Security Evaluation Model for Virtual Learning Environments

M. Callejas-Cuervo, A. C. Alarcón-Aldana
Software Research Group, Engineering Faculty
Universidad Pedagógica y Tecnológica de Colombia
Tunja, Colombia
mauro.callejas@uptc.edu.co; acalarcon@gmil.com

A. Barinas López
Engineering Faculty
Fundación Universitaria Juan de Castellanos
Tunja, Colombia
alexbari99@gmail.com

***Abstract*—In order to estimate the security of the Web apps, there has been proposed the design and built of a model for evaluating security on Virtual Learning Environments (VLE), starting from the identification of security criteria proposed in handbooks, rules and standards, and there were established objectives and activities that gave patterns for carrying out such process, making emphasis on three criteria: integrity, confidentiality and availability of the information. Once criteria were established, some metrics were analyzed to quantify such relationship, easing the validation of the proposed model which was applied to Moodle and Dokeos VLEs, two platforms of open source and free distribution that allow carrying out a reliable value judgement in qualitative and quantitative, close to the security status of the VLEs.**

Keywords—Information security; web security; vulnerabilities analysis; Virtual Learning Environments

I. INTRODUCTION

Nowadays information is the most valuable asset for the development of activities in companies. With the rise of the Internet, most of the companies have opted for migrate its data and apps to the Web, exposed to unauthorized accesses, change and exposure of the information by hackers.

Because of the needs regarding to information security, some communities, groups or organizations have emerged with the purpose of minimizing security risks; in this way the OWASP (Acronym for Open Web Application Security Project) project was born, which is an open source project to determine and fight what makes software unsafe. Besides, norms as ISO 9126 and related are described in order to establish the security criteria for designing and elaboration of security evaluation model for VLEs.

This article presents the summary of developed activities based on some raised objectives. In the first place, there is a research about security rules and standards, as well as guides or organizations treating the security issue; emphasis is made on security tools and vulnerabilities analysis focused to VLE. Then there are established the security criteria for evaluation on VLEs, the elaboration of the model and the making of tests by applying the model with the purpose of verify the security level of the VLEs.

II. THEORETICAL FUNDAMENT

The security is a primary aspect that every single system should incorporate in order to protect assets from any threat [1]; for this it becomes necessary to have knowledge about information security and protection mechanisms to safeguard assets [2].

A. Web Security

Currently on the Internet there are countless services and applications running on the network [3], from e-commerce, transactions of huge amounts of money, web searches, e-mail, as well as social networks with important and private information of its users [4]. Meanwhile there is a considerable increase in the number of network connections [5], as well as a migration of applications and users to Internet services; the demand of secure web services grows up, the threats and impacts against the attacks of the data are incalculable, because of the vulnerabilities of greatest impact as [6-7]: SQL injection, loss of authentication and management of sessions, sequence of cross-site scripting (XSS), CSRF vulnerability (Cross-site request forgery), wrong security settings, remote file inclusion, among others; showing the weaknesses exposed of the web apps.

B. Related Jobs

In order to carry out this research, there have been referenced a series of works and articles related to the topic, each of which introduces the studies developed around the problem that allow supporting the topic being developed in the process of research.

The work "A model for implement security to a web application using aspect-oriented programming", analyses that one of the causes of the vulnerability of the Web apps to attacks is because the client application is out of the server control. It considers that the security issue in an application should include, transversely, the whole system, and this is possible through aspect-oriented programming (AOP), a paradigm that allows a modularized implementation of cross-cutting issues, defining for this a model for implement the security of a web application by using POA [8].

