[1]Aristotel Aaron Agpaoa

[2]Lhester P. Cariaga

[3]Jona Marie T. Mariano

[4]Richard Monreal

Development and Employment of Cyber Security of e201 File Web Application for Data Center College of the Philippines of Laoag City, Inc.

JES Journal of Electrical Systems

Abstract: **-** Web-based systems in today's interconnected world play a vital role and need of enhanced cybersecurity measures to protect sensitive information since cybercrimes are increasing rapidly. The focus of the study is on the development of an e201 file web application for the Data Center College of the Philippines which will be accessed through a web browser. The objective study is to evaluate the cybersecurity of the developed application, particularly in handling essential personnel records using confidential data OWASP ZAP security testing tool and its software quality based on ISO 25010 specifically in software functionality, usability, and security to determine if it is ready for live deployment. The study utilizes the Research and Development model as its research design to achieve its purpose. The conceptual framework of the study utilized the used of Input-Process-Output model and the Agile Iterative model in the development. The result of the security testing and suggestions of the OWASP ZAP, cyber security was employed in the web application including Content Security Policy Header, HTTOnly Cookie flags, SameSite attribute, X-Content-Type-Options Header, and Anti-CSRF Token. With an overall mean of 4.41 in the result of Users Acceptance Testing, it implies that the system is a great help for the institution. The positive feedback received from evaluators confirmed that the development of the e201 files web application were successful. This study implies that utilizing the OWASP Zap is a great help in strengthening cybersecurity and ISO 25010 in the software quality assurance of web applications of educational institutions.

Keywords: Web application, Cybersecurity, Development, OWASP ZAP and ISO 25010.

INTRODUCTION

In today's interconnected world, web-based systems are one of the technologies that play a vital role in the improvement and expansion of institutions and organizations [1]. This kind of system might face numerous security challenges that require improved measures to protect sensitive information and infrastructure since cybercrimes are increasing rapidly as days go by [2]. The Data Center College of the Philippines of Laoag City, Inc., must address a range of security concerns to safeguard its assets and maintain the trust of its stakeholders.

The study aims to develop a proposed e201 file web application for the Data Center College of the Philippines a PHP web application that will be deployed in a hosting server and accessible through a web browser provided with an internet connection and evaluate the cyber security of the developed application. The proposed Electronic 201 files will contain essential personnel records and confidential data. These data handled by the web application should be secure and require robust security measures to protect them from cyber threats. Implementing effective cybersecurity measures in the web application handling electronic 201 files is crucial to safeguarding the privacy and integrity of this sensitive information.

REVIEW OF RELATED LITERATURE

The importance of raising awareness about cybersecurity issues and enhancing digital literacy to recognize and manage threats effectively. Service-oriented architecture (SOA) offers numerous benefits, such as increased efficiency and open access to applications and services. However, this openness also creates significant security

[1] College of Information Technology and Computer Science, University of the Cordilleras, Baguio City

[2]College of Information Technology and Computer Science University of the Cordilleras, Baguio City

[3]College of Information Technology and Computer Science University of the Cordilleras, Baguio City

[4]College of Information Technology and Computer Science University of the Cordilleras, Baguio City

[1] arisaaronagpaoa@gmail.com[2]lcariaga.data@gmail.com, [3]jtm8995@students.uc-bcf.edu.ph, and [4]rnmonreal@uc-bcf.edu.ph

challenges for organizations. On addressing the security challenges of SOA, considering both their business and technical impact. It maps out mitigation measures and tools to counter these challenges. The process involves identifying major security vulnerabilities and researching preventive solutions for cyber-attacks. Additionally, it suggests business-level measures to mitigate cybersecurity risks and vulnerabilities in SOAs. To enhance security in the context of SOA implementations [3].

The increasing use of online proctored examinations in academic and professional settings highlights the role of AI and Machine Learning technology in supporting authentication, authorization, and operational control of these systems. It focuses on mitigating cybersecurity vulnerabilities associated with online proctoring systems (OPS) through administrative, physical, and technical controls. Two classes of OPS are considered: fully automated AI-enabled systems and hybrid systems that combine automated AI with live proctors. The online proctoring systems explore methods for multi-factor authentication and authorization, including challenge-response, and biometrics (face and voice recognition). Operational controls are discussed, covering lockdown browsers, webcam detection of fraud indicators, endpoint security, VPN and VM usage, screen-sharing, keyboard listening programs, and other technical measures to address spatial control issues [4].

