's Ragdalin to gather information on the evaluation of the web-based application. Subsequently, the analysis summarizing the case study findings from the interviews will be presented.

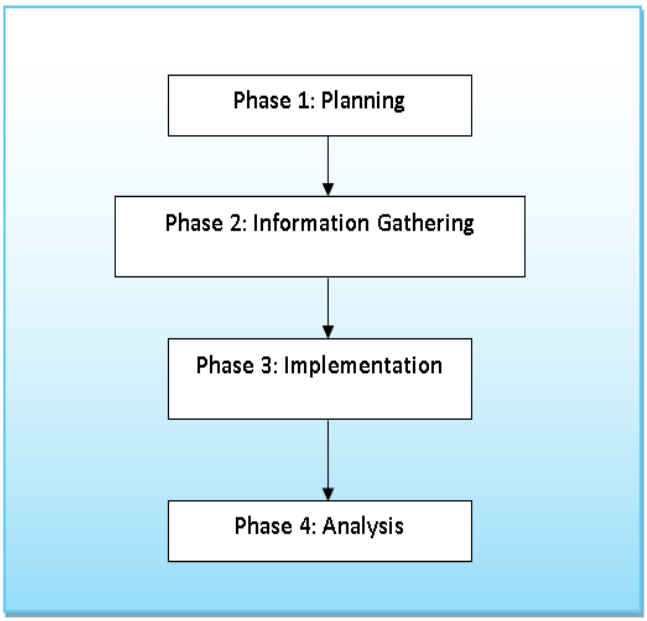

Figure 1: Research Methodology

4.1 Validated criteria by Categories

The criteria for evaluating web-based applications are categorized to ensure consistent focus on the key design and implementation choices that most impact the application's security. These validated criteria, organized by categories, are detailed in TABLE 1.Additionally, a thorough analysis of application-level threats can be achieved by organizing them according to application vulnerability categories, as described in TABLE 2.

Input validation

Input validation becomes a security concern if an attacker identifies that your application assumes certain types, lengths, formats, or ranges for input data without verification. The attacker can then exploit these assumptions by supplying specially crafted input to compromise your application.

تم استلام الورقة بتاريخ: 2/ 2024/10م
وتم نشرها على الموقع بتاريخ: 30/ 2024/10م

Authentication

There are different ways to verify someone's identity for your system, but picking the wrong one or setting it up poorly can leave security holes that hackers can sneak through.

Authorization

The system checks a user's ID and role to see if they're allowed to use something specific, like a file or program.

Configuration management

Many programs offer tools for administrators to manage settings, update content, and carry out regular maintenance tasks.

Sensitive data

Important information is vulnerable to different dangers. Hackers can try to steal or change this data by attacking the places it's stored (like databases) and the ways it travels (like networks).

Session management

Web applications handle keeping track of user sessions, and this plays a vital role in keeping the application secure overall.

Cryptography

To keep information confidential, most applications rely on cryptography that scrambles and protects the data.

Parameter manipulation

Hackers can mess with a web application's conversations with users by modifying data sent back and forth. This can involve tinkering with various parts of the communication, like website addresses, form entries, cookies, and HTTP headers, and even hidden instructions.

Exception management

When errors happen in a web application and the user sees the exact error message, it can be like giving a robber a blueprint of your house. This information might not be helpful to the average person, but attackers can use it to find weaknesses and potentially break in. In addition, if the application doesn't handle errors properly, attackers might be able to crash it completely.

Auditing and logging

Keeping track of user activity (auditing and logging) helps catch strange behavior early on, like someone trying to figure out the system (footprinting) or repeatedly guessing passwords. This can stop them before they do any real damage. It also helps prove who did what (deal with repudiation) if something suspicious happens.

TABLE 1.Validation criteria by categories

No. Category	Categories	Definition
C 1	Input validation	Input validation refers to how your application filters, scrubs, or rejects input before additional processing.
C2	Authentication	Authentication is the process that an entity uses to identify another entity, typically through credentials such as a username and password.
C3	Authorization	Authorization is the process that an application uses To control access to resources and operations.
C4	Configuration Management	Configuration management refers to how your application handles these operational issues.
C5	Sensitive Data	Sensitive data is information that must be protected either in memory, over the wire, or in persistent stores. Your application must have a process for handling sensitive data.
C6	Session Management	A session refers to a series of related interactions between a user and your Web application. Session management refers to how your application handles and protects these interactions.
C7	Cryptography	Cryptography refers to how your application enforces confidentiality and integrity.
C8	Parameter Manipulation	Parameter manipulation refers to both how your application safeguards tampering of these values and how your application processes input parameters.
C9	Exception Management	Exceptions that are allowed to propagate to the client can reveal internal implementation details that make no sense to the end user but are useful to attackers.
C10	Auditing and Logging	Auditing and logging refer to how your application records security-related events.

