مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (٩) العدد (٥) ٢٠٢٥
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (9) No. (5) 2025

تحليل المخاطر الأمنية في النّظام Moodle كنظام تعليميّ إلكترونيّ مفتوح المصدر

د. باسل حبيب حسن *

ايمان عزيز نعامه **

(تاريخ الإيداع ٢٠٢٤/١٠/٢٨ . قُبِل للنشر في ٢٠٢٥/٥/٥)

□ ملخّص□

أدّى الاعتماد واسع النّطاق على منصات التعليم الإلكتروني في السنوات الأخيرة الماضية ولا سيّما خلال فترة جائحة كورونا، إلى قلق متزايد بشأن المخاطر الأمنية المرتبطة بالتعليم عبر الانترنت. أصبحت منصات التعليم الإلكتروني مفتوحة المصدر مثل Moodle، ذات شعبية متزايدة لأنها توفر العديد من الفوائد، بما في ذلك توفير التكاليف وخيارات التخصيص والتعديل في الكود البرمجي بما يتوافق مع حاجة المنظمة. ومع ذلك، قد يتشكل في هذه المنصات مخاطر أمنية فريدة بسبب طبيعتها مفتوحة المصدر ومجتمع المطورين الكبير. تهدف هذه الدراسة إلى إجراء تحليل مخاطر أمنية لنظام Moodle، باستخدام المعيار NISTIR 8286 كمبدأ توجيهي. يحدد هذا البحث المخاطر الأمنيّة ونقاط الضعف الأكثر أهمية المرتبطة بنظام Moodle، بالإضافة لإجراء محاكاة لهجمة أمنية وذلك بتطبيقها على نسخة مثبتة محلياً Moodle v.4.1. يمكن للمعلمين والإداريين والمطورين استخدام نتائج هذه الدراسة لتحسين الأمان في منصات التعليم الإلكتروني القائمة على نظام Moodle، وبالتالي تقليل مخاطر اختراق البيانات وضمان سرية المعلومات الحساسة وسلامتها وتوافرها.

الكلمات المفتاحية: التعليم الإلكتروني، البرمجيات مفتوحة المصدر، أمن المعلومات، محاكاة هجوم، تحليل المخاطر.

*أستاذ – قسم البرمجيات ونظم المعلومات – كلية الهندسة المعلوماتية – جامعة تشرين – اللاذقية – سورية. Email: basel.hasan@tishreen.edu.sy

**طالبة دراسات عليا (ماجستير) - قسم البرمجيات ونظم المعلومات – كلية الهندسة المعلوماتية – جامعة تشرين – اللاذقية – سورية.
Email: iman.naamah@tishreen.edu.sy

Security Risk Analysis of Moodle as an Open Source E-Learning System

Dr. Basel Habib Hasan *
Iman Aziz Naamah**

(Received 28/10/2024 . Accepted 5/5/2025)

□ **ABSTRACT** □

The widespread adoption of e-learning platforms in recent years, particularly during the pandemic, has led to growing concern about the security risks associated with online education. Open source e-learning platforms like Moodle are becoming increasingly popular because they provide many benefits, including cost savings and options for customization and modification in code to match the organization's need. However, these platforms may pose unique security risks due to their open-source nature and large developer community. This study aims to conduct a security risk analysis for the Moodle system, using NISTIR 8286 as a guideline. This research identifies the most significant security risks and vulnerabilities associated with the Moodle system, as well as simulating a security attack by applying it to a locally installed version of Moodle v.4.1. Teachers, administrators, and developers can use the results of this study to improve security in Moodle-based e-learning platforms, thereby reducing the risk of data breaches and ensuring the confidentiality, integrity, and availability of sensitive information.

Keywords: e-learning, open source software, information security, attack simulation, risk analysis.

* Professor, Department of Software and Information Systems, Faculty of Informatics Engineering, Tishreen University, Lattakia, Syria. Email: basel.hasan@tishreen.edu.sy

** Postgraduate Student (Master), Department of Software and Information Systems, Faculty of Informatics Engineering, Tishreen University, Lattakia, Syria.
Email: iman.naamah@tishreen.edu.sy

١ – مقدّمة:

خضع جميع مقدمي التّعليم على مستوى العالم لتحول كبير نحو نمط الدراسة الإلكتروني خلال جائحة كوفيد-١٩ [1]، ويُعرَّف التّعليم الإلكترونيّ بأنّه العملية التّعليميّة التّي يتم من خلالها إيصال المعلومة إلى الطّالب باستخدام الحاسب الآليّ وبرمجياته وأدوات الانترنت التّفاعليّة دون التقيّد بالمكان أو الزّمان. يستخدِم التّعليم الإلكترونيّ لهذا الغرض ما يسمّى بأنظمة إدارة التّعلّم (Learning Management Systems) LMS. هناك نوعان لأنظمة إدارة التّعلّم، الأولى مغلقة المصدر (Closed Source LMS) وتكون الشّيفرة البرمجيّة الخاصة بها غير متاحة للمستخدم أما الثّانية مفتوحة المصدر (Open Source LMS) وغالباً ما تكون مجانية والتّي تعني أن المبرمجين الذّين قاموا بتطوير النّظام يوفرون الشّيفرة البرمجيّة التّي كُتب بها. سنركز في بحثنا هذا على النّوع الثّاني وهو أنظمة التّعليم الالكترونيّ مفتوحة المصدر وبشكل خاص الجانب الأمني لها وسنأخذ كحالة دراسة النّظام Moodle الذي يندرج تحت رخصة GPL (General Public License) [2] وهي إحدى رخص البرمجيات مفتوحة المصدر والتي توفر حرية الاستخدام والتعديل والتوزيع للشيفرة البرمجية بشرط أن يتم توزيع التعديلات تحت نفس الرخصة (GPL) [3]. في هذا البحث تم اختيار منصة Moodle نظراً لكثرة استخدامها من قبل الكثير من الجامعات حيث بلغ عدد الدول التي تستخدمه حوالي ٢٣٧ دولة مع عدد مستخدمين يصل إلى 432,537,994 مستخدم [1] ، ونظراً لهذا العدد الكبير من المستخدمين لابدّ من دراسة القضايا والمخاطر الأمنية التي يمكن أن يتعرّض لها النظام لكي تكون الجامعات على دراية ووعي بالمخاطر التي قد تتعرض لها هذه المنصات وذلك من أجل اتخاذ التدابير المناسبة في مرحلة مبكرة قبل أن يتدهور الأمان في النظام، هذا ما دفعنا للتفكير في بناء كتالوج مخاطر يأخذ بعين الاعتبار الربط بين ثلاثة جوانب وهي التعليم الإلكتروني والبرمجيات مفتوحة المصدر والأمان.