METHODOLOGY

This study's main purpose was to develop an e201 file web application for DCCP and evaluate its cybersecurity. To realize this objective, the Research and Development (R&D) model also called the research-based development method was used.

The conceptual framework of the study utilized the used of Input-Process-Output (IPO) model. The input has two components: problems encountered in the manual process of managing employee information and documents of the institution and the features and functions of the e-201 file. The process is made up of stages that the proponents take to develop the system using interviews, survey questions, data gathering and data analysis, and the agile methodology. The output of the study is the "e-201 File", which will be a web-based system for the Data Center College of the Philippines.

INPUT	PROCESS	OUTPUT
• The problems encountered in the manual process of managing the employee information and documents. • The functions and features of e-201 file.	• **Data Gathering and Data Analysis** • **Iterative Method** • Planning • Design • Implementation • Testing • Evaluation • Deployment· • **Cyber Security Testing** • **User Acceptance Testing**	**e-201 File Web Application**

Figure 1. Conceptual Framework.

In the development of the system, Agile Software Development was used. The Iterative approach in Agile Software Development that emphasizes early, straightforward implementation before progressively adding complexity and a wider feature set until the whole system is produced. Implementing iteratively provides flexible scope modifications based on user and client feedback. This approach adds flexibility to the delivery model by enabling development team to reprioritize and implement changes to raise the value of the final web application [9].

Figure 2 illustrates the web application's iterative development process, which includes various phases, including planning, design, programming, testing, deployment, and feedback.

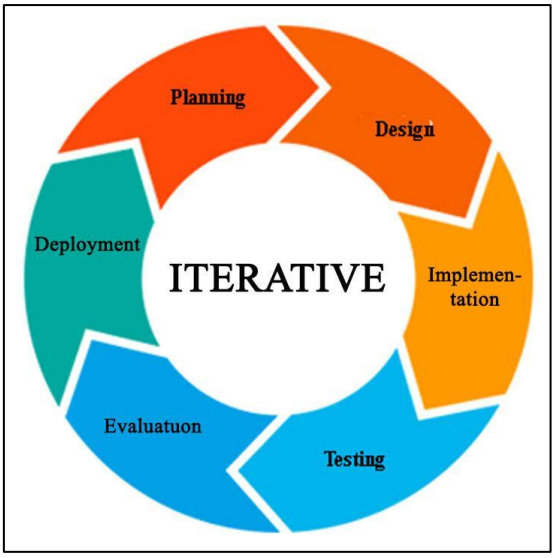

Figure 2. Iterative Model

Planning phase

This phase's goals include learning more about the issue statement, identifying potential solutions, and estimating the resources, costs, timelines, and other factors that need to be taken into account at this point. Interviews with the study's participants and organizations are done by the researcher. These interviews aided the researcher in identifying the issues found with the current system and helped them come up with improvements.

Design phase

The purpose of this phase is to turn all requirements into a thorough and detailed system design specification that addresses every one of the system's components. The researcher worked to implement the ideas and choices, taking into account system constraints, software platform interfaces, and system documentation.

Implementation Phase

Researchers created code and translated design documentation into actual software during the software development phase. A variety of programming languages and editing software are used to create the program. Additionally, encryption techniques will be employed to protect user's data stored within the system.

Testing Phase

The researcher thoroughly evaluated the system. This enables the entire team, as well as users or other external stakeholders, to assess where the project was, where it should be, what can or should be changed, and so on. Before installation, this phase establishes the system's benefits and drawbacks.