978-1-5090-6149-5 / 16 / $ 31.00 © 2016 IEEE

Olso, in the research "Guide for the application of UNE-ISO/IEC 27001 standard about security on information systems for SMEs", presents the adoption process of the ISO/IEC 27001 standard in small and medium-sized enterprises, with the purpose of enhance the Information Security Management System (ISMS), by designing a model; running it; verifying the attainment of the expected results and according to that evaluation, taking decisions to correct the flaws submitted and thus try to improve the information security. Chapter 4 presents the way to evaluate the asset inventory through confidentiality, integrity and availability of the information, by establishing values for each asset according with its relevance [9], and similarly the research of Chamorro "Model for evaluation in informatics security to software products, based on ISO/IEC 15408 Common Criteria", proposes to design and implement a model for evaluation in informatics security with this standard, to a set of software products that Colombian laws require them for informatics security, which concludes that the standard in Colombia isn't very common and in Latin America there are no labs or research center that certify this standard; however, it becomes necessary adopting it, because of the approach of development and production of technology in the country [10].

Luisa Romero in her article "Informatics security on work with Moodle platform", describes the security aspects of this platform, taking into account that both professors and tutors need to work with security and have confidence that its tools are protected against unwanted informatics attacks and that its files are adequately protected, for which it describes the basic settings in the weaker levels: server security, authentication security, security with passwords and roles [11].

The article "Good Practice Guide of informatics security on processing of health data for health personnel in primary care", suggests the need for strengthen health personal data security to guarantee its privacy. There is also presented a good practices guide of informatics security in data handling, that shows a classification of the threats that faces the security of an organization, as well as the protection of the health information from three basic aspects: confidentiality, integrity and availability of this one [12].

Another approach is oriented to presented that total safety on Internet is impossible, asserts that the way to security on Internet "is a cat and mouse fight, an endless race...We will never be able to say that a system is totally safe". It warns that insecurity in the cloud is increasing because everything is shifting to the virtual world. It shows how in the last times, the Internet giants: Apple, Facebook, Microsoft and other technologies, are focusing their efforts in beating hackers which want to infringe security systems [13-14]. Thus the importance of internet security, since the origin of this network, there is a worry from the enterprises and people using this service, since as well as it can be used for increasing the productivity of a company, attracting customers and finding new opportunities; it is also used for committing informatics crimes, impersonations, criminal acts, manipulating information, obtaining sensitive and confidential data that can end with the prestige of a company or the dignity of people [15-16]; Olso supports in the work "Security on internet" that describes the importance of the security online due to the information that is managed there in digital way, taking into account that from there can be fought complex issues as informatics crimes, identity impersonation, data modification or robbery of information by hackers [17].

According to the articles and presented works, some of these are focused on software models for obtaining security requests; other make reference to tendencies to take advantage of the security weakness on web to commit any act that attacks confidentiality, integrity and the availability of the information. There is also an asset inventory evaluation system. On the other hand, there are shown methodologies for vulnerabilities measurement in organizational data networks, and vulnerabilities analysis in real systems

III. METHODOLOGY

The methodology used for the development of this research follows the process shown on fig. 1, which is based on the proposed objectives and traces a series of phases which include a previous research of guides, rules and standards that allowed identifying the security criteria in web applications; then security tools were selected and were used to analyze VLEs vulnerabilities specified on Table I. The metrics were established for the criteria's evaluation by assigning them values according to the degree of importance; the steps for criteria's evaluation and VLEs evaluation methods were determined. Finally a security evaluation was made to Moodle and Dokeos VLE (table II), according to the model, and the security level was verified; so the same the model functionality was validated.

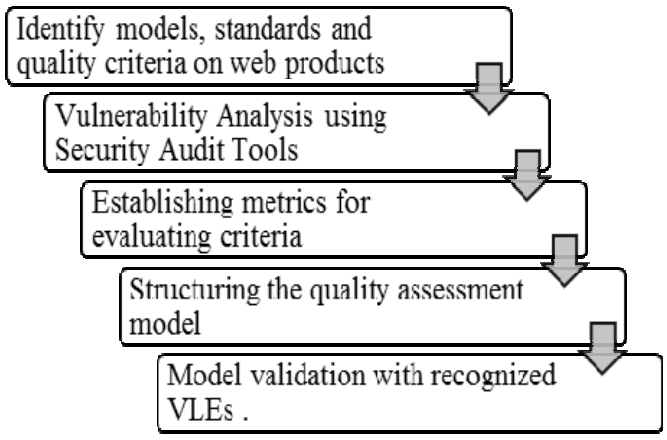

Fig. 1. Methodological Design

IV. RESULTS

A. *Analysis of vulnerabilities to Moodle and Dokeos VLES*

The tools described on Table I are used for the security analysis in web applications, which allow helping both administrators and security professionals to assure information systems or take decisions with the purpose of improving and protect informatics infrastructures, but also can be used by hackers for illegal purposes.

