A Model for Security Evaluation of Digital Libraries: A Case Study on a Cybersecurity Curriculum Library

Nnatubemugo (Ugo) Ngwum
Department of Computer and Information Sciences
Towson University
Towson, MD, USA
nngwum1@students.towson.edu

Sagar Raina
Division of Mathmatics and Information Technology
Mount Saint Mary College
Newburgh, NY, USA
sagar.raina@msmc.edu

Sabina Aguon
Department of Computer and Information Sciences
Towson University
Towson, MD, USA
saguon1@students.towson.edu

Blair Taylor
Department of Computer and Information Sciences
Towson University
Towson, MD, USA
btaylor@towson.edu

Siddharth Kaza
Department of Computer and Information Sciences
Towson University
Towson, MD, USA
skaza@towson.edu

***Abstract*—The use of digital libraries (DLs) is increasing. To attract users and sustain digital libraries, security of these systems is critical. However, few studies in the digital library literature have focus on evaluating the security of a DL system. Through review of existing literature, standards and other security guidelines, we propose a novel model for security evaluation of digital libraries. We test the effectiveness of the model using the CLARK cybersecurity curriculum digital library (www.clark.center) at Towson University. We identify five core security criteria that are broken down into several requirements, in the model, that a DL should fulfill to achieve security. Results from the evaluation, which include static code analysis and expert review of CLARK's security mechanisms, indicate the proposed model is significantly effective in evaluating the security requirements of digital libraries.**

Keywords—digital libraries, security evaluation, security metrics, cybersecurity digital library

I. Introduction

A digital library (DL) is a complex information system (IS) that stores and manages digital content. With the convenience, cost-effectiveness and ability to access digital content from anywhere, DLs facilitate knowledge creation and large-scale dissemination. Several DL projects across domains have been undertaken, seeking to provide various services to its users/clients [1].

Considering the increasing use of digital libraries, there is need for evaluation of these systems to probe for challenges and limitations that could deter their use and large-scale adoption by their target audiences. Research studies have addressed DL evaluation from different perspectives, ranging from user-centered [2,3,4], system-centered [5] to impact analysis of DL usage [6] in various fields of study. However, these evaluation efforts have subtly addressed or totally ignored the security aspect of DLs.

To attract and retain an active user base to achieve their goal, DL systems must be evaluated to address security issues, as security is a critical concern of any information system. Therefore, in this paper, we address the following research questions:

RQ1: Are there effective models or tools for security evaluation of digital libraries?

RQ2: What components should be included in the security evaluation of a DL?

To address these questions, we conduct a literature research and identify gaps in existing security evaluation studies and models for specifically evaluating security requirements of DLs. Consequently, we develop a model for security evaluation of digital libraries, which is further broken down into specific security requirements in the evaluation checklist used. We then pilot this model to evaluate the CLARK digital library to test its potential effectiveness in assessing other DLs.

The sections that follow present a review of existing evaluation efforts (II), research framework and proposed evaluation model (III), results and findings (IV), and conclusion and future direction (V).

II. Background

In this section, we examine the scholarly work that exists on the security evaluation of digital libraries. However, as digital libraries are a type of complex information system, we must explore, generally, existing security requirements models, approaches and evaluation efforts for information systems. We then proceed to discuss researches that focus on security requirements of various information system's components, as we narrow down to digital libraries, which is the focus of our study. We explore existing research efforts,

This project is partially funded by the National Security Agency under Grant H9830-17-1-0405.

starting from studies focused on user-centered evaluations, usability assessment, impact analysis, system-centered studies and security evaluation of DLs.

A. Information Systems Security Evaluation Studies

Although standards such as Information Security management system (ISMS) has been appropriate for managing security of information systems, Sanghyun and Kyungho [6] develop a mutually exclusive paradigm based on ISO 27000 series to address the critical requirement of safety, in addition to the core security attributes of confidentiality, availability and integrity in industrial control systems (ICS). Sandip and Jigish [7] proposed a cybersecurity risk-assessment model for evaluating information systems. While the mathematical model investigates the quantitative (and financial) impact of cyber-attack on information systems, security requirements of the system itself was not covered. Daniel et al. [8] developed a Security Requirements Engineering Process (SREP) based on security standards such as Common Criteria and System Software Engineering Capability Maturity Model (SSE-CMM), which offers a repeatable and systematic approach to security engineering in software development process. It describes the steps for integrating these standards into software development lifecycle. Just like some other approaches, it is a good guide that points out necessary security engineering tasks, although it did not delve into the details of the requirements those individual tasks should accomplish. Similar to other reviews [9], [10] that investigate software engineering process, Daniel et al. [11] provides a thorough summary with evidences on security engineering studies as a basic for advancing security engineering research. While these studies aim at improving security engineering process, there is need for identifying the specific security requirements of the different aspects of an information system.

As digital libraries are a type of information system whose core services rely on frequent access of its repository, a contextualized security model that identifies specific security requirements for DLs becomes necessary, for protecting user data, services and database from compromise that could propagate as users disseminate its collection. On database (collection) security requirements, we leverage the exhaustive survey conducted by Iqra et al. [12] on the issues, threats and security requirements of a system's database to stir considerations while modelling database security requirements in line with standards. In addition, the technical report by Adam [13] explores various aspect of database security threats with a focus on improving traditional intrusion strategy. By proposing a novel intrusion detection system architecture which integrates with all database transactions rather than the tradition approach that constitute an intrusion detection system as an external layer of security, their work demonstrates the greater efficacy of security implementation during system development than later after system is in operation. Considering the increasing shift from relational to NoSQL databases, Samaraweera and Morris [14] explored the unique security and privacy challenges posed by the Big-Data applications and identify database security requirements through their survey of various database models. With their work inspiring specific database security considerations, we also explored studies focused specifically on technical security requirements of information systems.

