ثغرات الإدخال في قواعد البيانات لنظام موودل المستخدم في جامعة السودان المفتوحة وحمايتها *

أ. محمد عوض محمد عطا الفضيل **

* تاريخ التسليم: 2014/10/8م، تاريخ القبول: 2014/12/2م.

** محاضر/ مركز التعليم الإلكتروني/ رئاسة الجامعة/ جامعة السودان المفتوحة.

ملخص:

قام الباحث بتقسيم البحث إلى ثلاثة أطر رئيسة، الأول الإطار العام للبحث الذي يشمل مشكلة البحث وأهدافه وأهميته وفرضياته وإجراءاته، كما تناول فيه مصطلحات البحث.

والإطار الثاني هو الإطار النظري للبحث الذي شمل تجربة جامعة السودان المفتوحة في تطبيق التعليم الالكتروني؛ ونظام موودل؛ وثغرات الإدخال في قواعد البيانات والدراسات السابقة.

أما الإطار الثالث فهو الإطار العملي للبحث الذي خصصه الباحث للشيفرات البرمجية للملفات المصابة وترقيعها. وأخيراً تناول الباحث نتائج الدراسة والتوصيات.

هدف البحث لمعرفة مدى وجود ثغرات إدخال قواعد البيانات في شفرة نظام موودل MOODLE الأساسية، ومدى إمكانية ترقيع هذه الثغرات للحيلولة دون اختراق هذا النظام وحماية البيانات فيه. وللوصول لأهداف هذا البحث استخدم الباحث المنهج التطبيقي، الذي استخدم فيه خبرته الشخصية في التعامل مع نظام موودل والتعامل مع لغة البرمجة PHP، وكذلك استخدم أداة Acunetix Web Vulnerability Scanner. وخلص البحث إلى وجود ثغرتين في الشفرة البرمجية الأساسية للنظام قيد الدراسة. وقام الباحث في نهاية المطاف بترقيع هذه الثغرات على النظام. طبقت الدراسة العملية على موقع منطقة الخرطوم التعليمية بجامعة السودان المفتوحة والمستخدم فيه نظام موودل كنظام أساسي.

Input Gaps in the Databases and Protection of the Model System Used in Sudan Open University

Abstract:

This research deals with the issue of (Sql injection in MOODLE which used in the Open University of Sudan) . It includes three frameworks: the first is the general framework of the research, which consists of the research problem, objectives, importance, hypotheses and procedures of the research; the second discusses the theoretical framework of research, which includes the E- Learning in the Open University of Sudan, MOODLE, Sql Injection and the previous studies, and finally, is the practical framework where the researcher writes the vulnerabilities and loopholes in MOODLE code. At the end of the research, the researcher discusses the results and recommendations.

This research aims to find out how the presence of sql injection threats in the core of MOODLE code and the possibility of patching these threats to prevent the hacking of the system and protect the data therein. The research found out two of the software vulnerabilities and loopholes in MOODLE code, sql injection and blind sql injection. Eventually the researcher patched these vulnerabilities through using a practical approach, which depend on the researcher experience in dealing with MOODLE and PHP programming language, as well as using the Acunetix Web Vulnerability Scanner tool. The study was applied to the Open University of Sudan, Khartoum region web site, where MOODLE is used as a main platform.

الإطار العام للبحث:

1ـ مقدمة البحث:

يعدُّ نظام موودل من نظم إدارة المحتوى التعليمي مفتوحة المصدر، وهو نظام عالمي مستخدم في عشرات الآلاف من المؤسسات التعليمية حول العالم، والعدد في تزايد مستمر يوماً بعد يوم (http://www.moodle.org) .وبناء على المميزات الكثيرة التي تميز نظام موودل عن غيره من نظم إدارة المحتوى التعليمي، نظَّمت حكومة السودان ممثلة بوزارتي التعليم العالي والبحث العلمي ووزارة العلوم والاتصالات دورتين تدريبيتين في 2009م و2013م لتدريب أساتذة الجامعات السودانية للتعامل مع النظام، وذلك تمهيداً لاعتماده كنظام أساس في إدارة التعليم الالكتروني بالبلاد [1] ، وكان نتاج ذلك أن قامت الكثير من الجامعات السودانية باعتماده كنظام أساس لإدارة عملية التعليم الالكتروني بها؛ وأولى هذه الجامعات هي جامعة السودان المفتوحة.