٢ –مشكلة البحث:

تكمن مشكلة البحث في أنّ أنظمة التّعليم الإلكترونيّ بشكل عام معرّضة لثغرات أمنيّة قد تسبب مخاطر كبيرة لمستخدمي هذه الأنظمة كالطّلاب والمعلمين ومدراء الموقع ولا سيما عندما يكون عدد المستخدمين كبير جدّاً وتزداد المشكلة صعوبة عندما تكون هذه الأنظمة مفتوحة المصدر وذلك لأنّ الشّيفرة البرمجيّة تكون متاحة وبإمكان المهاجمين الوصول لها ومحاولة فهمها واستغلال نقاط الضّعف فيها لتنفيذ هجمات قد تسبّب مثلاً تسريب بيانات هامّة مثل أسئلة امتحان مقرّر ما، أو مثلاً أن يحاول طالب رفع محاضرة بدلاً من مدرس المقرر أو أن يرى الطّالب درجات غيره من الطّلاب وكثير من السّيناريوهات التّي تسبّب انهيار أمان النّظام وفقدان الموثوقيّة من قبل المستخدمين، إضافة إلى أنّ استخدام برمجية مفتوحة المصدر قد يرافقه مخاطر عديدة متعلقة بتخصيص النظام والذي قد يؤدي إلى عدم توافقية بين وحدات النظام حيث أن تعديل الكود وتخصيصه في مكان ما قد يسبب خلل في مكان آخر [4].

٣–دراسات سابقة ذات صلة:

بيّنت الدراسة في الورقة البحثيّة [5] أنّ تصميم وتنفيذ نظام تعليم إلكترونيّ من الصّفر، ليس خياراً جيّداً اقتصاديّاً وتقنيّاً، وكان الحلّ المقترح هو استخدام البرمجيات مفتوحة المصدر وتطويرها، أو على الأقل، الاستفادة الجزئيّة من الهندسة المعماريّة الخاصّة بها للخروج بنظام برمجيات جديد للتّعليم الإلكترونيّ؛ وذلك بتخصيص النظام بما يخدم ويلبّي حاجة الجامعة.

[1] https://stats.moodle.org/

نلاحظ أنّه تمّ التركيز على البرمجيات مفتوحة المصدر والتعليم الإلكتروني ولكن لم يتم التطرّق للمخاطر الأمنية التي قد ترافق عملية التخصيص وتأثيرها على أصول (assets) التعليم الإلكتروني التي ستقوم بها الجامعة.

بينما حدد الباحثون في الورقة البحثيّة [6] نقاط الضّعف المعروفة لـ Moodle v. 1.9 ومحاولات استغلال هذه الثّغرات الأمنيّة بالإضافة إلى تحديد نقاط الضّعف الجديدة في النسخة التالية لها وهي Moodle v. 2.1، وبينت الورقة أنّ العديد من هذه الثّغرات المعروفة، تستمر في الظهور مما يشير إلى إمكانية استغلال ذلك من قبل الطّلاب.

نلاحظ هنا أنه تم التركيز على الجانب الأمني في منصة مفتوحة المصدر دون التطرّق إلى تفصيل حول أصول التعليم الإلكتروني المتأثرة بتلك الثغرات، في بحثنا سندرس نسخة أحدث وهي Moodle 4.1 ونرى هل عدد الثغرات تناقص مقارنة بالنسخ السابقة وماهي الأصول الأكثر تعرّض للثغرات في بيئة التعليم الإلكتروني.

ركز الباحثون في الدراسة [1] على المخاطر المرتبطة بالتعليم الإلكتروني خلال جائحة كوفيد-١٩، ويقترح المؤلفون إطاراً للمخاطر يُقسم إلى فئتين: المخاطر العامة (التي تؤثر على جميع أصحاب المصلحة) والمخاطر المحددة (التي تؤثر على مجموعات محددة من أصحاب المصلحة؛ مثل مطوري المحتوى والمدرسين والمؤسسات وما إلى ذلك). كما يسلط الضوء على المخاطر الجديدة التي أدخلها الوباء، مثل الافتقار إلى الاستعداد وزيادة خروقات الأمن، مع التأكيد على الحاجة إلى التدريب والتحفيز وحملات التوعية كتدابير تخفيفية. نجد أنّ هذا البحث ركز على المخاطر بشكل عام في بيئة التعليم الإلكتروني ولم يسلط الضوء على البرمجيات مفتوحة المصدر.

في حين قام الباحثون في الدراسة [7] باستكشاف نقاط الضعف الأمنية في أنظمة التعليم الإلكتروني مفتوحة المصدر Moodle وChamilo وIlias قبل وأثناء وبعد جائحة COVID-19. ومن خلال تحليل شامل للأدبيات الموجودة، وجمع البيانات من قاعدة بيانات CVE، وتحليل البيانات الإحصائية، تم الحصول على رؤى قيّمة حول طبيعة هذه الثغرات، وتأثيرها، واتجاهاتها المحتملة. وقدم الباحثون في نهاية البحث توصيات لأصحاب المصلحة لتحسين الأمان وجعل الأنظمة أكثر استدامة على المدى الطويل.