These tools were analyzed and were evaluated through a research process according to its functionality, ranking of better tools and the purpose for analyze. Later, three tools were selected to carry out the process of realization of safety tests to VLEs, in which were selected: SQLMap, W3AF and OWASP ZAP, which are the best suited to make the research because of its specific features, criteria and metrics for evaluation.

TABLE I. VULNERABILITY ANALYSIS TOOLS

Tool	Description	License/ Version
OWASP ZAP (Zed Attack Proxy Project)	Open source Java from OWASP Project to make, in the first instance, penetration tests on web apps.	Apache 2.0 Ver. 2.3.1
SQLMap	Open source penetration testing tool that automates the process of detecting and exploiting SQL injection vulnerabilities.	GNU Ver. 0.9-3758
W3AF	Project which main objective is develop a Framework to help protecting web apps through the search and exploitation of vulnerabilities.	GPL 2.0 Ver. 1.6

The virtual platforms chosen for this research were Moodle and Dokeos, two open source platforms which are freely obtained with the ease of being downloaded and installed with the purpose of making the respective security tests, being Moodle one of the best known tools and used worldwide. Likewise, Dokeos is platform though less known than Moodle, is also welcomed by many organizations as content management tool, unlike platform owners as it is impossible to acquire them because obtaining a license would involve cost.

TABLE II. TECHNICAL FEATURES OF MOODLE AND DOKEOS VLES

Feature	Dokeos	Moodle
Version	2.0	2.4.5
Size	104 MB	129 MB
Number of files	13.955	14.074
Architecture	Model view controller (MVC)	Model view controller (MVC)
Language	PHP	PHP
Data base	MySQL	MySQL, PostgrSQL, MSMSQL, Oracle, SQLite
Required permissions	Reading/ writing	Reading/ writing

The analysis process begins with the collection of information relevance to Dokeos and Moodle apps, followed by security tests and analysis of results.

The kind of security analysis carried out was the penetration tests [18-19], commonly known as intrusion test, is the kind of analysis that leads to the performance of tasks associated to the vulnerabilities exploitation and post-exploitation. The purpose of this kind of security analysis is to detect weak points, looking for exploit the security vulnerabilities in order to break the integrity, confidentiality and availability of information.

The applied method within this test was the black-box-testing. This kind of test is based on the ignorance about internal processes that interact with the information; that way, is only evaluated the inning against its departure and thus its correct working is verified.

TABLE III. VULNERABILITIES IDENTIFIED ON MOODLE AND DOKEOS PLATFORMS

Item	Moodle	Dokeos
Code execution	0	0
SQL Injection	0	0
XSS	0	0
Bypass Something	0	0
Gain information	3	5
CSRF	0	0
File inclusion	0	0
Flow control	0	0
Total	3	5

It is clear that in order to make this comparison, security analysis tools were used and different criteria were taken into account with the purpose of reducing the subjectivity of the evaluation, since the data in the table belong to vulnerabilities verified with manual inspections, therefore don't appear false positives generated in the tests.

The framework W3af gave false positives as CSRF vulnerabilities and click jacking, which were manually examined; W3af found vulnerabilities of sensitive information leakage as absolute routes and default settings. OWASP ZAP, didn't report any false positive and also achieved to find vulnerabilities of sensitive information leakage, as directories list, and cookies management bugs, since nor Moodle nor Dokeos stated the HttpOnly directive, which indicates to the browser that the cookie shouldn't be directly accessed. This action may allow that a hacker can steal the session of an user and in the worst case of a system manager. SQLMap didn't report any vulnerability of a SQL injection kind, or XSS, as can be seen on Table III.