Any form of software may be subjected to software security testing as part of the software development life cycle (SDLC). Its major objective is to identify security holes and vulnerabilities in a piece of software [5]. To test the e201 web application cybersecurity, this study will use OWASP ZAP, an open source for web application vulnerabilities. The ZAP is an integrated penetration testing tool for web application vulnerabilities, suitable for developers and functional testers with diverse security experience. It offers automated scanners and manual vulnerability detection tools [6]. The OWASP methodology overview includes understanding the framework, highlighting the critical security risks faced by web applications, and defining the scope and objectives of implementing security measures. According to reports, vulnerability information with the following risk categories high level, medium levels, low levels, and informational can be obtained by scanning with the ZAP tool [7]. The researcher conducted a comprehensive assessment through secure code reviews and utilizing the OWASP to implement cyber security to ensure data confidentiality, prevent leakage, and ensure intended functionality is maintained in the web application [8].

Deployment Phase

The researcher will be deployed online using a paid server host. The researcher will conduct cyber security testing and execute the pilot testing of the application to identify the user's response according to the overall usability and functionality of the application. Once the product is tested and ready to launch, the researcher follows the process and procedures to ensure the code and technology are deployed properly.

User's Acceptance Testing

The developed application will be undergoing User Acceptance Testing where a questionnaire checklist based on ISO 25010 will be used to check the usability.

In the pilot testing process, the researchers deployed first the system, gave basic orientation and training on how the system works users then gave the research questionnaire for the users to answer. The user's acceptance test questionnaires were based on the ISO/IEC 25010 which is considered as the cornerstone of a product quality evaluation system. The said questionnaire assessed the three (3) characteristics of a system. The characteristics are as follows:

- **Functional Sustainability**. The extent in which the system satisfies the stated requirements by the end-users.
- **Usability**. The extent to which certain users can effectively, efficiently, and satisfactorily utilize the software to achieve specified goals in a certain condition.
- **Security**. The level to which software and data are protected so that users may access the right information based on their level of accessibility.

RESULTS AND DISCUSSION

With the developed e201 File Web Application System for DCCP (Data Center of the Philippines of Laoag City, INC), the researchers presented the cyber security threats results with the use of OWASP ZAP tool and the User's Acceptance Test Result with the usability of the Web Application.

OWASP ZAP Results.

Figure 3 presents the security risk results using the Owasp Zap security testing tool in the newly developed e201 file application. This includes the absence of Anti-CSRF Tokens and Content Security Policy (CSP) Header Not Set with Medium Level Security Risk; Cookie No HttpOnly Flag, Cookie without SameSite Attribute, Cross-Domain JavaScript Source File Inclusion and X-Content-Type-Options Header Missing with Low-Level Security Risk; and Loosely Scoped Cookie, Modern Web Application and Session Management Response Identified under Information Level Security Risk.

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	1
Content Security Policy (CSP) Header Not Set	Medium	1
Cookie No HttpOnly Flag	Low	1
Cookie without SameSite Attribute	Low	1
Cross-Domain JavaScript Source File Inclusion	Low	14
X-Content-Type-Options Header Missing	Low	1
Loosely Scoped Cookie	Informational	1
Modern Web Application	Informational	2
Session Management Response Identified	Informational	1

Figure 3. OWASP ZAP Results in Newly Develop e201 Files Web Application System.

Figure 4 presents the security risks results using OWASP Zap security testing tool after the alteration of codes to remove the security risks in the e201 file Web Application System which only shows one informational Risk

Level that according to the description in of the testing tool it no longer needs any changes which means that under Cyber Security the Web Application is ready to launch.

Name	Risk Level	Number of Instances
Modern Web Application	Informational	1

Figure 4. OWASP ZAP Results in e201 Files Web Application System After Alteration of Code.

The Employed Cyber Security for the e201 file Web Application

Based on the security vulnerabilities needed for the developed application, cybersecurity has been employed in the system which includes employing Content Security Policy (CSP) headers, the HttpOnly flag is set for all cookies, SameSite attribute is set to either 'lax' for all cookies and Anti-CSRF tokens to prevent Session Hijacking and Cross-Site Scripting (XSS) attempts, the web application server sets to Content-Type header appropriately, and the X-Content-Type-Options header sets to 'nosniff' to prevent Multipurpose Internet Mail Extensions (MIME) Sniffing in older version of web browsers that causing to interpret the body of web pages.