Josang and Knapskog [15] present a trust model for evaluating IT systems, which adopts an approach based on subjective logic. The article models an evaluation scheme to show the various metrics (i.e., sources of evidence or factors) that could corroborate and influence user's trust of a system for security; however, there was limited discussions on what each of those factors entail.

Elaborating on industry 4.0 concept and the increasing exposure of industrial processes, machines and systems interactions to cyber threats (with examples), Pereira et al. [16] creates awareness for stirring proactive actions for ensuring security in industrial production activities and systems. In an attempt to understand and address these security issues for operational efficiency, Hofbauer [17] adapts SixSigma approach to investigate the security requirements of industrial systems and controls required to meet the requirements, based on established security standards. His methodology, based on SixSigma, defines five steps (Define, Measure, Analyze, Improve and Control) for identifying security requirements and mapping them to controls from established security standards. Several other studies [18], [19], [20], [21] and reviews [22], [23] focused on security requirements of the Industrial Internet of Things (IIoT) have also laid the foundation and created solid context for formulating strategies for securing distributed systems. Going forward, we explore research works on digital libraries (a representative, complex information system), starting from studies on general evaluation of digital libraries to those focused on security evaluation of digital libraries.

B. Digital Library Evaluation Studies

Blandford et al. [24] proposed a framework for planning and conducting DL evaluation with a user-centric approach that focuses on user-system interactions. Similarly, Tsakonas et al. [25] explored the interaction of the various components of a DL (user, collection and system) and the dynamic relationship they share as a cohesive whole. Bertot et al. [26] adopted a multi-method approach for evaluating DLs. These user-centric studies attempt to capture functionality, usability and accessibility testing, with little or no emphasis on system security. Saracevic et al. [27] introduced the foundational framework for evaluating digital libraries, enumerating four elements – context, construct, criteria, measures and methodology – which any evaluation study should consider. Several studies have used this framework to structure their evaluation exercise; however, the framework acts like a guide for guiding DL evaluation studies, but not as an actual tool for assessing or evaluating the system itself. Nicholson [28] claims a holistic approach by viewing the evaluation from four different quadrants: the internal view, which compared system's component against standard; the external view, which focused on the system results; the external view of use, focused on how the results are valued; and the internal

view of use that examined the interactions between the technical components.

With few studies focusing on both user-centered and system-centered considerations [27], [28], [29], others remain within usability confines [30]. Besides usability assessments, understanding the actual impact of DL usage on users' learning outcomes has also been explored [31], while Gocalves et al. [32] proposes a quality model for assessment how good a digital library is based on some key quality indicators they identified.

C. Security-Related Evaluation Studies on Digital Libraries

Few studies have captured security considerations of DLs as part of regular technical evaluation [33], [34], while some attempt to explore the security requirements of digital libraries [35],[36] as a whole. Barely any of these studies offered a dedicated security-centered approach or model for evaluating and ensuring all-round security of digital libraries. Hao [37], however, attempts a holistic approach to digital library security by analyzing the critical factors (hardware and software related) that affect security of digital libraries, and then proposes a strategic approach for information security policy of digital libraries.

A digital library is a software system with several components including front-end application, collection or database and back-end servers and functionality mechanisms. Wang et al. [34] defines a set of security metrics for evaluating software systems. Their work only focused on the quantitative rating of software vulnerabilities, while Kuzma et al. [38] specifically investigated vulnerabilities in eighty digital library software of four European countries to understand impact of security issues on patrons' data. Several other security-evaluation attempts on digital library have been conducted [39], [40], [41], with almost all restricting their work to vulnerability assessment of the DL software. Although Ismail and Zainab [42] captures relevant considerations in their security model for evaluating digital library, their model appears too broad to include organizational measures. In our work, we focus in not only contextualizing security in the digital library, but also narrowing the considerations in our easy-to use assessment tool and model to the critical security requirements for effectively evaluating and securing any digital libraries.

III. Research Methodology

The DL evaluation framework by Saracevic [27], which we adopt as our methodology for this study, outlines the key elements or areas any digital library evaluation study should address. These elements include: (1) the context, which explains the goal or focus of the evaluation (e.g., usability, impact analysis, technology, security, etc.); (2) construct, which defines the exact components or parts of the system to be evaluated; (3) criteria, which defines parameters of performance; and (4) methodology, which describes the measures, instruments and approach for conducting the evaluation. We discuss these elements as it relates to our study in the following subsections.

A. Context

The goal of this study is to address security of a digital library. This involves ensuring confidentiality, integrity and availability of information assets (i.e., data, hardware, software, etc.). Applying mechanisms to attain these security attributes prevents unauthorized access to digital resources (confidentiality), protects data from unauthorized modification (integrity), and ensures that resources are always accessible to only authorized users (availability) [43]. Based on this context, we hypothesize that security of a digital library is achieved when each of the DL components, as defined by Tsakonas (user, collection, system), exhibits the confidentiality, integrity and availability attributes.

B. Construct

A typical digital library consists of three core components including user, system and collection [3]. Each of these components must be secured to secure the entire DL system [44].

User component focuses on user interaction with digital library using application interface. This interaction could be used as a possible attack surface if the user behavior is not restricted. Examples include the interface allowing invalid inputs, interface not warning users of unsafe actions, GUI storing sensitive information in clear text and so on.

System component includes all hardware and software that enable the overall functionality of the digital library (e.g., servers, platforms, programming frameworks and libraries, security architectural approach etc.). As users request information from a DL, the entities in this component interact, process the request and return the results to the user. The interaction between these entities is another possible attack surface that could be exploited. Therefore, adequate security measures are required within the entities of the system component to prevent security breaches.