نجد أنّ هذه الورقة كانت عبارة عن معلومات إحصائية حول الثغرات الأمنية في الكود البرمجي قبل وخلال وبعد COVID-19 ولكنها لم تقم بتصنيف لأصول التعليم الموجودة في تلك المنصات.

٤-هدف البحث:

تحديد ومناقشة القضايا الأمنية المحتملة ذات الصلة بأنظمة التعليم الالكتروني مفتوحة المصدر وسيتم ذلك من خلال:

- -تحليل نظام التّعليم الإلكترونيّ Moodle وبناء كتالوج مخاطر بالاعتماد على نتائج التّحليل.
- -اختبار بعض القضايا الأمنيّة ضمن الـ Moodle.
- -مناقشة نتائج الاختبار.

٥-مواد البحث وطرائقه:

قبل البدء بالدراسة النظرية وتحليل المخاطر ذات الصلة بأنظمة التعليم الإلكتروني مفتوحة المصدر كان لابدّ من تجهيز بيئة العمل وذلك بتشغيل نسخة محليّة من نظام التعليم الإلكتروني Moodle حيث تمّ تجهيز آخر نسخة متوفرة في الموقع الرسمي ل Moodle عند بدء البحث في عام ٢٠٢٢ وهي النسخة Moodle v.4.1 التي سيتم تحليل المخاطر وإجراء تقييم الأمان لها حيث تمّ سحب نسخة من النّظام Moodle v.4.1 وتثبيتها على سيرفر محلي، علماً أنّ الشيفرة البرمجية لنظام Moodle مكتوبة بلغة PHP ومن خلال إعدادات التثبيت اخترنا مخدم الويب Apache ونظام قواعد البيانات MySQL.

٥-١-تحليل المخاطر:

تعتبر عملية تحليل وتقييم المخاطر خطوة مهمة في إدارة المخاطر والتي يتم من خلالها فهم تأثير المخاطر واحتمالية وقوعها، وهذا يساعد في فهم العواقب المحتملة وتحديد أولويات الاستجابة لها وبفضل هذا التحليل، يمكن وضع خطة شاملة لإدارة المخاطر. هذه الخطة تتناسب مع حجم المشروع وطبيعته، مما يضمن نجاحه.

لتحليل المخاطر في Moodle تم اختيار المعيار NISTIR 8286 وهو منشور صادر عن المعهد الوطني للمعايير والتكنولوجيا National Institute of Standards & Technology (NIST) يوفر إرشادات لدمج إدارة مخاطر الأمن السيبراني في استراتيجية إدارة المخاطر المؤسسية الشاملة للمنظمة.

٥-١-١-سجل المخاطر(كتالوج المخاطر):

تمّ اتباع إرشادات هذا المعيار بما يتناسب مع طبيعة Moodle كنظام برمجي وبما يتناسب مع أهداف البحث حيث يوفر هذا المعيار كتالوج (سجل) مخاطر يسمى National Cybersecurity Risk Register على شكل ملف Excel حيث تم التركيز فيه على الأعمدة التي تصف احتمالية حدوث الخطر Likelihood وتأثير الخطر Impact ومقدار التعرّض للخطر Exposure والشكل (١) يوضح هيكلية هذا الكتالوج:

Notional Cybersecurity Risk Register											
ID	Priority	Risk Description	Risk Category	Current Assessment			Risk Response Type	Risk Response Cost	Risk Response Description	Risk Owner	Status
				Likelihood	Impact	Exposure Rating					
1											
2											
3											
4											
5											
Continually Communicate, Learn and Update											

الشكل(١) هيكلية سجل مخاطر الأمن السيبراني [8]

٢-١-٥-مصفوفة التأثير والاحتمالية:

لتحديد مقدار التعرّض للخطر تم الاعتماد على مصفوفة التأثير والاحتمالية التابعة للمعيار NIST SP 800-30 [8] الموضحة في الشكل (٢) حيث نأخذ القيمة التي تقع في تقاطع عمود التأثير مع صف الاحتمالية فهي التي تعبر عن مقدار التعرّض فمثلاً لو أُخِذ التأثير High والاحتمالية Moderate عندها سيكون مقدار التعرّض للخطر هو تقاطعهما أي القيمة Moderate.

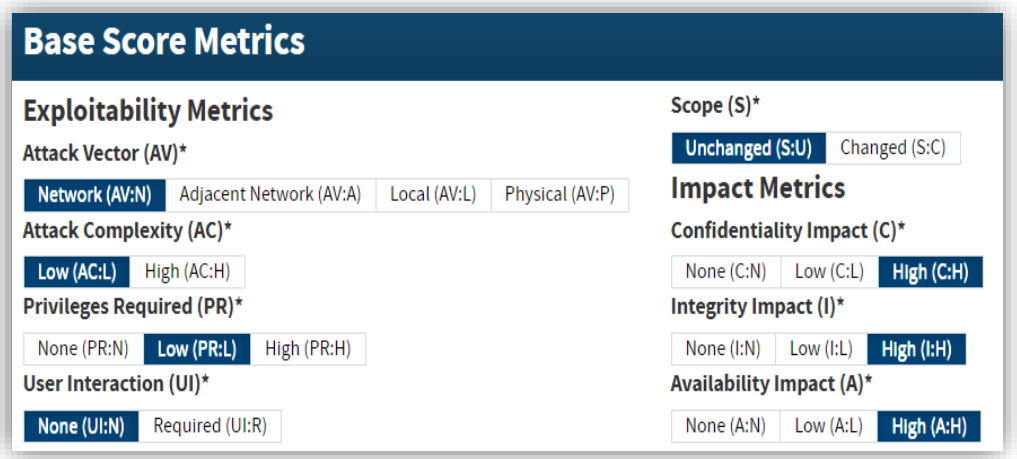
Likelihood (threat occurs and results in adverse impact)						
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low
	Very Low	Low	Moderate	High	Very High
			Level of Impact		

الشكل (٢) مصفوفة التأثير والاحتمالية [8]