B. Security evaluation model to VLES

To build the security evaluation model, the most relevant criteria described on the guides, rules and security standards were taken into account along with the specification of the evaluation metrics that accounts for the relevant aspects to evaluate the security of a certain software product, in this case,

Moodle and Dokeos VLEs. The criteria taken into account are: Confidentiality (C), Integrity (I) and Availability of the information (D), and the metrics established in this research have been product of OWASP security guides [20], as shown on fig. 2:

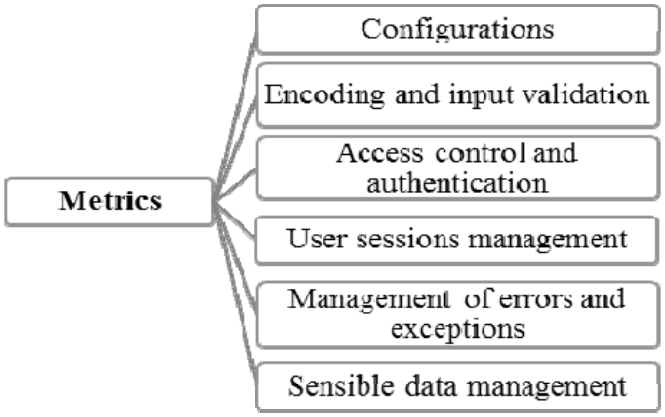

Fig. 2. Security evaluation metrics

Once established the six metrics for the evaluation of the three general security criteria (integrity, confidentiality and availability), it was necessary to set values and indicators to quantify such criteria and, in this way, have as final result the level of security of Moodle and Dokeos VLEs. With the purpose of quantifying the information security evaluation, it was decided that each one of the six metrics will have a different weighing, as shown on Table IV. These weightings assigned to the metrics were specified according to the impact of each one in the business and this was calculated based on the exploitability and prevalence values, and the detection of a possible vulnerability.

TABLE IV. TABLE OF WEIGHTS TO EACH METRIC

Metric	Short	weighing	Maximum individual value	Value according to OWASP
Metric for configuration Management	MGC	14%	14	0 - 14
Metric for coding management and input validation	MGCVE	25%	25	0 - 25
Metric for access control management and authentication	MGCA	16%	16	0 - 16
Metric for session management and users	MGSU	16%	16	0 – 16
Metrics for error handling and exceptions	MGEE	6%	6	0 - 6
Metrics for management sensitive data	MGDS	23%	23	0 - 23

The security general evaluation is made according to a values scale (table V) with the purpose of indicating different security levels in which an application (VLE) can be; so a quantitative value in the range (0 a 20), means that the total value of the app evaluation is in a "low" qualitative level, which allows the Agent Evaluator (AE) making the respective decisions to carry out an improvement plan or making value judgments about possible failures or criticality of the system, and the possible consequences for an organization.

TABLE V. QUALITATIVE AND QUANTITATIVE VALUES

Qualitative Value	Quantitative Value
Low	0 – 20
Medium-low	21 – 40
Medium	41 – 60
Medium-high	61 – 80
High	81 – 100

Each metric has a series of questions to evaluate which each one corresponds to the criteria of Integrity (I), Confidentiality (C) and Availability (A), as shown in the table VI:

TABLE VI. METRIC OF CONFIGURATION MANAGEMENT EVALUATION

No.	Question	I.	C.	A.
1	¿ Do you have any software without updating? This includes the SO, Server Web/application, DBMS, applications and all the code libraries.	8	4	8
2	¿Are enabled or installed any unnecessary features (e.g ports, services, pages, accounts, privileges)?	2	2	2
3	¿Are default accounts and its passwords still enabled and without changing?	2	6	2
4	¿Do you lack of security settings on your development framework (e.g Struts, Spring, ASP.NET)?	2	2	2
	Total:	14	14	14

Once the other metrics are developed, these ones are applied to evaluate the VLEs security, in which each question is answered in affirmative or negative way (YES/NO), giving as general result the security level of the VLEs, as presented on fig. 3 and fig. 4.