بدأ تطبيق النظام بجامعة السودان المفتوحة منذ عام 2009م، ومن خلال التجربة تبين أن هناك عقبات عدة تواجه تطبيق هذا النظام وكان من أهمها العقبة الأمنية، وذلك من ناحيتين، الناحية الأولى هي ثغرات الإعدادات الأمنية في نظام موودل، وتم التغلب عليها بوساطة تدريب مدير النظام في الجامعة، أما الناحية الثانية فتمثلت في وجود عدد من الثغرات البرمجية التي نفذ من خلالها القراصنة في العام 2012م وقاموا بسرقة بيانات النظام.ومن هنا تبين أنه لابد من إجراء دراسة بحثية للوقوف على هذه الثغرات وترقيعها.

2ـ مشكلة البحث:

تتمثل مشكلة البحث في أن نظام موودل معرض للهجمات الالكترونية عبر كثير من الثغرات التي لا يجيد مديرو النظام في الجامعات السودانية طرق التعامل معها وسدها.وفي هذا البحث يقوم الباحث بالإجابة عن السؤال الرئيس الآتي:

ما الثغرات المكتشفة في إدخال قواعد البيانات لنظام موودل وكيف يمكن حمايتها؟ والذي يتفرع إلى سؤالين فرعيين على النحو الآتي:

1. ما الثغرات المكتشفة في إدخال قواعد البيانات لنظام موودل المستخدم في جامعة السودان المفتوحة؟

(1) كان الباحث أحد أفراد لجنة التدريب.

2. كيف يمكن حماية قواعد البيانات لنظام موودل المستخدم في جامعة السودان المفتوحة من الاختراق؟

3ـ أهمية البحث:

تنبع أهمية هذا البحث مما يأتي:

1. التغلب على أهم مشكلة تواجه مستخدمي النظم مفتوحة المصدر في التعليم الإلكتروني، وهي مشكلة أمن البيانات والمعلومات وسريتها.

2. اكتشاف ثغرات الإدخال في قواعد البيانات في نظام موودل النسخة 1.9.5 يفيد جامعة السودان المفتوحة والجامعات الشبيهة بها، والتي تستخدم هذه النسخة من النظام في المحافظة على البيانات والمعلومات في قواعد بيانات النظام، والتي تشمل معلومات الطلاب ومعلومات مدير النظام ومعلومات الاختبارات وغيرها.

3. تم من خلال التطبيق العملي للبحث حماية قواعد بيانات نظام موودل النسخة 1.9.5 المستخدمة في جامعة السودان المفتوحة.

4ـ حدود البحث:

1. الحدود الزمنية: الفترة من فبراير 2014م وحتى أغسطس 2014م.

2. الحدود المكانية: جامعة السودان المفتوحة – مركز التعليم الالكتروني – منطقة الخرطوم التعليمية.

3. الحدود الموضوعية: نظام التعليم الإلكتروني MOODLE النسخة 1.9.5

5ـ مصطلحات البحث:

◄ **الثغرات**: يستخدم الباحث تعبير الثغرات للإشارة إلى أماكن الضعف في هذه النظم، والتي تتيح للمهاجم الاعتداء على سلامة النظام.

◄ **الإدخال في قواعد البيانات**: يقصد بها الباحث تضمين شفرات برمجية ضمن النص البرمجي للنظام للتأثير على قواعد البيانات فيه بصورة غير شرعية.