تم جمع البيانات حول التأثير والاحتمالية للمخاطر المسجّلة في كتالوج المخاطر من عدة مصادر بعضها اعتمد على مراجعة بعض المقالات ضمن مجال البحث[4],[10],[11]، ومنها ما اعتمد على التجريب العملي بالإضافة للتقارير السنوية لأمان نظام Moodle حيث تم الاستفادة من موقع CVEDetails[٢] الذي يتضمن أرشيف واسع حول الثغرات التي تم تسجيلها في Moodle وتم تحليل تأثير واحتمالية الثغرات بالدخول على نوع الثغرة ورؤية تفاصيلها وعدد الثغرات التي تندرج تحت هذا النوع وأكثر الخواص التي تشترك بها هذه الثغرات من ناحية تأثيرها على السرية والتكاملية والتوافرية وهي المبادئ الأساسية لأمن المعلومات وذلك بالانتقال إلى قاعدة البيانات العالمية NVD التي توفر معلومات مفصّلة عن كل ثغرة، وكمثال على ذلك نرى في الشكل (٣) تفاصيل ثغرة ما حيث نجد أنّ مقاييس التأثير على كل من السرية والتكاملية والتوافرية هو High ومنه نستنتج أن التأثير هو High أما بالنسبة لمقاييس الاستغلال نجد أن الثغرة تؤثر عبر الشبكة وتعقيد الهجوم منخفض والصلاحيات (privileges) المطلوبة لتنفيذها قليلة وبالنسبة لتفاعل المستخدم فهي لا تحتاج لتفاعل حتى يظهر تأثيرها عبر الموقع وبالتالي يمكن تقدير احتمالية حدوثها High.

[2] https://www.cvedetails.com/product/3590/Moodle-Moodle.html?vendor_id=2105

[3] https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2023-28329&vector=AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H&version=3.1&source=NIST



الشكل(٣) تفاصيل ثغرة عبر قاعدة البيانات NVD

٣-١-٥-تحديد الأصول (assets)

تم تحليل النظام Moodle والتعرّف على الأصول assets الموجودة فيه، بالنسبة لبحثنا نجد أنّ بعض الأصول أكثر صلة بالكود البرمجي (كبرمجية مفتوحة المصدر)، وبعضها الآخر أكثر صلة بالتعليم الإلكتروني وجميعها معرّضة للخطر، تم استخراج الأصول وفقاً لما ورد من أصول في البحث [9]، مع إضافة الأصول المستخرجة من النسخة المثبتة لدينا من Moodle والجدول(١) يوضح ما تم استنتاجه من الأصول:

جدول (١) الأصول الموجودة في النظام Moodle [9]

الأصول (assets)	وصف الأصول
موارد التعلّم (lessons)	هي الأصول التي تزود الطلاب بالمحاضرات والملاحظات التعليميّة
الاختبارات عبر الإنترنت (quizzes)	هي الأصول التي تشمل أسئلة الامتحان وإجابات الطلاب
نتائج الطلاب(grades)	يحتفظ هذا الأصل بالمعلومات المتعلقة بأداء الطالب مثل التقييم المستمر، نتائج الوظائف والاختبارات للطالب.
ملف تعريف المستخدم (user profile)	معلومات عن المستخدم
محتويات المنتدى (Forum Contents)	–يتم استخدام هذه الخدمة من قبل الطلاب والمعلمين للمناقشات.
الإعلان (Announcement)	يتم استخدام هذه الخدمة من قبل المسؤول والمعلّم لنشر المعلومات للمستخدم بشكل خاص للطلاب.

الوظائف والواجبات (Students' Assignment)	يقوم الطلاب بتسليم وظائفهم عن طريق تحميل أعمالهم على شكل ملفات في النظام.
الدردشات (chats)	يسمح هذا الأصل للمشاركين في الدورة بإجراء مناقشة متزامنة في الوقت الفعلي في دورة Moodle.
Wikis	هي الأصول التي تسمح للطلاب والمعلمين بإنشاء مستند تعاوني من خلال بناء الصفحات معاً.
معلومات تسجيل الدخول	كلمة المرور
Database(MySQL)	هي الأصل الذي يمكن أن يقوم المستخدم بالاستعلام منه لقراءة معلومات وكذلك التعديل عليه بالإدخال أو الحذف أو التحديث.
Web server	هو الأصل الذي يتم تنفيد الكود البرمجي عليه.
Source code	الكود البرمجي لنظام Moodle مكتوب بلغة PHP وهو متاح لأي مطور ليقوم بإجراء تعديلات عليه.
Plugins	هي مجموعة من الوظائف الإضافية التي يمكن أن تتم إضافتها إلى النواة الأساسية للتطبيق.

١-٣-١-٥- تصنيف الأصول:

يجب معرفة طبيعة هذه الأصول من حيث تأثيرها على المنظمة عندما يتم الكشف عنها أو تغييرها أو إتلافها دون إذن من أشخاص غير مصرح لهم بذلك أو عند حدوث انقطاع في الوصول إليها فإن كان التأثير كبير تسمى أصول مقيّدة وإن كان سلبي عندها تدعى أصول سرية أو أنّ تأثيرها ضئيل فهي أصول عامة وتم تصنيف الأصول بالاستفادة من البحث [9]:

جدول (٢) تصنيف الأصول [9]

الأصول	تصنيف الأصل
التقييم عبر الإنترنت، database(MYSQL) web server, source code, plugins,	مقيّدة
موارد التعلّم، نتائج الطلاب، الوظائف والواجبات، معلومات تسجيل الدخول.	سرية
ملف تعريف المستخدم، محتويات المنتدى، الإعلانات، wikis، الدردشات.	عامة

٤-١-٥ تصنيف المخاطر

تم تصنيف المخاطر ضمن أربعة فئات وهي: مخاطر من نوع ثغرات في الكود ومخاطر ذات صلة بالتصميم ومخاطر ذات صلة بالتطوير بالإضافة لمخاطر تخص الوصول غير المصرح به إلى دور (role) أحد المستخدمين في النظام (مدير النظام – المعلم – الطالب)

٥-٢ أدوات تنفيذ هجمة أمنية:

١. استخدام متصفحين أحدهما متصفح للمهاجم Microsoft Edge والآخر متصفح للضحية Mozilla Firefox.