The collection component includes the digital library database, one of the critical resources of the DL system. DL database stores the user data and the content. A primary goal of the attackers is to target the system database. Therefore, security of the DL database becomes critical. Appropriate measures (as described in the criteria section) should be put in place to prevent any database breaches.

C. Criteria

To evaluate the security of a digital library, we identify five key security criteria's including: 1) Encryption, 2) Authentication and Authorization, 3) Platform weakness and vulnerabilities, 4) System and Security Audit, and, 5) Usability and Human-factor. These are further broken down into specific security requirements (Table I in Appendix).

1) Encryption Mechanism

Cryptography involves conversion of data to forms unreadable to third parties (who can be potential adversaries) and re-conversion of same data to the original readable form at the receiving end or system using a secret key. Encryption ensures confidentiality of the data [45]. Under this criterion,

we identify DL components (user, system or collection) where implementing cryptographic mechanisms are necessary. In addition, we assess cryptographic tools and strategies that are deployed in DL systems for adequacy and alignment with security standards.

2) Authentication and Authorization Mechanism

Authentication and Authorization of users in an information system is a critical security measure. In order to ensure security of a digital library, correct controls for granting and controlling/managing access between user-system and system-system interactions must be implemented [46]. This criterion assesses the authentication and access control mechanisms of the DL system.

3) Platform Weaknesses and Vulnerabilities

The majority of successful cyber attacks are attributed to insecure software development [47]. In addition, recent system/software development trends reveal that programmers are increasingly leaning towards the use of frameworks and libraries rather than developing code from scratch [48]. Often, these reusable components exhibit inherent vulnerabilities that are potentially transferred to the program or system in which they are used. Therefore, it is important to identify and assess vulnerabilities in DL components that may impose a significant threat to the system.

4) System/Security Audit

Logging system events, both legitimate activities and attack exposures, is a critical security measure to identify significant system intrusions [49]. In this criterion, we identify standard requirements for system events logging, log records management responsibilities, and action plans for identified security events.

5) Usability and Human-Factor Support

Usability refers to how easy-to-use a system's interface or website is, while human factors is a broader term which seeks to address and limit inappropriate and risky user behaviors by means of adequate security mechanisms. A popular perception in technology industry is that "the more the security, the less usable a system". While this perception may hold for several scenarios, we posit that for a system's security features to be effective, they have to "lend themselves to be easily configured and used" [50]. Neglecting to design the system's architecture, features, data flow, and especially user interfaces, to support security and reduce risky user behaviors would increase a system's exposure to security incidents [51]. Furthermore, a non-usable system would naturally deter usage and affect its massive adoptions due to navigation challenges limiting its availability. Moreover, availability is a key security attribute that must be ensured.

Figure 1 represents our model, with three merging sectors that represent the three DL components that come together to form the system. The model (Figure I) depicts three DL components (user, system, collection). Each component is divided into three clusters that represent the security attributes of confidentiality (pink), integrity (orange) and availability (green). The idea of having these clusters run through all components as a ring is to demonstrate the need to meet each of these security attributes in each of the DL components for overall security.

Furthermore, each cluster is comprised of several sectors that represent the security items for ensuring the security attribute that the cluster stands for. We further break down the security items in the model into specific security requirements in the checklist (Table I in Appendix). The checklist is an evaluation tool, which delineates all the specific security requirements an evaluator should check for in a DL for security. The collective fulfilment of the security items established in the model represents the security of digital library. We describe these security items briefly in Table II.