◄ **جامعة السودان المفتوحة**:

هي جامعة حكومية سودانية أُنشئت عام 2002م، وهي تتبنى التعليم المفتوح في السودان.

6ـ إجراءات البحث:

1.6 منهج الدراسة:

اتبع الباحث المنهجين الوصفي التحليلي والتطبيقي الإجرائي، واختار الباحث هذين المنهجين بعد اطلاعه على الأدبيات ذات الصلة بطرق البحث ومناهجه.ويقصد بالمنهج الوصفي التحليلي، ذلك المنهج الذي يرتبط بدراسة الواقع الحالي لظاهرة حاضرة بقصد وصفها وتفسيرها، ومن ثم تحسين الظروف التي تهيئ لها أفضل مما هي عليه، وهذا يدل علي أن المنهج الوصفي التحليلي يتعدى وصف الظاهرة موضوع الدراسة المدروسة وتفسيرها لتقديم مقترحات لعلاج ما قد يظهر فيها من قصور ونقاط ضعف بغرض تطويرها والوصول بها إلي الأحسن، وهذا المفهوم يتفق مع ما سعى إليه الباحث في دراسته الحالية، إذ إنه حاول التعرف إلى ثغرات الإدخال في قواعد البيانات في نظام موودل المستخدم في جامعة السودان المفتوحة، ومن ثم الإسهام في وضع الحلول وتقديم البدائل المناسبة للتغلب على ما قد تظهره نتائج البحث.

أما المنهج التطبيقي الإجرائي فيقصد به ذلك المنهج الذي يوجه نحو مهمة معينة، ويهدف إلى إنتاج معرفة مرتبطة بإيجاد حل يمكن تعميمه على مشكلة عامة.وهذا المفهوم أيضاً يتفق مع ما سعى إليه الباحث في دراسته الحالية، إذ إنه قام بترقيع الثغرات التي توصل إليها في النظام المستخدم في جامعة السودان المفتوحة، ويمكن تعميم ما قام به الباحث على نظام موودل في المؤسسات الشبيهة.

2.6 مجتمع البحث وعينته:

اختار الباحث نظام إدارة التعليم الالكتروني مفتوح المصدر (موودل) ليقوم بإجراء الدراسة عليه، وذلك لما يتميز به النظام من إمكانات برمجية فائقة، ولأنه النظام الأول عالمياً المستخدم في إدارة نظم التعليم الالكتروني في المؤسسات الأكاديمية المختلفة من جامعات ومدارس ومعاهد وغيرها، وأخيراً لأنه النظام المستخدم في جامعة السودان المفتوحة لإدارة العملية التعليمية، وهي الجامعة التي اختارها الباحث لتطبيق الدراسة التطبيقية.

والنظام الذي أجرى عليه الباحث دراسته هو النسخة المستخدمة على موقع التعليم الالكتروني لجامعة السودان المفتوحة قطاع الخرطوم http:// ous– edu.com/ kha/ ، وهي النسخة 1.9.5 من النظام.

3.6 أدوات الدراسة:

1. برنامج Acunetix Web Vulnerability Scanner.
2. لغة البرمجة PHP.

1. برنامج

Acunetix Web Vulnerability Scanner. (http:// www.acunetix.com)

هو برنامج يقوم بفحص كل ما هو موجود على الموقع الالكتروني بصورة دقيقة، ويقدم تقريراً شاملاً عن الثغرات في الموقع، وهو من أكثر الأنظمة التي يستخدمها المخربون للبحث عن الثغرات في المواقع والأنظمة، وذلك لتحديد الثغرات الموجودة في النظام، سواء كانت ثغرات برمجية أم ثغرات إعدادات، ومن ثم اختراق المواقع عبرها.وقد استخدم الباحث هذا النظام للبحث عن مزيد من الثغرات في النظام قيد الدراسة بعد أن قام بالعثور على جزء منها عن طريق الفحص اليدوي.