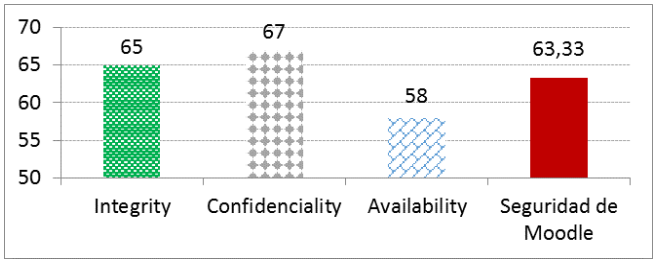

Fig. 3. Final results of Moodle security

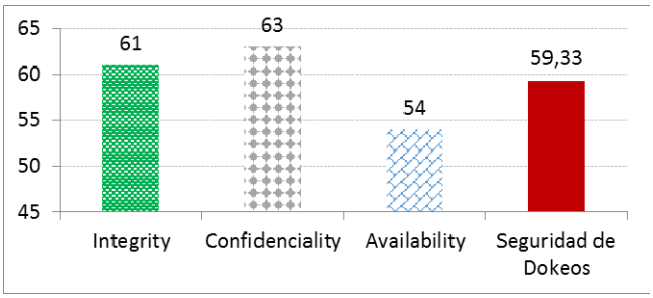

Fig. 4. Final results of Dokeos security

C. *General Result of Moodle and Dokeos Security by Applying the Evaluation Model*

When comparing the results of the security evaluation to the Moodle and Dokeos VLEs with the proposed model, this has allowed establishing a quantitative and qualitative value of the security level of the VLEs; thus Moodle obtained a score of 63.33 for a medium-high scale while Dokeos obtained a score of 59,33 and its scale was medium level, as presented on table VII.

TABLE VII. COMPARISON OF SECURITY EVALUATION RESULTS OF THE VLES

Evaluation metrics	**Values in Moodle**	**Values in Dokeos**
Tests for configuration management	-2.66	-2.66
Tests for encoding and input validation	25	25
Test of access controls and authentication	2	2
Session management and users test	16	12
Test of error handling and exceptions	6	6
Sensitive data management test	17	17
Total Value	63.33	59.33

According to the above, the VLEs, both Moodle and Dokeos, had a negative value in the metric of "configuration management", because this tests have been made with old versions of the applications, therefore this fact affects the general security values. The metric of the management of access and authentication controls, shows that both applications were weak in avoiding brute force attacks to its authentication mechanisms, as well as none of them could verify the authenticity of the petitions in cross-sites.

By making the security comparison between Moodle and Dokeos, it is observed that both platforms take measures in the management and the coding of entries, which is a critical mainstay to keep the security level of the platforms and, even though the Dokeos app had a lower value than Moodle in the metric of access and authentication controls management; it keeps a security level reliable for its implementation on output environments.

The model is useful for measuring the state of security of a Web application modularly, allowing to know which are the weak links of the applications (settings, coding and validation of entries, etc), so the low cost can be analyzed when running measures to mitigate possible security risks. Namely, taking into account the Moodle and Dokeos security, both applications proved to be safe and require measures to mitigate the risks as regard its settings and access and authentication controls, wherewith, its cost is equitable on both of them; whence, the decision of which of them should be implemented in an organization, is conditional by that one that had obtained the highest security level.

V. CONCLUSIONS

The security evaluation process allows establishing the reliability degree in VLEs, evaluated through an in-depth study of previously investigated criteria and whose results can turn into the supporting source for making decisions in educational establishments interested in acquiring a VLEs as appeal of support for teachers and instructors.