979-8-6425-4896-7/20/$26.00 ©2020 CISSE

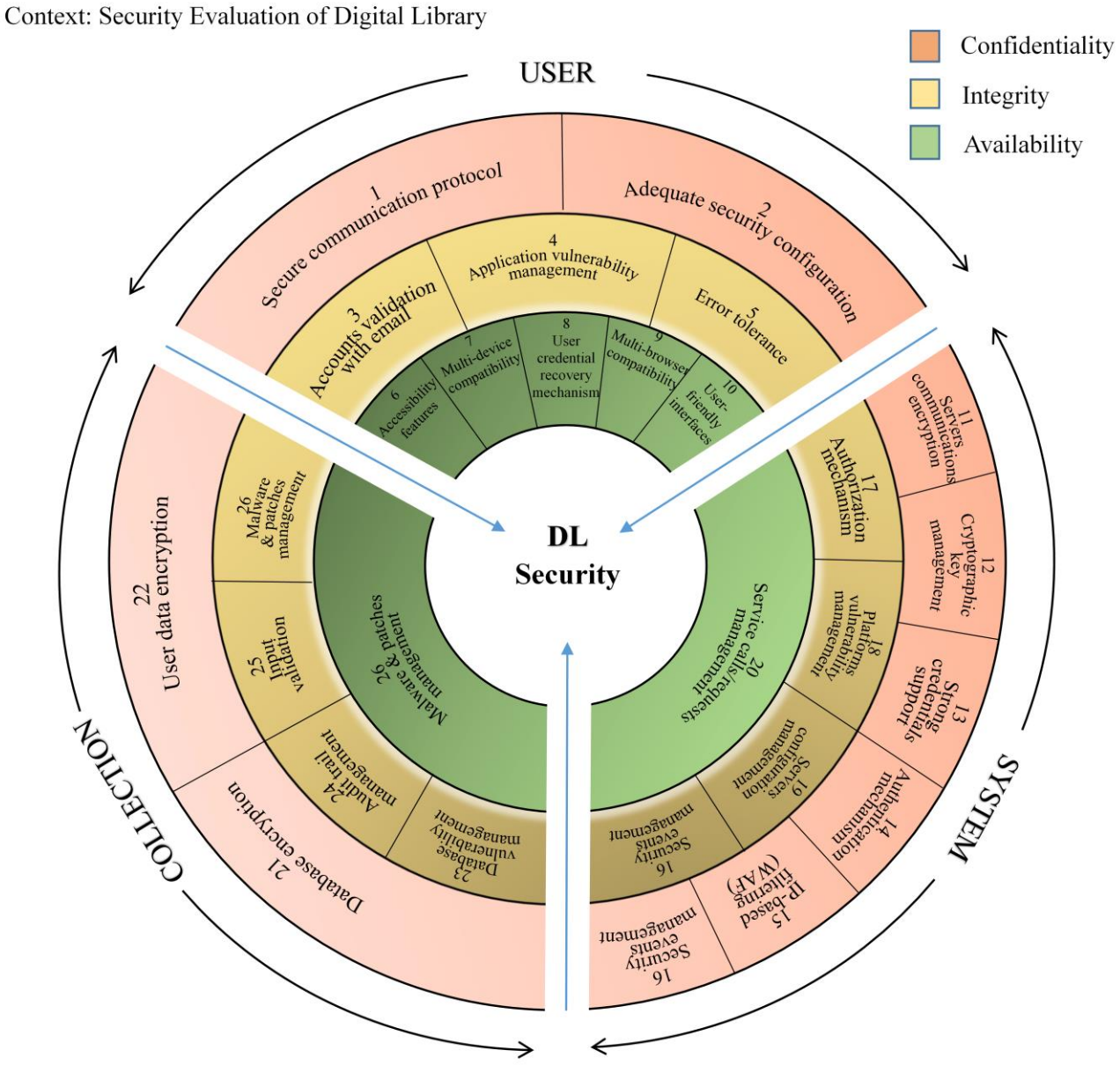

Fig. 1. A model for security evaluation of digital libraries.

979-8-6425-4896-7/20/$26.00 ©2020 CISSE

TABLE II. DESCRIPTION OF DL SECURITY MODEL ITEMS

Item No.	Security consideration/item	Description
1	Secure communication protocol	Ensures TCP/IP communications are encrypted
2	Adequate security configuration	Ensures secure, customized configuration for servers, etc.
3	Accounts validation with email	Deals with verifying all user accounts during sign-up
4	Application vulnerability management	Ensures front-end application is vulnerability-free
5	Error tolerance	How does the application recover from unexpected errors?
6	Accessibility features	Does the DL application features support disabled users?
7	Multi-device compatibility	Can one access the system using several devices (e.g., desktop, laptop, mobile phones, etc.)?
8	User credential recovery mechanism	Can I recover forgotten or lost credentials?
9	Multi-browser compatibility	Can I access the system using different browsers?
10	User-friendly interfaces	How intuitive and easy-to-use are the application interfaces?
11	Server communication encryptions	Are there encryptions for server communications?
12	Cryptographic key management	Are there procedures for managing and recycling keys?
13	Strong credential support	Does the DL mechanism enforce use of strong password?
14	Authentication mechanism	Are there identity verification mechanisms?
15	IP-based filtering (WAF)	Are there web application firewall (s), or other form of web filtering?
16	Security events management	Any procedure/mechanism for security events monitoring and mitigation?
17	Authorization mechanism	Are there access control mechanisms?
18	Platform vulnerability management	How is vulnerability management across the DL platforms?
19	Servers configuration management	Are the servers custom configured and modified as needed?
20	Service calls/requests management	Are there thresholds and mechanisms for limiting requests (i.e., anti-DOS attack mechanism)?
21	Database encryption	Is the database encrypted and collection protected?
22	User data encryption	Are user data stored safely in encrypted form?
23	Database vulnerability management	Ensures vulnerability-free database
24	Audit trail management	Ensures proper event recording, auditing and actions
25	Input validation	Ensures mechanisms that check inputs for safety and correctness before execution
26	Malware & patches management	Are there procedure for updating components?

D. Methodology

We adopt tool-based and qualitative approaches to evaluate the CLARK digital library. CLARK is a living repository of cybersecurity curriculum contributed by cybersecurity scholars and professionals from several US institutions. While we use a tool-based approach to assess security criterion 3 (vulnerabilities) of the checklist, we use a qualitative approach to assess security criteria 1 (Encryption Mechanism), 2 (Identification, Authentication, Authorization Mechanisms), 4 (System/Security Audit) and 5 (Usability & Human-factor Support).

1) Tool-Based

To investigate vulnerabilities across the digital library components, we use vulnerability scanning/penetration testing tools. Because it is important to choose the right tool(s), we studied several open-source and commercially available tools. Each tool has its unique features and strengths [52]. We identified WebSecurify and Zed Attack Proxy (ZAP) [53] for vulnerability scanning and Burp Suite for penetration testing. We chose WebSecurify and ZAP for vulnerabilities scanning because Websecurify is free, fast, user-friendly and efficient, while ZAP specifically checks for the OWASP top 10 vulnerabilities [53]. ZAP is also multi-operating system compatible, and has better report generation and customization features. To conduct the scan on the CLARK DL, we modified the proxy settings on ZAP for the standard mode intended for just vulnerability scanning. Burp Suite was selected for penetration testing because of its various scanning and attack features that are very customizable. Its free version offers several uses and comes pre-installed with recent Kali distributions.

2) Qualitative Approach

Here, assessment is guided by the security checklist we developed (Table I in Appendix). The checklist delineates the specific DL security requirements based on best practices derived from security standards [45],[46],[54], common criteria [49], scholarly articles on security metrics [55], etc. We map the security requirements in the checklist to the security items of the model (described in Table II) by their item numbers. In the checklist, each section represents a criterion with its set of specific security requirements. The "supports item" column shows how each requirement in the checklist connect to our model's item. "Max" weight is the highest possible score for meeting an associated requirement, while the "earned" weight is the achieved score during evaluation.