٢. استخدام الأداة Ncat وهي أداة لكتابة الأوامر تُستخدم لقرأءة وكتابة البيانات عبر الشبكة حيث يستخدمها المهاجم للحصول على ملف تعريف ارتباط (Cookie) الضحية.

٣. استخدام Cookie-Editor وهي ملحق يمكن إضافته للمتصفّحات حيث يتيح محرر ملفات تعريف الارتباط للمستخدمين إضافة ملفات تعريف الارتباط المرغوبة أو تعديلها أو إزالتها على أي موقع ويب.

٦-التطبيق العملي:

١-٦-محاكاة هجمة أمنية:

إنّ فهم طبيعة وتأثير الهجمات الأمنية يزيد الوعي بالمخاطر الأمنية بين المطورين والمسؤولين، فمن خلال توثيق وتقديم محاكاة لهجمة أمنية، يمكن تطوير وتنفيذ تدابير أمنية فعّالة لتعزيز أمان منصة التعليم الإلكترونيّ وهذا ما يعزّز إرشادات معيار NISTIR 8286.

الغرض الأساسي من محاكاة الهجوم الإلكتروني هو تحديد ومعالجة الثغرات الأمنية بشكل استباقي داخل البنية التحتية للأمن الإلكتروني في المؤسسة، إنه نهج واقعي لفهم مدى قدرة المؤسسة على الصمود في مواجهة أنواع مختلفة من التهديدات الإلكترونية. من خلال محاكاة تكتيكات وتقنيات وإجراءات الهجوم في العالم الحقيقي، فإنّه يختبر فعالية تدابير الأمن الحالية وقدرات الاستجابة للحوادث. كما أنه يساعد في تحديد الثغرات التقنية والإجرائية التي يمكن أن يستغلها الخصوم. يساعد هذا التقييم الاستباقي في تعزيز وضع الأمن الإلكتروني العام للمؤسسة، مما يجعل من الصعب نجاح الهجمات الإلكترونية الفعلية.

١-١-٦-هجمة أمنيّة من النوع Stored XSS:

ما هي ثغرة Stored XSS؟

XSS اختصار لـ Cross-Site Scripting(البرمجة النصية عبر المواقع)، وهي نوع من الهجمات التي تحدث عند إدخال تعليمات برمجية ضارة في صفحة ويب لحقنها أو تشغيلها لاحقاً من قبل زائرين آخرين للصفحة قد تكون مثلاً عن طريق زيارة رابط ما أو التمرير فوق عنصر ما في الصفحة. "Stored XSS" أو "Persistent XSS" [12] تعني أن الشيفرة البرمجية الضارة يتم تخزينها في قاعدة بيانات التطبيق المستهدف بحيث يتم

[4] https://nmap.org/ncat/guide/index.html
[5] https://cookie-editor.com/

تنفيذها في كل مرة يتم فيها تحميل الصفحة المحقونة، تسبب هذه الثغرة أضراراً لأنها يمكن أن تتيح للمهاجمين سرقة بيانات المستخدمين، تنفيذ الأكواد الضارة، والتحكم في جلسات المستخدمين دون علم منهم أو وجود إشارة تدل على أنّه تم التعرض لهجوم ما.

لماذا تم اختيار هذا النوع من الثغرات في منصة التعليم الإلكتروني Moodle؟

عند العودة إلى تقارير الأمان في قاعدة البيانات CVE نجد أن أكبر عدد من الثغرات في Moodle تابع للنوع XSS وتم اختيار النوع Stored XSS نظراً لخطورته على الأصول البرمجية وأصول التعليم الإلكتروني ولأنّه يستمر بالظهور في كل مرة يتم تحميل الصفحة المحقونة بكود ضار أي أنّ تأثيرها ليس لمرة واحدة وإنّما مستمر طالما لم يتم معالجته.

٢-١-٦- متطلبات تنفيذ الهجمة الأمنية من النوع Stored XSS:

قبل البدء في تفاصيل الهجمة الأمنيّة تم إنشاء حساب لعدة أنواع من المستخدمين على النّظام Moodle وهم: حساب لمدير النظام (admin) وحساب لمعلم (teacher) وحساب لطالب (student)، حيث يختلف كل حساب عن الآخر من ناحية الصلاحيات المتاحة لكل مستخدم علماً أن مدير النظام يملك أعلى الصلاحيات يليه المعلم ثم الطالب. في هذه الهجمة الأمنية يوجد مستخدم سيقوم بحقن تعليمات برمجية ضارة وهو يعتبر المهاجم ومستخدم آخر سينفذ هذه التعليمات بطريقة ما دون أن يعلم وهو يعتبر الضحيّة.

٣-١-٦-الخطوات التي تم تنفيذها لاستغلال الثغرة Stored XSS:

١. في نظام Moodle يُسمح لمدير النظام أو المعلم أن يقوم بإنشاء wiki، في هذه المحاكاة سجلنا دخول إلى Moodle بدور المعلم (المهاجم) عبر متصفح Microsoft Edge وقمنا بإعطاء هذه ال wiki اسم

E-learing oss.

٢. عند البدء بإنشاء wiki نلاحظ وجود حقل لإضافة وصف لهذه ال wiki (wiki description)، يقوم المهاجم بجعل الوصف على شكل رابط link والذي يتطلب إدخال العنوان الذي سيتوجه إليه الرابط.