The lack of efficient checks by platforms to prove the security of these ones, is a feature that should be implemented on future versions of these platforms. Additionally, the support and maintenance teams of Moodle and Dokeos should strengthen its collaborative tools in order to know more quickly its upgrades, seeking to reduce potential intrusions or repercussions of these applications.

Although there are various guides, rules and standards about informatics security and about the information at a general level in an organization, there is little what exists regarding to security rules on Web applications. Thanks to OWASP project, which has dedicated its research and concerns about the relevant vulnerabilities described on the top 10 ranking of this one, allow architects, developers and software and networks managers to be on the lookout for improving and applying good practices on assets security.

REFERENCES

[1] J. Areitio, Seguridad de la información: redes, informática y sistemas de información. Editorial Paraninfo: Madrid (España), 2008.

[2] P. Aguilera, Seguridad informática. Editex: Madrid (España), June 2010.

[3] H. Holm, “Performance of automated network vulnerability scanning at remediating security issues, ” Computers & Security, vol. 31(2), pp. 164–175, March 2012.

[4] A. Romero, “Aspectos básicos de la seguridad en aplicaciones Web”. Available:http://www.seguridad.unam.mx/documento/?id=17, April 2016.

[5] Feng, N., H. Wang and M. LI, “A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis,” Information Sciences, vol 256, pp. 57–73, January 2014.

[6] E. Ofuonye and J. Miller, “Securing web-clients with instrumented code and dynamic runtime monitoring,” Journal of Systems and Software, vol. 86 (6), pp. 1689–1711, Jun 2013.

[7] OWASP. “Category: OWASP Top Ten Project. Bel Air (MD, USA): OWASP Foundation”, . Available: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project, 2015.

[8] L. Hernández, “Un modelo para la implementación de la seguridad de una aplicación Web con el uso de la programación orientada a aspectos,” Editor: Cuba: D - Instituto Superior Politécnico José Antonio Echeverría. CUJAE. 2012.

[9] Gómez, L. and A. Andrés, “Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes, ” Editorial AENOR - Asociación Española de Normalización y Certificación. 2012.

[10] J. Chamorro, “Modelo para la evaluación en seguridad informática a productos software, basado en el estándar ISO/IEC 15408”. Master’s degree work, 2011.

[11] L. Romero, “La seguridad informática en el trabajo con la plataforma Moodle,” Revista de Humanidades, vol 17, pp. 169 – 190, December 2010.

[12] A. Sánchez, J. Fernández, A. Toval, I. Hernández, A. Sánchez, and J. Carrillo, “Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria”. Atención Primaria, vol 46 (4), pp. 214-222, April 2014.

[13] D. Hong, “Challenges on privacy and reliability in cloud computing security,” International conference on Information Science, Electronics and Electrical Engineering, vol. 2, pp. 1181-1187, April 2014.

[14] El financiero, La seguridad total en internet es imposible de lograr, advierte experto. Noticias Financieras. Available:http://search.proquest.com/docview/1439058277?accountid=38880. May 2016.

[15] J. Gómez, La importancia de la seguridad en internet. Portafolio, Available:http://search.proquest.com/docview/859060826?accountid=38880, May 2016.

[16] Y. Chen, Three essays on internet security-understanding users' security perceptions and behaviors. Doctoral Dissertation , University of Wisconsin, 2012.

[17] E. Rincón, La seguridad en internet. Portafolio. Available: http://search.proquest.com/docview/1643368939?accountid=38880, May 2016.

[18] E. Sallis, C. Caracciolo and M. Rodríguez, Ethical hacking. Un enfoque metodológico para profesionales. Buenos Aires. Alfaomega, 135 p, 2010.

[19] M. Agé, S. Baudru and N. Crocfer, Seguridad informática: ethical hacking: conocer el ataque para una mejor defesa. Ediciones ENI, 2013.

[20] A. López, OWASP Testing Guide v4.0. Guía de seguridad en aplicaciones Web. Available: https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/Owasp_4, May 2016.