We adapt the mini-Delphi technique to assign weights and scores to the security criteria and requirements respectively. The scores and weights were assigned by the team of experts, comprised of programmers, usability experts, system/software architects, and information system specialists. Ranking was based on their perceived unique impact of each criterion on the security of a DL (or any IS) through rounds of scoring, justification and reconciliation. The varying weightings of the criteria sum up to a total of 100 achievable points. Eventually, we modified the checklist to capture all relevant security requirements, testable through vulnerability scanning, expert review of functionalities, and usability testing.

To use the checklist to evaluate CLARK, we investigated and checked off all boxes for the security requirements met by CLARK. Next, we summed up all earned points within each criterion to get the subtotals for each. Finally, we were able to arrive at the total score achieved by the system by summing up all the subtotals. The following section presents the results of this study.

IV. Results

In this section, we present results for both the tool-based and qualitative assessment.

A. Tool-based

Vulnerability scanning on CLARK using WebSecurify shows that the cybersecurity DL passed 80% of the OWASP top ten security risk assessment giving CLARK an A grade. In addition, the vulnerability scanning performed using ZAP tool resulted in two false positive alerts: a low-risk, third-party domain script detection and a path traversal error marked as high risk. While the first error is due to the discrepancy in hostnames of CLARK's website and that of the external script (i.e., google analytics, which is safe), ZAP threw the second flag, having found "etc" in the word "Fetches" that it literally parsed. This similar flag is common whenever ZAP detects strings like "bin" or "boot", and so on. In this case, both alerts pose no security risks to the system.

Modifying proxy settings (amongst other configuring) on Burp Suite, and with the use of Burps fuzzer tool (capable of identifying injection, buffer overflow and cross-site scripting (XSS)), we further conducted penetration testing on CLARK. With Burps' intruder tool, and using some common XSS attacks retrieved online and uploaded into the payload options, results for the inserted payloads is as shown in Figure 2.

With the first result being the baseline request, it is important to point out that the closer the length of a request is to the length of the baseline, the more likely the payload was not harmful to the application. Here, we see that majority of the payloads gave a 200 response, which means that the status is acceptable.

B. Qualitative Study

The results of the qualitative study on CLARK are presented based on the criteria and specific security requirements defined in our checklist (Table I).

Encryption Mechanism: In this criterion, which examines the overall encryption mechanisms, evaluation results indicate that CLARK has secure transport layer encryption using TLS/SSL (Transport Layer Security/Secure Sockets Layer). This fulfills client-server and server-server communication security requirement. CLARK database runs on MongoDb, which runs on Amazon Web Services (AWS) engine, and uses 256-bit Advanced Encryption Standard in Galois/Counter Mode (AES256-GCM) for the Linux

operating system, and AES256-CBC for the Windows OS. In addition, user data is hashed while cryptographic key are encrypted and stored with strong cipher as defined by AWS. With both the database and transport layer communications across services secure, CLARK satisfies this criterion, scoring the full 20 points for this category.

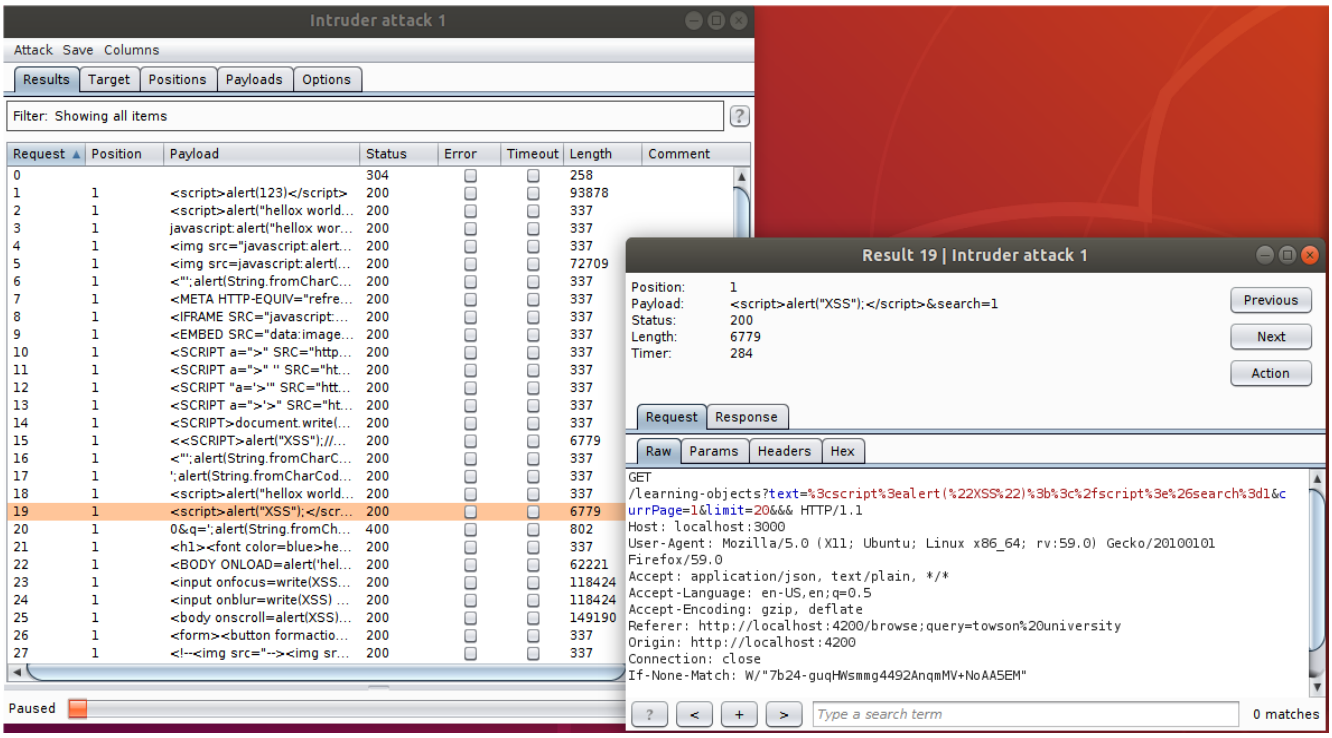

Fig. 2. Results from Burp Suite intrusion on CLARK

Authentication and Authorization Mechanism: Although CLARK shows limited or no controls for some of the security requirements under this criterion, such as support for strong password, limited failed login, single sign-on support, inactive session termination, it meets some key requirements which includes authorization mechanism and web application firewalls (WAFs), for the services and the database. Overall, CLARK performed relatively low under this criterion as seen in Table III.