4.2 Analysis of results

A website designer at the Higher Institute of Science and Technology, Ragdalin, was interviewed. Based on the information obtained, an analysis was conducted to identify security weaknesses in their web portal. The goal was to uncover common problems by identifying patterns in the findings. These problems were then grouped into categories for more organized resolution. TABLE 1. was used to define these categories. After

reviewing the interview results Table (2), most categories showed security issues ("Yes"), while a few did not ("No").

The question arises: why do most categories in Table (2) indicate "Yes," while a few indicate "No"?

I will explain that one by one. If you look at TABLE 2. you will find that categories such as (Q1-C8), (Q2-C1), (Q3a-C6), (Q3b-C9), (Q4-C4), (Q5-C4), (Q6-C4), (Q7a-C2), (Q7b-C3), (Q9a-C9), (Q9b-C9), and (Q10-C10) indicate "Yes" because the answers to the questions in these categories conform to the descriptions in TABLE 1. However, categories such as (Q3b-C6), (Q7c-C5), (Q8-C3), (Q10a-C10), and (Q10b-C10) indicate "No" because the answers to the questions in these categories do not conform to the descriptions in TABLE 1.

Moreover, Figure 2 shows the count of numbers Categories by the enforcement of security elements. It reveals that 10 items on security issues are applied in the security process and indicated as "Yes," while 5 items are not included in the security process and indicated as "No."

TABLE.2. Results of analysis

No. Category	Enforcement of security elements Yes	Enforcement of security elements No
(Q1-C8)	Yes	
(Q2-C1)	Yes	
(Q3a-C6)	Yes	
(Q3b-C6)		No
(Q4-C4)	Yes	
(Q5-C4)	Yes	
(Q6-C4)	Yes	
(Q7a-C2)	Yes	
(Q7b-C3)	Yes	
(Q7c- C5)		No
(Q8-C3)		No
(Q9a-C9)	Yes	
(Q9b-C9)	Yes	
(Q10a -C10)		No
(Q10b -C10)		No

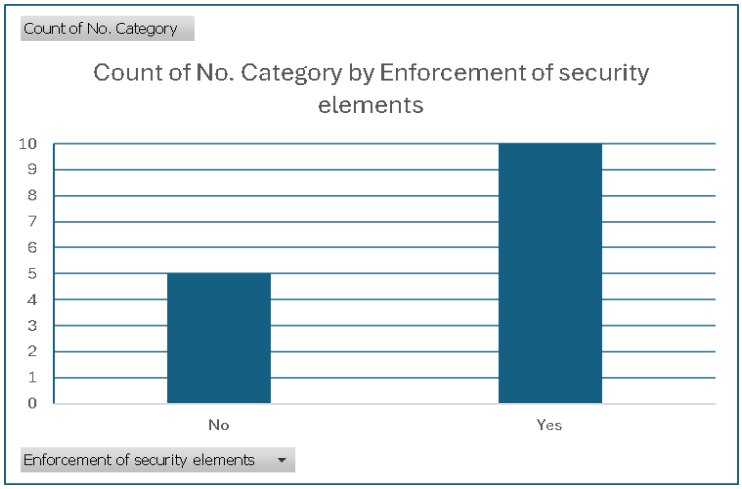

Figure 2: Count of No. Category by Enforcement of security elements

The results of this study proved that 70%, or 10 out of 15 items on security issues, are applied in the Higher Institute of Science and Technology, Ragdalin website, while 30%, or 5 out of 15 items, are not included in the security process.

The analysis of the Higher Institute of Science and Technology, Ragdalin web portal, revealed security gaps, particularly in authorization, cryptography, and parameter manipulation. These weaknesses stem from unanswered interview questions related to these security elements, suggesting a potential lack of security expertise or inadequate security staffing to comprehensively address all security aspects and ensure the portal's complete security.