2. لغة البرمجة PHP:

هي لغة برمجة نصية صممت أساساً من أجل استخدامها لتطوير تطبيقات الإنترنت وبرمجتها، كما يمكن استخدامها لإنتاج برامج قائمة بذاتها وليس لها علاقة بالانترنت.ولغة أل PHP هي لغة مفتوحة المصدر يطورها فريق من المتطوعين تحت رخصة PHP، وهي تدعم البرمجة كائنية التوجه.ويستخدمها الباحث في هذه الدراسة، لأنها اللغة المكتوب بها النظام قيد الدراسة، وبالتالي سيستخدمها في كتابة الشفرات البرمجية في الدراسة التطبيقية.

4.6 خطوات البحث:

- تحديد المشكلة وأبعادها.
- تحديد منهج وأدوات البحث.
- إجراء دراسة نظرية عن:
  - نظام موودل.
  - تجربة جامعة السودان المفتوحة في التعليم الالكتروني.
  - ثغرات الإدخال في قواعد البيانات.
- الاطلاع على الدراسات السابقة.
- تقديم النتائج والتوصيات.

الإطار النظري للبحث والدراسات السابقة:

1ـ تجربة جامعة السودان المفتوحة في التعليم الالكتروني (جامعة السودان المفتوحة 2011م):

أتى الاهتمام بالتعليم الالكتروني في جامعة السودان المفتوحة كضرورة ملحة للانتشار الواسع للحاسوب، والتطور المذهل لتقنيات التعليم وبرمجياته، ولما يقدمه من مميزات ووسائط تساعد وبشكل ملحوظ في درجة التحصيل وتبسيط المعلومة للطالب وتتمثل أهمها في:

- يحقق للجامعة عالمية الانتشار.
- يعطي الجامعة أفضل درجات الجودة والترتيب العالمي بين الجامعات.
- أفضل وأسرع وسيلة لتحقيق شعار الجامعة التعليم للجميع.
- يقلل تكلفة التعليم ويختصر المسافات والوقت.
- يزيد من جودة التعليم.

لذلك تم إنشاء مشروع التعليم الالكتروني كي يلبي ولو جزء من احتياجات هذا القطاع العريض.

1-1 نشأة مركز التعليم الالكتروني (جامعة السودان المفتوحة 2011م) :

بدأ التعليم الالكتروني في جامعة السودان المفتوحة كقسم بإدارة إنتاج الوسائط التعليمية، وهي الإدارة التي كانت تعنى بعملية إنتاج الوسائط التعليمية جميعها من كتب ووسائط سمعية وبصرية والكترونية؛ وفي عام 2007م حُلَّت إدارة الإنتاج ووزِّعت أقسامها ومهماتها إلى إدارات أخرى، وكان أن تحول قسم التعليم الالكتروني ليكون تحت إشراف إدارة البرامج الأكاديمية، وأخيراً وفي عام 2009م تحول إلى مشروع (باسم مشروع التعليم الالكتروني) ، ومن ثم إلى (مركز التعليم الإلكتروني) وما زال بهذه الصفة وهذا المسمى حتى اليوم.

كان الإنتاج الالكتروني يتم عن طريق شركات متخصصة في هذا المجال، حيث كانت الإدارة تتعاقد مع الشركات التي تأنس فيها الكفاءة لإنتاج مقررات الجامعة في شكل الكتروني، وفي سياق التعاقد نفسه مع الشركات، قامت إدارة الجامعة بإنشاء شراكة مع شركة كوش تتمثل في تكوين شركة باسم شركة أعمال التعليم لتتولى الإنتاج الالكتروني لمقررات الجامعة عام 2005م – 2006م، ولم تصمد هذه الشراكة طويلاً حيث انسحبت الجامعة بعد تقويم التجربة؛ ومن الشركات التي تعاملت معها الجامعة في مجال الإنتاج الالكتروني شركة إمام للتقنية وشركة الفاروق للإنتاج الفني وشركة قرطبة للإنتاج الإعلامي.