TABLE III. CONSOLIDATED EVALUATION RESULTS

Security Criteria	Score	
	Achievable	*Earned*
Encryption Mechanism	20	20
Authentication and Authorization Mechanism	20	8
Platform Weaknesses and Vulnerability	20	18
System/Security Audit	15	12
Usability & Human-Factor Support	25	20.5
Total	100	78.5

Platform Weakness and Vulnerability: The quantitative assessment results of CLARK (using Websecurify scanner) shows that CLARK passed 80% of the OWASP's top ten security risks. CLARK's database is considered secure, enjoying all the standard protection/shield offered by Amazon Web Services (AWS) that it runs on. The system also uses Docker to encapsulate all tools in identical containers for the development, test and production environment, thereby ensuring configuration consistency for those environments that the system traverse during its development cycle. All these are geared towards minimizing vulnerabilities, affording CLARK a score of 18 out of 20 for this criterion.

System/Security Audit: Our investigation shows that CLARK captures all events using Amazon CloudWatch, a

monitoring service for AWS cloud resources and applications, while it uses Sentry to track application errors, log and report to admins for resolution. These two features satisfy this requirement with 12 out of 15 points earned.

Usability & Human-Factor Support: Although accessibility features were yet to be adequately implemented, CLARK has an overall good outlook when it comes to usability of its web application. We also found that AWS Identity and Access Management (IAM) super user can and does grant minimal privilege as he creates other users – a strategy for checking inappropriate use and reducing human-factor threats. Greenkeeper handles application libraries (and other dependencies, security patches, etc.) updates, while all backend infrastructures/services that run on AWS are being maintained and updated by AWS. These would ensure normal system-user interactions for reducing security incidents. With a score of 20.5 out of 25, CLARK provides a quality user experience and adequate support for user-system interactions.

V. Discussion & Conclusions

In this study, we identified the key security requirements of a digital library through extensive review of literature on evaluations studies, security standards and security guidelines. Considering these requirements, we developed a model as our contribution and a tool (checklist) for guiding system developers, evaluators, and system administrators on the requirements for ensuring security of digital libraries. We also evaluated the CLARK cybersecurity digital library [56], to test the effectiveness of the model, adopting a tool-based and qualitative assessment approach.

For the tool-based study, we used free, ease-to-use, speedy and automatic testing tools that offer valuable penetration testing phases under a single framework; however, their limitations include the report of false positives that require efforts to confirm that the alerts are not harmful. In both the vulnerability scanning (with WebSecurify and ZAP) and penetration testing (with Burp suite), CLARK did well with an eighty percent score. As for the qualitative evaluation of CLARK, summing up the scores for all the criteria resulted in an overall score of 78% out of 100%, implying that CLARK is considerably secure. The successful use of our model and checklist to evaluate CLARK demonstrates the effectiveness of our model for evaluating any other digital library. In our next study, we plan to evaluate multiple digital libraries.

References

[1] Zorich, Diane M. *A Survey of Digital Cultural Heritage Initiatives and Their Sustainability Concerns. Managing Economic Challenges*. Council on Library and Information Resources, 1755 Massachusetts Ave., NW, Suite 500, Washington, DC 20036, 2003.

[2] Carlo Bertot, John, et al. "Functionality, usability, and accessibility: Iterative user-centered evaluation strategies for digital libraries." *Performance Measurement and Metrics* 7.1 (2006): 17-28.

[3] Tsakonas, Giannis, Sarantos Kapidakis, and Christos Papatheodorou. "Evaluation of user interaction in digital libraries." *Notes of the DELOS WP7 workshop on the evaluation of Digital Libraries, Padua, Italy*. 2004.

[4] Blandford, Ann, et al. "The PRET A Rapporter framework: Evaluating digital libraries from the perspective of information work." *Information Processing & Management* 44.1 (2008): 4-21.

[5] Nicholson, Scott. "A conceptual framework for the holistic measurement and cumulative evaluation of library services." *Proceedings of the American Society for Information Science and Technology* 41.1 (2004): 496-506.

[6] Park, Sanghyun, and Kyungho Lee. "Advanced approach to information security management system model for industrial control system." *The Scientific World Journal* 2014 (2014).

[7] Patel, Sandip C., James H. Graham, and Patricia AS Ralston. "Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements." *International Journal of Information Management* 28.6 (2008): 483-491.

[8] Mellado, Daniel, Eduardo Fernández-Medina, and Mario Piattini. "A common criterion based security requirements engineering process for the development of secure information systems." *Computer standards & interfaces* 29.2 (2007): 244-253.

[9] Martins, Luiz Eduardo G., and Tony Gorschek. "Requirements engineering for safety-critical systems: A systematic literature review." *Information and software technology* 75 (2016): 71-89.

[10] Shuaibu, Bala Musa, et al. "Systematic review of web application security development model." *Artificial Intelligence Review* 43.2 (2015): 259-276.

[11] Mellado, Daniel, et al. "A systematic review of security requirements engineering." *Computer Standards & Interfaces* 32.4 (2010): 153-165.