Content Security Policy Header

In the e201 files web application for DCCP made with PHP, the Content Security Policy (CSP) header is employed to mitigate Session Hijacking. The CSP header is set to restrict the sources from which content, scripts, and other resources can be loaded, thereby preventing unauthorized access and execution of malicious scripts. It enforces a strict policy on allowed domains, inline scripts, and other potential attack vectors. By doing so, it fortifies the application against session-related vulnerabilities and XSS attempts, enhancing the overall security and protecting user data from potential exploitation.

HttpOnly Cookie

The HttpOnly flag is set for all cookies to all the pages in e201 File Web Application to prevent cookies to be accessed by JavaScript. If a malicious script is able to execute on the sites, the cookie becomes accessible and can be sent to another site. If it's a session cookie, session hijacking is potentially possible.

SameSite Attribute

SameSite attribute is set to 'lax' for all cookies in e201 File Web Application will allow most cross-domain cookie-sharing if they are originating from a top-level GET request, SameSite prevents the cookie to be sent as a result of a 'cross-site' request. The SameSite property defends against cross-site request forgery, cross-site script entry, and timing attacks.

X-Content-Type-Options Header

The X-Content-Type-Options header was set to 'nosniff' to prevent Multipurpose Internet Mail Extensions (MIME) Sniffing. This prevents earlier Web Browser versions from doing Multipurpose Internet Mail Extensions (MIME) sniffing on the response body, which might result in the response body being interpreted and presented as a content type different than the defined content type.

Anti-CSRF Token

The e201 files web application employs an Anti-CSRF (Cross-Site Request Forgery) token to prevent Cross-Site Scripting (XSS) attacks. The Anti-CSRF token is a unique, unpredictable value inserted into forms and requests. When users submit forms like the user sign-in form, the application validates the token's authenticity to ensure the request originated from the expected source. This defense prevents malicious attempts to execute unauthorized actions through manipulated forms or scripts. By implementing this security measure, the application safeguards against XSS attacks that could otherwise exploit user interactions and data, enhancing the overall protection and reliability of the web application.

Users Acceptance Testing Results

The intended users of the web application are the employees of the institution were in 72 faculty members and 10 staff from the Data Center College of the Philippines of Laoag City Inc were involved in the software testing evaluation. The result of the users' acceptance testing is shown in table 1.

For the functional sustainability characteristic evaluation result in which the application should provide functions that need or meet the end-user's requirements with a mean of 4.50 which implies that the web application is functionally sustainable in where in the application can completely do its specified tasks with appropriate and accurate information, especially in storing and retrieving employee's documents.

For the usability characteristic evaluation result in which the end-users should able to use the web application with effectiveness, efficiency, and satisfaction. With the mean of 4.32, the result indicates that the web application is easy to navigate within its simple design which prevents the end-users to commit errors, is accessible, and is designed for employees and administrators of the institutions.

Lastly, for the security characteristic evaluation result in which the end-users have different levels of accessibility or authorization in the system. With a mean of 4.40, the user's acceptance testing result implies that the web application is secured and only gives access to those users who have signed up for an account in which every account type has a different level of accessibility.

Based on the overall result shown in table 1, the web application was accepted by the different evaluators in the user acceptance testing in terms of ISO 25010 software quality characteristics with an overall mean of 4.41, implying that the developed web application is a great help for the institution's employees and administration.

Summary	Mean	Remarks
Functional Sustainability	4.50	Agree
Usability	4.32	Agree
Security	4.40	Agree
Overall Mean	**4.41**	**Agree**

Table 1. Summary of the Acceptability Response of users on the web application.

SUMMARY AND CONCLUSION

Summary

In the contemporary interconnected landscape, web-based systems are pivotal for organizational growth and enhancement. However, these systems confront significant security challenges due to the escalating cybercrimes. This study aimed to address this issue by developing the "e201 File" web application for the Data Center College of the Philippines (DCCP) to securely manage vital personnel records and confidential data. The principal objective was to ensure the security and integrity of sensitive information through robust cybersecurity measures.