بعد ذلك اتجه قسم التعليم الالكتروني بإدارة الإنتاج إلى الإنتاج الذاتي، ففي بدايات عام 2007م قام المشروع بتدريب مجموعة من المتعاونين على كيفية إنتاج المقررات التعليمية وفق معايير ونظام التعليم الالكتروني المعتمد لدى الجامعة وهو نظام موودل MOODLE حيث أنتج أكثر من 400 مقرَّر من مقررات الجامعة في تلك الفترة بصورة الكترونية.بعدها قام المشروع بوضع معايير لإنتاج مقررات الدراسات العليا، ودُرِّبت مجموعة من المتعاونين على ذلك، حيث تمكن المشروع حتى الآن من إنتاج ما يربو على مائة مقرر من مقررات الدراسات العليا بالجامعة.

يتكون المركز حالياً من وحدات عدة لكل منها مهمتها، وهي:

- وحدة إدارة المواقع التعليمية.
- وحدة الوسائط المتعددة.
- وحدة الفصول والمعامل الافتراضية.
- وحدة المتابعة والتنسيق.
- وحدة تطوير التعليم الالكتروني.

2-1 المهمَّات الرئيسة للمركز (جامعة السودان المفتوحة 2011م) :

1. إدارة النظام التعليمي الالكتروني بالجامعة.
2. جدولة جميع المناهج المعتمدة حالياً بالجامعة لوضعها على هيئة إلكترونية.
3. تدريب منسوبي المركز على تطوير برامج التعليم الالكتروني.
4. العمل على إنشاء وإدارة الفصول والمعامل الافتراضية.
5. المساهمة في تطوير المكتبة الإلكترونية بالجامعة، وذلك بزيادة مقتنياتها وجعلها متوفرة ومتاحة للجميع.
6. العمل مع الجهات المسئولة بالجامعة لتوفير البنية التحتية الخاصة بالتعليم الالكتروني.
7. إدارة وتطوير موقع الجامعة.
8. توفير التدريب والتنمية والدعم الفني لهيئة التدريس والمعنيين بالجامعة فيما يخص دمج التكنولوجيا في التعلم.
9. إجراء الدراسات والبحوث ومواكبة التطور العالمي في مجال التعليم الالكتروني.

3-1 نظام التعليم الإلكتروني المعتمد في الجامعة (جامعة السودان المفتوحة 2011م) :

اختير نظام موودل MOODLE كنظام أساسي للتعليم الالكتروني بالجامعة، وهو نظام مفتوح المصدر ومجاني، ويعد من أفضل نظم إدارة المحتوى التعليمي في العالم وأكثرها نمواً وتطوراً، وهو مدعوم ومستخدم في كبريات المؤسسات التعليمية والمنظمات التربوية في العالم.

4-1 إنجازات المركز (جامعة السودان المفتوحة 2011م) :

1. أكثر من 420 مقرراً من مقررات الجامعة لمستوى البكالوريوس.
2. أكثر من 100 مقرر من مقررات الجامعة للدراسات العليا.
3. تصميم موقع الجامعة الرئيسي وكل مواقع التعليم الالكتروني على شبكة الانترنت.
4. تطوير أكثر من 80 مقرراً من مقررات الجامعة المختلفة.
5. إنتاج العديد من المقررات الالكترونية بالتعاون مع بعض الجامعات الأخرى.
6. تنفيذ برنامج الاختبارات الالكترونية بالجامعة.
7. زوار الموقع الرئيس للتعليم الالكتروني بالجامعة في هذا العام فقط تجاوز الـ 440.944 زائراً.