[12] Basharat, Iqra, Farooque Azam, and Abdul Wahab Muzaffar. "Database security and encryption: A survey study." *International Journal of Computer Applications* 47.12 (2012).

[13] Call, Adam. "Review of Database Intrusion Detection Methodologies using Attribute Dependence." *Technical Report, Department of Computer and Information Sciences Indiana University South Bend* (2013).

[14] Samaraweera, Gamage Dumindu, and Morris J. Chang. "Security and Privacy Implications on Database Systems in Big Data Era: A Survey." *IEEE Transactions on Knowledge and Data Engineering* (2019).

[15] Jøsang, Audun, and Svein J. Knapskog. "A metric for trusted systems." *In Proceedings of the 21st National Security Conference*. NSA. 1998.

[16] Pereira, T., L. Barreto, and A. Amaral. "Network and information security challenges within Industry 4.0 paradigm." *Procedia Manufacturing* 13 (2017): 1253-1260.

[17] Hofbauer, David, et al. "On the Cost of Security Compliance in Information Systems." *arXiv preprint arXiv*:1905.06122 (2019).

[18] Bicaku, Ani, et al. "Monitoring Industry 4.0 applications for security and safety standard compliance." *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*. IEEE, 2018.

[19] Ma, Zhendong, et al. "Security viewpoint in a reference architecture model for cyber-physical production systems." *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2017.

[20] Bakhshi, Zeinab, Ali Balador, and Jawad Mustafa. "Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models." *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*. IEEE, 2018.

[21] Langfinger, Michael, et al. "Addressing security challenges in industrial augmented reality systems." *2017 IEEE 15th International Conference on Industrial Informatics (INDIN)*. IEEE, 2017.

[22] Tange, Koen, et al. "Towards a systematic survey of industrial IoT security requirements: research method and quantitative analysis." *Proceedings of the Workshop on Fog Computing and the IoT*. ACM, 2019.

[23] Lezzi, Marianna, Mariangela Lazoi, and Angelo Corallo. "Cybersecurity for Industry 4.0 in the current literature: A reference framework." *Computers in Industry* 103 (2018): 97-110.

[24] Blandford, Ann, et al. "The PRET A Rapporter framework: Evaluating digital libraries from the perspective of information work." *Information Processing & Management* 44.1 (2008): 4-21.

[25] Tsakonas, Giannis, Sarantos Kapidakis, and Christos Papatheodorou. "Evaluation of user interaction in digital libraries." *Notes of the DELOS WP7 workshop on the evaluation of Digital Libraries, Padua, Italy*. 2004.

[26] Carlo Bertot, John, et al. "Functionality, usability, and accessibility: Iterative user-centered evaluation strategies for digital libraries." *Performance Measurement and Metrics* 7.1 (2006): 17-28.

[27] Saracevic, Tefko. "Digital library evaluation: Toward an evolution of concepts." (2000).

[28] Nicholson, Scott. "A conceptual framework for the holistic measurement and cumulative evaluation of library services." *Proceedings of the American Society for Information Science and Technology* 41.1 (2004): 496-506.

[29] Huang, Kuo Hung, ed. *Digital Libraries: Methods and Applications*. BoD–Books on Demand, 2011.

[30] Jeng, Judy. "Usability assessment of academic digital libraries: effectiveness, efficiency, satisfaction, and learnability." *Libri* 55.2-3 (2005): 96-121.

[31] Borgman, Christine L., et al. "Evaluating digital libraries for teaching and learning in undergraduate education: a case study of the Alexandria Digital Earth Prototype (ADEPT)." (2000).

[32] Gonçalves, Marcos André, et al. "'What is a good digital library?'–A quality model for digital libraries." *Information processing & management* 43.5 (2007): 1416-1437.

[33] Hoe-Lian Goh, Dion, et al. "A checklist for evaluating open source digital library software." *Online Information Review* 30.4 (2006): 360-379.

[34] Wang, Ju An, et al. "Security metrics for software systems." *Proceedings of the 47th Annual Southeast Regional Conference*. ACM, 2009.

[35] Singh, Mr Anuj Kumar. "DIGITAL LIBRARY AND ITS SECURITY ISSUES: AN OVERVIEW." *Journal Current Science* 20.1 (2019).

[36] ANDAY, Audrey, et al. "Information Security Issues in a Digital Library Environment: A Literature Review." *Information World/Bilgi Dunyasi* 13.1 (2012).

[37] Hao, Tingting. "The information security analysis of digital library." *2015 8th International Conference on Intelligent Computation Technology and Automation (ICICTA)*. IEEE, 2015.

[38] Kuzma, Joanne. "European digital libraries: Web security vulnerabilities." *Library Hi Tech* 28.3 (2010): 402-413.

[39] Huang, Shuiqing, et al. "Factor identification and computation in the assessment of information security risks for digital libraries." *Journal of Librarianship and Information Science* 51.1 (2019): 78-94.

[40] Han, Zhengbiao, et al. "Risk assessment of digital library information security: a case study." *The Electronic Library* 34.3 (2016): 471-487.

[41] Elstrøm, Gry, and Jette Junge. "Self-assessment of the Digital Repository at the State and University Library, Denmark-a Case Study." *iPRES*. 2014.

[42] Ismail, Roesnita, and Awang Ngah Zainab. "Assessing the status of library information systems security." *Journal of Librarianship and Information Science* 45.3 (2013): 232-247.

[43] Maconachy, W. Victor, et al. "A model for information assurance: An integrated approach." *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*. Vol. 310. United States Military Academy, West Point. IEEE, 2001.

[44] Conklin, William Arthur, Dan Shoemaker, and Anne Kohnke. "Cyber resilience: Rethinking cybersecurity strategy to build a cyber-resilient architecture." *ICMLG2017 5th International Conference on Management Leadership and Governance*. 2017.