٣. ضمن حقل العنوان يقوم المهاجم بحقن حمولة (تعليمات برمجية ضارة) بلغة جافا سكريبت كمايلي:

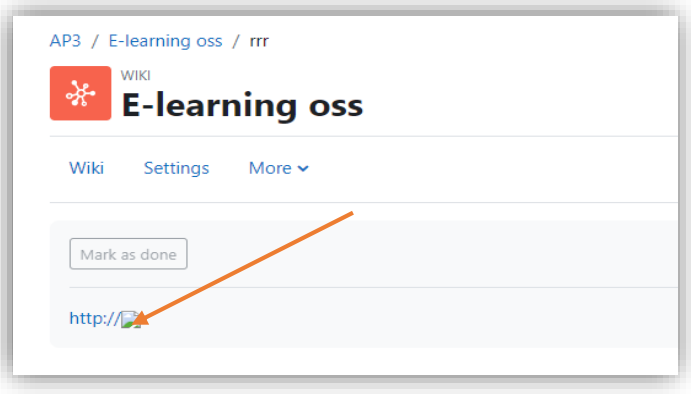
```
<img src=x onerror="(new Image()).src='http://127.0.0.1:8000/' +
document.cookie">
```

شكل(٤) الحمولة التي تم حقنها

وصف هذه الحمولة وتأثيرها:

تقوم هذه الحمولة بالإشارة إلى صورة مصدرها src غير موجود وبالتالي ينشأ خطأ نتيجة ذلك، هذا الحدث يُنشئ صورة على السيرفر 127.0.0.1:8000 ومع تلك الصورة يستقبل هذا السيرفر ملف تعريف ارتباط المستخدم الذي سيرى وصف ال wiki.

في كل مرة يقوم بها مستخدم بالدخول على ال wiki حكماً سيرى الوصف الخاص بها والذي هو على شكل رابط لصورة وعندها سيتم إرسال ملف تعريف ارتباط هذا المستخدم إلى سيرفر المهاجم (المعلم).



الشكل(٥) وصف ال wiki على شكل رابط

٤. يقوم المهاجم بتجهيز سيرفر خاص به ليقوم باستقبال ملفات تعريف ارتباط المستخدمين الآخرين، هذا السيرفر تم تشغيله باستخدام أداة Ncat كما يلي:

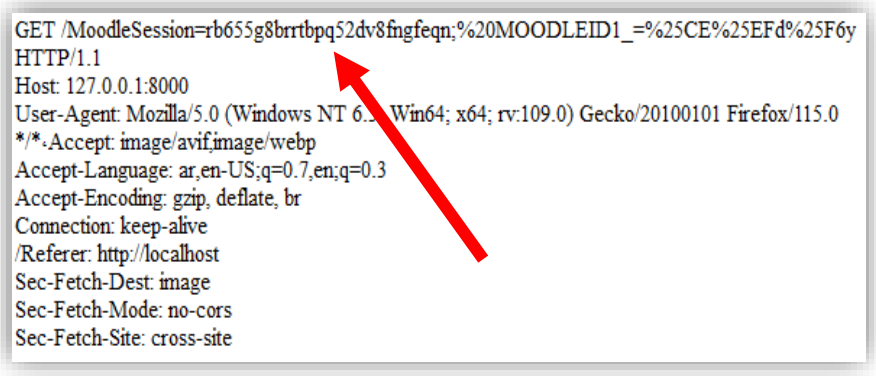
١- التنصت على المنفذ رقم ٨٠٠٠ من خلال الأمر ncat –l –p 8000

٢- تشغيل السيرفر على المنفذ ٨٠٠٠ من خلال الأمر ncat –nv 127.0.0.1:8000.

٣- الاحتفاظ بالبيانات المسروقة ضمن ملف نصي من خلال الأمر

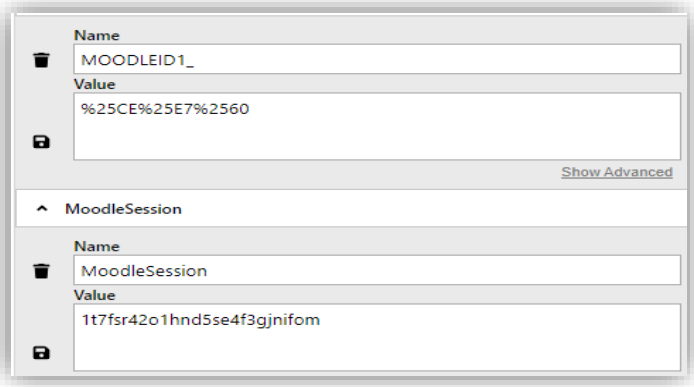
Echo –e 'HTTP\1.1 200 ok\r\n' | ncat –lp 8000> result.txt

٥. الدخول إلى تلك ال wiki عن طريق حساب مدير النظام (الضحية) من متصفح Mozilla Firefox وبالتالي مجرد أن يرى وصف ال wiki سيتنفذ كود الجافا سكريبت ويتم إرسال ملف تعريف الارتباط الخاص به إلى سيرفر المهاجم (المعلم) الذي يحتفظ به في الملف النصي result حيث يتضمن ملف تعريف الارتباط في Moodle على مكونين هما MoodleSession وMOODLEID كما يظهر في الشكل (6):

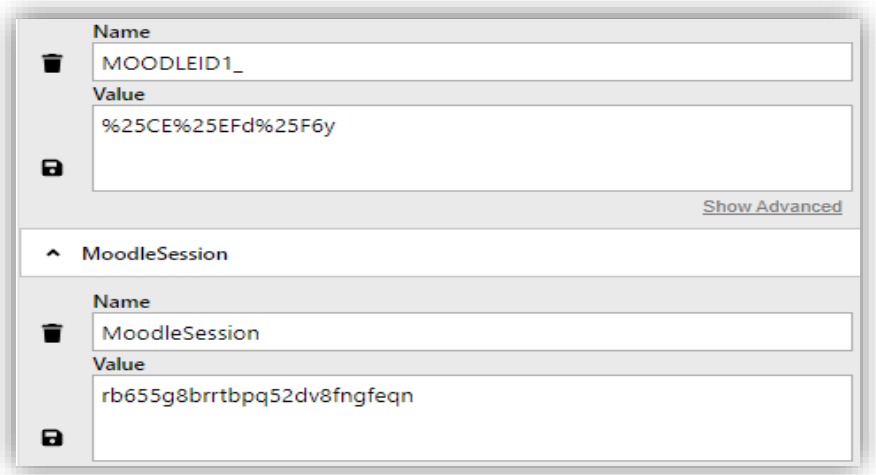


الشكل(٦) cookies التي تمت سرقتها

٦. يستخدم المهاجم الأداة cookie Editor ليضع ملف تعريف مدير النظام بدلاً من ملف تعريفه وعندها سيحصل على وصول غير مصرح به إلى حساب مدير النظام وبإمكانه التحكم بأي إعدادات أو مهام كان يقوم بها مدير النظام.