2ـ نظام موودل (MOODLE) : (جميل اطميزي 2012م)

هو نظام إدارة تعلم مفتوح المصدر صُمِّم على أسس تعليمية ليساعد المدربين على توفير

بيئة تعليمية الكترونية، ومن الممكن استخدامه بشكل شخصي على مستوى الفرد، كما يمكن أن يخدم جامعة تضم 40000 ألف متدرب.كما أن موقع النظام يضم 75000 من المستخدمين المسجلين، مسجل ويتكلمون 70 لغة مختلفة من 138 دولة.**أما من ناحية تقنية فإن النظام صمم باستخدام لغة (PHP) ولقواعد البيانات (MySQL) ، ويعدُّ**:

- أحد أنظمة إدارة المقررات CMS– Course Management System.
- أحد أنظمة إدارة التعليم LMS – Learning Management System.
- أحد أنظمة إدارة محتويات التعليم LCMS–

Learning Content Management System

- وأحد منصات التعليم الإلكتروني (E_Learning Platform) .

وهو ليس وعاء للمقررات فقط، بل أيضاً يمكن تطوير أنشطة تعليمية عليه، ويستعمل من قبل جامعات، كليات أهلية، مدارس ثانوية، أعمال تجارية، بل ويمكن للمحاضر أن يستعمله لإضافة تقنية الويب إلى المقررات.وهو حالياً مستعمل من قبل آلاف المؤسسات التربوية حول العالم لإيجاد مقررات أون لاين على الإنترنت وإنتاجها، ولدعم المقررات التقليدية (التعليم وجهاً لوجه) ، وكذلك لإيجاد مواقع ويب على الإنترنت.

وهو برنامج مفتوح المصدر (Open Source software) ، ويوزع تحت رخصة GNU العامة، ويعني ذلك بأنه يحق للكل بأن يقوموا بتحميله وتركيبه واستعماله وتعديله وتوزيعه مجاناً.

ويعمل النظام دون تعديل على أنظمة التشغيل كلها، ويمكن أن يدعم العديد من أنواع قاعدة البيانات وبخاصة، (MySQL) ، كما أن البرنامج يحوي ميزة مهمة لدى كثير من المستخدمين وهي خدمته لكثير من اللغات العالمية، ومنها اللغة العربية.

ولاستخدام نظام موودل، نحتاج إلى أن نحمله على خادم server حتى يتمكن المستخدمون من الاتصال به عن طريق الانترنت.وبعد ذلك يكون لكل راغب في التعامل مع النظام حساب دخول للنظام عبارة عن اسم مستخدم وكلمة مرور.وفي موودل كثير من الخصائص الإضافية التي يمكن أن تساعد المعلمين في إنشاء مقررات الكترونية مطروحة بالكامل على الإنترنت تتسم بالفعالية، سواء كان هذا المقرر معد مسبقاً أو يعد تدريجياً ويضاف إليه في أثناء التدريس.وهذه الخواص تجعل موودل صالحاً للاستخدام بطرق متنوعة وفق حاجات المؤسسة التعليمية وإمكاناتها، ابتداء من الإدارة البسيطة للفصل إلى المقررات المقدمة كلياً بالانترنت أو كمقرر مساند للمقرر التقليدي داخل الفصل يقدم محتوى الكترونياً، واستخدامات توسع من نطاق التعليم الذي يتم داخل الفصل.ويمكن دمج مكتبات الوسائط وروابط خارجية– وغيرها من البرامج التي يمكن

شراؤها– في مقررات موودل الالكترونية.ويقدم موودل استخدامات مثل: حفظ النسخ الاحتياطية والتبادل واستعادة (استرجاع) مكونات المقرر.(جميل اطميزي 2012م).

والصفحة الرئيسة لموودل عبارة عن بوابة معلومات ذات قوالب، مثل التقويم والدخول والأخبار، يمكن تشكيلها وتغييرها حسب الرغبة.ويتكون الجزء الأوسط من الشاشة من قائمة من المقررات التي أنشئت وهي موجودة ومرتبة في مجموعات (فئات) .وأي مقرر منها عبارة عن مجموعة منظمة من الدروس والمصادر والأنشطة.حيث يقوم مؤلف المقرر بتجميع المادة العلمية وأشكالها.ويمكن تنظيم المقرر على أساس زمني يحدد تاريخ الانضمام إلى المقرر وتواريخ محددة للواجبات، ويمكن تنظميه على هيئة مجموعة من الموضوعات التي يمكن تغطيتها دون ترتيب معين وفقاً لسرعة الطالب.ويحتوي النظام على وظائف إدارية مثل تسجيل الطلاب والواجبات ووضع الدرجات والاختبارات.(جميل اطميزي 2012م).