[45] *International Organization for Standardization*. ISO 27001. www.iso.org/isoiec-27001-information-security.html. Accessed 27 March 2019.

[46] *International Organization for Standardization*. ISO 27002. https://www.iso.org/standard/54533.html. Accessed 27 March 2019.

[47] Kaza, Siddharth, Blair Taylor, and Kyle Sherbert. "Hello, World!—Code Responsibly." *IEEE Security & Privacy* 16.1 (2018): 98-100.

[48] *TechBeacon*, 9 code and framework trends to watch in 2018, https://techbeacon.com/app-dev-testing/9-code-framework-trends-watch-2018. Accessed 27 March 2019.

[49] *The Common Criteria*. Publications, www.commoncriteriaportal.org/cc/. Accessed 27 March 2019.

[50] Alexander, Eldridge "Part 1: Usability is Security." *Duo Labs*, duo.com/blog/part-1-usability-is-security. Accessed 27 march 2018.

[51] Atzeni, Andrea, Shamal Faily, and Ruggero Galloni. "Usable Security." *Advanced Methodologies and Technologies in System Security, Information Privacy, and Forensics*. IGI Global, 2019. 348-359.

[52] Fonseca, Jose, Marco Vieira, and Henrique Madeira. "Testing and comparing web vulnerability scanning tools for SQL injection and XSS attacks." *13th Pacific Rim international symposium on dependable computing (PRDC 2007)*. IEEE, 2007.

[53] *The OWASP Foundation*. www.owasp.org/index.php/Main_Page, Accessed 27 March 2019.

[54] *National Institute of Standards and Technology*. Computer and Security Resource Center, csrc.nist.gov/projects/cryptographic-module-validation-program/standards. Accessed 27 March 2019.

[55] Swanson, Marianne M., et al. *Security metrics guide for information technology systems*. No. Special Publication (NIST SP)-800-55. 2003.

[56] Cybersecurity Labs and Digital Knowledgebase (CLARK) digital library. Effective cybersecurity curriculum at your fingertips, clark.center/home. Accessed 27 March 2019

APPENDIX

TABLE I. DIGITAL LIBRARY SECURITY CHECKLIST

Security Criteria				Weight	
1	**Encryption Mechanism**	**Supports item**		**Max.**	**Earned**
	• Secure client-server communication/connection (i.e., SSL/TSL encryption)	1	☐	5	
	○ Client-server and server-server communication uses standard cryptographic algorithm (i.e., AES-256				
	• Database security (database encryption or file-system level encryption) exists	21	☐	5	
	• User data is stored in encrypted form	22	☐	5	
	• Well-defined and consistent approach for cryptographic key management and recycling	12	☐	5	
	Sub-Total			**20**	
2	**Identification, Authentication, Authorization Mechanisms**	**Supports item**		**Max.**	**Earned**
	• Support strong user credentials (i.e., Alphanumeric password, symbol, at least 8-eight characters)	13	☐	3	
	• User groups with varying privilege levels exist (i.e., admin, user, reviewers, upper and lower case, etc.)	17	☐	3	
	• Limited failed login attempts (i.e., three attempts)	14	☐	2	
	• User account is disabled after defined period of inactivity	14	☐	2	
	• System supports single logon session at a time	14	☐	2	
	• Content owner can only authorize changes to their content (i.e., read-only, write, can modify, etc.)	17	☐	2	
	• Login sessions terminate after 30mins of user inactivity	14	☐	2	
	• IP-based filtering (Web application firewall)	16	☐	4	
	Sub-Total			**20**	
3	**Platform Weaknesses and Vulnerability**	**Supports item**		**Max.**	**Earned**
	• Low/mitigated vulnerability risks to database	23	☐	5	
	• Low/mitigated vulnerability risks to front-end application	4	☐	5	
	• Low/mitigated vulnerability risks to back-end services platforms	18	☐	5	
	• Identical configuration for servers (i.e., development, test and production)	19	☐	5	
	Sub-Total			**20**	
4	**System/Security Audit**	**Supports item**		**Max.**	**Earned**
	• Identity-based logging of servers events Date, time, IP address, username, nature of operation, etc.	24	☐	3	
	• Real-time security events analysis mechanism (e.g., IDS/IPS)	16	☐	3	
	• Log files are constantly monitored and acted upon	24	☐	3	
	• Well-defined roles or/and action plans for security events in audit records	24	☐	3	
	• Secure storage of audit trail	24	☐	3	

Security Criteria				Weight	
	Sub-Total			**15**	
5	**Usability & Human-Factor Support**	**Supports item**		**Max.**	**Earned**
	• System allows only single account on a particular email address	14	□	1	
	• User credential recovery mechanism	8	□	1	
	• Account validation during creation via email	3	□	1	
	• Easy and intuitive navigation	10	□	1	
	• Multi-browser compatibility	9	□	1	
	• Multi-device compatibility (i.e., desktop, laptop, tablets, mobile phones, etc.)	7	□	1	
	• Supports accessibility features	6	□	0.5	
	• Consistent page design	10	□	0.5	
	• Interactive features	10	□	0.5	
	• Web pages contents not cluttered and overwhelming	10	□	0.5	
	• User-friendly and efficient search feature	10	□	1	
	• Error tolerance	5	□	1	
	• Custom security configuration	2	□	3	
	o Routine security configuration strengthening				
	o Unused default settings disabled				
	o Minimal privilege allowed for roles/operations				
	• Thresholds set for service calls	20	□	3	
	• Patches update enabled	26	□	2	
	• Anti-malware installed on servers and updated regularly	26	□	2	
	• Software components upgrade and maintenance plan	26	□	2	
	• Validation of input data	25	□	3	
	Sub-Total		□	**25**	
	Total Score			**100**	