Employing the Research and Development (R&D) model, the study followed an iterative approach to develop the e201 File web application. The process encompassed identifying existing challenges in manual employee information management, conceptualizing web application features, executing system development, meticulous testing, and eventual deployment. The adoption of Agile Software Development methodologies facilitated incremental progress, flexibility, and efficiency throughout the development phases.

Cybersecurity remained a central concern throughout the study. Leveraging the OWASP ZAP open-source tool, the study conducted a comprehensive security evaluation of the developed application. The assessment unveiled vulnerabilities including the absence of Anti-CSRF tokens, lacking Content Security Policy (CSP) headers, and

other risks categorized by severity levels. Remedial actions were undertaken through the incorporation of security measures such as CSP headers, HttpOnly flags for cookies, application of SameSite attributes, and integration of Anti-CSRF tokens. These measures substantially bolstered the application's resilience against potential cyber threats.

User Acceptance Testing, conducted as per the ISO 25010 standard, gauged the e201 File web application's user experience. The assessment spanned functionality, usability, and security dimensions. Feedback from 72 faculty members and 10 staff members at DCCP attested to the application's efficacy, user-friendliness, and robust security provisions.

CONCLUSION

In today's changing world the development of secure and efficient web applications is incredibly important. This study successfully addressed this need by introducing the e201 File web application, for the Data Center College of the Philippines (DCCP). The application effectively manages personnel records and confidential data thanks to its focus on robustness, adaptability and user centered design.

One crucial aspect emphasized in this study was cybersecurity. The OWASP ZAP assessment was utilized to ensure that the e201 File system is well protected against threats like session hijacking and cross site scripting. Measures such as CSP headers, HttpOnly flags, SameSite attributes and Anti CSRF tokens were implemented to strengthen security.

To assess its effectiveness User Acceptance Testing aligned with ISO 25010 standards was conducted. The positive feedback received from faculty and staff of the institution confirmed that the efforts put into designing this application were successful. In conclusion this study highlights how designed and securely developed web applications can enhance efficiency and safeguard sensitive information, for educational institutions and organizations.

REFERENCES

[1] Caratiquit, Kevin. (2021). Web-based School Information and Publication System: A Developmental Study. 1. 45-55.

[2] Gade, Nikhita Reddy & Reddy, Ugander. (2014). A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies.

[3] Carmen Elena CÎRNU, Carmen Ionela ROTUNĂ, Adrian Victor VEVERA, Radu BONCEA (2018), "Measures to Mitigate Cybersecurity Risks and Vulnerabilities in Service-Oriented Architecture". from https://www.academia.edu/download/93457422/Art.-11-Issue-3-2018-SIC.pdf

[4] Ludwig Slusky. (2020), "Cybersecurity of Online Proctoring Systems"., Journal of International Technology and Information Management, Volume 29| Issue 1, https://scholarworks.lib.csusb.edu/jitim/vol29/iss1/3/

[5] Sawehli, Ali Fathi. (2019). Improving Software Security Testing of Software Development Life Cycle (SDLC) For Web-Based Applications By Providing A Quality System (Web-Vs) for Vulnerability Assessment - Master Dissertation - M.S.c In Software Engineering - Asia Pacific University. 10.13140/RG.2.2.17114.29128.

[6] OWASP, ZAP https://owasp.org/www-project-web-security-testing-guide/v41/6-Appendix/A-Testing_Tools_Resource

[7] Sunardi, Sunardi & Riadi, Imam & Raharja, Pradana. (2019). Vulnerability Analysis of E-voting Application using Open Web Application Security Project (OWASP) Framework. International Journal of Advanced Computer Science and Applications. 10. 135-143.

[8] Jaiswal, Arunima & Raj, Gaurav & Singh, Dheerendra. (2014). Security Testing of Web Applications: Issues and Challenges. International Journal of Computer Applications. 88. 10.5120/15334-3667.

[9] Făgărășan, Cristian & Popa, O & Pisla, Adrian & Cristea, Ciprian. (2021). Agile, waterfall and iterative approach in information technology projects. IOP Conference Series: Materials Science and Engineering. 1169. 012025. 10.1088/1757-899X/1169/1/012025.