5. Conclusion and Future Work

The interview with a website designer at the Higher Institute of Science and Technology Ragdalin indicates an awareness of security issues in the web portal. This suggests that the Higher Institute of Science and Technology Ragdalin might need more personnel to handle security monitoring and reviews, ensuring system safety. To improve user trust and overall reliability, the web application's security needs to be strengthened. After all, the success of any web application environment hinges on a strong security foundation.This study highlights the importance of detailed security criteria for web applications, particularly those relevant to the Higher Institute of Science and Technology Ragdalin portal. The hope is that these criteria can be used to develop better security practices for both the Higher Institute of Science and Technology Ragdalin portal and web applications in general. In the future, we will apply the proposed criteria to universities, higher institutes, or other organizations to evaluate their web-based applications from a security perspective

References

[1]. Wang, A. J. A. (2005). Improving Web Application Security. Proceedings of the 43rd Annual Southeast Regional Conference (ACM-SE 43). Retrieved May 8, 2007, from http://portal.acm.org.eserv.uum.edu.my/citation.cfm?id=1167295&coll=Portal&dl=GUIDE&CFID=22966583&CFTOKEN=61740085

[2]. Corporation, T. (2016). Download Accelerator Manager. [Online] Available at: http://www.damdownloader.com/ [Accessed 20 Nov 2015]. J. Jennings, Modeling of the fates and acute biological effects of the spilled oil on the water column, final report, April (2002),pp1-33.

[3]. Di Lucca, G. A. (2005). Testing Web-Based Applications: The State of the Art and Future Trends. Proceedings of the 29th Annual International Computer Software and Applications Conference (COMPSAC'05), IEEE.P.Vethamony, K.Sudheesh, Trajectory of an oil spill of goa, eastern Arabian sea: Field observation and simulations, Environmental pollution 148 (2007) pp. 438-444.

[4]. Fernandez, A., Insfran, E., & Abrahão, S. (2011). Usability evaluation methods for the web: A systematic mapping study. Information and Software Technology, 53(8), 789-817.

[5]. John, T., et al. (2006). Web-based Evaluation Instructional Systems. FSU Information Institute.RetrievedMay2,2007,from http://www.ii.fsu.edu/presentations/evalmod_arl2006.pdf

[6]. McGourty, J., Scoles, K., & Thorpe, S. (2002). Frontiers in Education, 2002. FIE 2002. 32nd Annual, 1, T1B-17 - T1B-22.

[7]. Meier, J. D., Vasireddy, S., Dunner, M., Escamilla, R., & Murukan, A. (2003). Improving Web Application Security: Threats and Countermeasures. Retrieved May 8, 2007, from http://www.cgisecurity.com/lib/Threats_Countermeasures.pdf.Yender, Fate and effect of oil and routes of exposure to commercial fisheries report, June (2006),pp.9-14.

[8]. Park, J. S., & Sandhu, R. (2001). Role-Based Access Control on the Web. ACM Transactions on Information and System Security, 4(1), 37-71.

[9]. Rim Rekik, R., Kallel, I., Casillas, J., & Alimi, A. M. (2018). Assessing web sites quality: A systematic literature review by text and. International Journal of Information Management, 201-216.

[10]. Sullivan, B., & Liu, V. (2012). Web Application Security: A Beginner's Guide. New York: The McGraw-Hill Companies.

[11]. Violante, M. G., & Vezzetti, E. (2015). Virtual interactive E-learning application: An evaluation of the student satisfaction. Computer Applications in Engineering Education, 23, 72–91

[12]. Chen, J. V., Rungruengsamrit, D., & Rajkumar, T. M. (2013). Success of electronic commerce Web sites: A comparative study in two countries. Information and Management, 50, 344–355.

[13].Nguyen, T. P., & King, I. (2021). Web application vulnerability detection: A survey. IEEE Transactions on Reliability, *70*(2), 548-568.

[14]. Hai, H. D., & Nga, P. T. (2018). Evaluating the security levels of the Web-Portals based on the standard ISO/IEC 15408. In Proceedings of the 9th International Symposium on Information and Communication Technology.

[15]. ISO/IEC. (2023). Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model. Retrieved from ISO. (Accessed on Jan. 21, 2023).

[16]. Charpentier, F. (2023). Common Criteria Web Application Security Scoring (CCWAPSS). Retrieved from Packet Storm Security. (Accessed on Feb. 3, 2023).

[17]. Okamura, H., Tokuzane, M., & Dohi, T. (2013). Quantitative security evaluation for software system from vulnerability database.

[18]. Yautsiukhin, A., et al. (2008). Towards a quantitative assessment of security in software architectures. In Nordic Workshop on Secure IT Systems (NordSec), Copenhagen, Denmark.

[19]. Banaei, O., & Khorsandi, S. (2012). A new quantitative model for web service security. In 2012 IEEE 14th International Conference on Communication Technology (pp. 201-206). IEEE.