الشكل(٧) ملف تعريف ارتباط المهاجم



الشكل(٨) تعديل ملف ارتباط المهاجم ووضع ملف تعريف ارتباط الضحية

٤-١-٦-كيف تؤثر هذه الهجمة على بيئة التعليم الإلكتروني؟

المعلم يمكن أن يقوم بهذا الهجوم ويستطيع أن يحقن كود الجافا سكريبت لأن لديه صلاحية إنشاء wiki، قد يتأثر بهذا الهجوم مدير النظام أو معلّم آخر أو أحد الطلاب، يقوم المعلم بذلك ليصل إلى صلاحيات لا تتوفر لديه فهو قد ينتمي لمقرر ما course ولا ينتمي لمقرر آخر فيهاجم مستخدم لديه صلاحيات الوصول للمقرر الآخر سواء كان هذا المستخدم مدير النظام أو طالب أو معلم آخر ولكن الأكثر خطورة هو أن يصل بشكل غير مصرّح به إلى حساب مدير النظام لأن مدير النظام يملك جميع الصلاحيات وله تأثير على كل الأصول في النظام فكلما زاد عدد الصلاحيات المتاحة لمستخدم ما كلما زادت الأصول المتأثرة.

٥-١-٦-التحسينات التي قد تخفف من هذا الهجوم:

١- بالعودة إلى الإعدادات الافتراضية لملف تعريف الارتباط ضمن النظام Moodle نجد أنّ مدة صلاحية ملف تعريف الارتباط هي ٨ ساعات ثم بعد ذلك يتم تسجيل خروج من حساب كل مستخدم ولذلك أحد الحلول لتجنب استمرار سيطرة المهاجم على حساب الضحية هو أن يتم تقليل مدة صلاحية الجلسة أي مدة صلاحية ملف تعريف الارتباط إلى مدة قصيرة.

٢- استخدام ماسحات الثغرات الأمنية باستمرار للتأكد من وجود ثغرات جديدة في الكود البرمجي والتي تكتشف وجود أكواد تم حقنها في الكود الأساسي للنظام Moodle.

٣- استخدام تقنيات تنقية المدخلات المقدّمة من المستخدم التي يتم إدخالها في المربع النصي الخاص بوصف ال wiki لكي يتم التأكد من أنّها لا تحتوي على مزيج من أكواد HTML و java script التي يمكن أن يتم حقنها في وصف wiki.

٧-النتائج والمناقشة:

١-٧-بناء كتالوج مخاطر:

تم بناء ملف Excel شامل وواسع يتضمن تفاصيل حول التأثير والاحتمالية ومقدار التعرّض للخطر بالإضافة لتصنيف الخطر Risk Category، والعمود الأخير في الجدول تمت إضافته بما يخدم البحث ليوضح ماهي أكثر الأصول المتأثرة بوقوع ذلك الخطر، والجدول (٣) يوضح مقتطف من ملف ال Excel مع مثال عن كل صنف من الأصناف المذكورة سابقاً.

جدول(٣) مقتطف لبعض المخاطر المضمنة في كتالوج المخاطر

Risk Description according CIA	Risk Category	Likelihood	Impact	Exposure Rating	Assets
XSS	Vulnerabilities in code	Low	Moderate	Low	Source code, plugins
Adoption of Immature MOODLE Platform	Development risk	Moderate	High	Moderate	Source code, plugins
Default setting	Design risk	Low	Moderate	Low	All assets
An unauthorized access to teacher role	Teacher's role risk	Moderate	Moderate	Moderate	Lessons, quizzes,forum content, chats, announcements, grades, assigments, wikis,

٢-٧-نتائج التطبيق العملي:

-نلاحظ أنّ إجراء محاكاة لهجمة أمنيّة يعزز الفهم أكثر لطبيعة النظام وأين قد تتواجد نقاط الضعف فيه (vulnerabilities) حيث نجد هنا أنّ الثغرة موجودة في المنطقة المخصصة لوصف الويكي (wiki description).

-تمكننا المحاكاة أيضاً من فهم تأثير الثغرة على النظام وكيفية تأثيرها على بيانات المستخدم أو اختطاف الجلسة أو تخريب صفحات الويب. في بحثنا، الثغرة كان لها تأثير على كافة المستخدمين في النظام حيث بإمكان المهاجم اختطاف جلسة أي مستخدم آخر.

-يساعد إجراء المحاكاة على تحسين الأمان: فمن خلال إجراء عمليات المحاكاة هذه، يمكنك تحسين الأمان العام لنظام Moodle، مما يضمن حماية حسابات جميع المستخدمين بشكل أفضل.

٨-الاستنتاجات والتوصيات:

من خلال البحث يمكن أن نستنتج ما يلي:

-استمرار وجود بعض الثغرات من أول نسخة ل Moodle وصولاً إلى النسخ الحديثة منه، مثل XSS و SQL Injection لا يعني بالضرورة أنّه لم يتم معالجة هذه الثغرات، وإنّما قد تتم معالجة ثغرات من هذه الأنواع في أحد مكونات Moodle ولكن نظراً لمجتمع المطورين الكبير والذي قد يؤدي إلى إضافة مكونات وتعليمات برمجية إضافية جديدة أو حذفها أو تعديلها والذي بدوره يسبب خلل جديد في النظام يمكن استغلاله من خلال إحدى الثغرات المذكورة.

-ضمن كتالوج المخاطر قد نرى أن بعض الثغرات معدل التعرض لها منخفض، ولكن هذا لا ينفي أنّ تأثيرها في حال حصلت سيكون كبير.

-استخدام برمجية مفتوحة المصدر في مجال التعليم الإلكتروني له جانب إيجابي من الناحية الأمنية لأن المجتمع الكبير من المساهمين يساعد على حل المشكلات الأمنية بأسرع وقت ممكن، وعند العودة إلى حالة الدراسة الخاصة بنا في نظام moodle نلاحظ أنّ الموقع لديه سياسة إفصاح فيما يخص الثغرات أي أنّ أي مطور يكتشف ثغرة عليه أن يقوم بإرسال المشكلة للموقع قبل أن يخبر بها عامة المستخدمين لكي لا يتم استغلالها من قبل عدد كبير

من المستخدمين قبل أن يتم إيجاد حل مناسب لها، لكن هذا لا ينفي أن هناك جانب سلبي وهو أنه قد يكون من اكتشف الثغرة هو مهاجم ولديه الخبرة في استغلال تلك الثغرة والذي بدوره يؤثر على عدد كبير من المستخدمين الضحايا له.

-التقارير السنوية لأمان moodle ليس بالضرورة أن تتضمن أو تحصر كل المشاكل الموجودة في النسخ وبالتالي قد يكون هناك ثغرات لم يتم اكتشافها بعد ولكن تحمل خطر كبير في حال حصلت، وقد تنشأ بعض الثغرات حسب ما تقوم به المنظمة من تخصيص للنظام على السيرفرات المحلية لها.

-على الرغم من أنّ بعض الأصول assets عامة ولكن يمكن من خلالها استغلال ثغرة ما وحقن كود برمجي ضار قد يسبب وصول غير مصرح به إلى أحد المستخدمين.

يساهم هذا البحث في تنامي المعرفة حول أمان منصة التعليم الإلكتروني Moodle ويوفر أساساً لمزيد من الدراسات حول النسخ الأحدث من Moodle التي لم تتضمن التقارير السنوية إلا القليل من الثغرات المكتشفة والمسجلة بشكل رسمي فيها وذلك لأنّها نسخ حديثة وما تزال تخضع للتجريب من قبل المستخدمين والمطورين والتي تحتمل في المستقبل تسجيل ثغرات إضافية نتيجة استخدامها على نطاق أوسع مع مرور الوقت. يوصي البحث بأن يكون لدى المنظمة التعليمية (مثل الجامعة) فريق متخصص في تكنولوجيا المعلومات يضم متخصصين في الأمن لدعم ومراقبة نظام التعليم الإلكتروني.

٩-المراجع:

1. Shersad, F., & Salam, S. (2020). Managing risks of E-learning during COVID-19. *International Journal of Innovation and Research in Educational Sciences*, *7*(4), 2349-5219.

2. Kurochkina, A. A., Lukina, O. V., Krasnov, S. V., & Kalinina, A. S. (2024). Improving the Efficiency of Using LMS Moodle in the Educational Process by Implementing Gamification Technologies. In *Understanding the Digital Transformation of Socio-Economic-Technological Systems: Dedicated to the 120th Anniversary of Economic*

Education at Peter the Great St. Petersburg Polytechnic University (pp. 419-435). Cham: Springer Nature Switzerland.

3. Vetter, G. R. (2008). Claiming Copyleft in Open Source Software: What if the Free Software Foundation's General Public License (GPL) Had Been Patented. *Mich. St. L. Rev.*, 279.

4. Council, F. F. I. E. (2004). Risk Management of Free and Open Source Software. *Financial Institution Letter (October 21), from http://www.ffiec.gov/ffiecinfobase/resources/info_sec/2006/frb-sr-04-17. pdf.*

5. Mohammadi, H., Monadjemi, S. A., Moallem, P., & Olounabadi, A. A. (2008). E-learning system development using an open-source customization approach. *Journal of Computer Science*, *4*(5), 360.

6. Floyd, C., Schultz, T., & Fulton, S. (2012). Security vulnerabilities in the open source Moodle eLearning system. In *Proceedings of the 16th Colloquium for Information Systems Security Education*.

7. Akacha, S. A. L., & Awad, A. I. (2023). Enhancing Security and Sustainability of e-Learning Software Systems: A Comprehensive Vulnerability Analysis and Recommendations for Stakeholders. *Sustainability*, *15*(19), 14132.

8. Stine, K., Stine, K., Quinn, S., Witte, G., & Gardner, R. K. (2020). *Integrating cybersecurity and enterprise risk management (ERM)* (Vol. 10). US Department of Commerce, National Institute of Standards and Technology.

9. Zamzuri, Z. F., Manaf, M., Ahmad, A., & Yunus, Y. (2011). Computer security threats towards the e-learning system assets. In *Software Engineering and Computer Systems: Second International Conference, ICSECS 2011, Kuantan, Pahang, Malaysia, June 27-29, 2011, Proceedings, Part II 2* (pp. 335-345). Springer Berlin Heidelberg.

10. Ally, M. S. (2016). Secure Software Deployment: Investigating the Security Vulnerabilities of MOODLE LMS in Public Higher Learning Institutions in Tanzania. *International Journal of Advanced Information Science and Technology (IJAIST), ISSN: 2319*, *2682*.

11. Stapić, Z., Orehovački, T., & Đanić, M. (2008). Determination of optimal security settings for LMS Moodle. In *Proceedings of 31st MIPRO International Convention on Information Systems Security* (Vol. 5, pp. 84-89).

12. 13- Mokbal, F. , Dan, W. , Xiaoxi ,W. , Wenbin, Z. , & FU, L. (2021) . XGBXSS: An Extreme Gradient Boosting Detection Framework for Cross-Site Scripting Attacks Based on Hybrid Feature Selection Approach and Parameters Optimization. Journal of Information Security and Applications, vol. 58, 10-16.