1ـ2 مميـــزاته:

أهم الأشياء التي تميز بها نظام موودل هي التغذية الراجعة، ومتابعة الطلاب، وكذلك الأنشطة الفصلية.وهذا يؤكد المستوى الرفيع الذي وصل له نظام (MOODLE) ، وكمية الأدوات المساعدة والسهولة في الاستخدام والتحديث السريع المتوافق مع تطورات التعلم الإلكتروني من قبل المطورين لهذا النظام بالرغم من أنه مفتوح المصدر.(جميل اطميزي 2012م).

2ـ2 ما إمكانات موودل؟:

موودل بيئة تعليمية للتواصل عن بعد عبر الانترنت، وهو يوفر المحتوى التعليمي للمساقات المختلفة، ويتيح إمكانية التواصل عبر الدردشة والمنتديات بين المتدربين والمنتسبين للمساق الواحد، كما أنه يوفر العديد من الإمكانات:

1. بيئة خاصة للمنظومة التعليمية.
2. مواد تعليمية مكتوبة ومقروءة ومرئية لكافة المتدربين.
3. منتديات حوار وغرف دردشة.
4. إمكانية تصميم امتحانات الكترونية وواجبات واستقصاءات وتصويت للمتدربين.
5. رصد علامات المتدربين إلكترونياً في دفتر العلامات الخاص بموودل.
6. عرض المحتوى التعليمي الكترونياً وتصميمه وفق العديد من معايير النشر الالكتروني.
7. التكامل بين موودل والبرمجيات الأخرى.
8. أمان وحفظ المعلومات، وذلك بتغليفها بمستويات أمان مختلفة وللوصول إليها لابد من كلمة مرور (http:// balance– group.net) .

ومن ناحية التصميم التعليمي فإن النظام يوفر عدة إمكانات تتمثل أهمها في:

1. تحميل المصادر التعليمية إلى الموقع، ووضع روابط لمراكز الأبحاث، والمواقع ذات الصلة بمحتوى المقرر.
2. يتيح النظام خيارات عدة لأستاذ المقرر لاختيار الطريقة المناسبة في تدريس المقرر.
3. تعيين المدرسين، والمدرسين المساعدين للمقرر.
4. يمكن وضع مقررات دراسية متعددة في النظام.
5. وضع المراجع العلمية لكل مقرر دراسي.(محمد محمد عبد الهادي 2012م).

أما من ناحية التحكم وإدارة النظام فإن أهم الإمكانيات التي يوفرها النظام فهي:

1. يوجد بالنظام خاصية التحكم في الأمور المتعلقة بالعملية التعليمية كلها، باستخدام خاصية الأجندة للمقرر.
2. لا يمكن الدخول للنظام إلا بالحصول على اسم مستخدم وكلمة مرور خاصة بالنظام، أو الدخول بصفة ضيف فقط.
3. يوجد في النظام عشرة قوالب جاهزة تمكن المستخدم من تغيير الواجهة حسب الرغبة.
4. توجد صلاحيات واسعة للمشرف على النظام، ولأستاذ المقرر. (عبد المجيد الدائل 2012م)

الشكل (1)

الصفحة الرئيسة لموقع نظام موودل

3ـ ثغرات الإدخال في قواعد البيانات SQL Injection:

تعد ثغرات الإدخال في قواعد البيانات من أكثر الأخطار الأمنية المهددة للمواقع الإلكترونية والشركات والمؤسسات الكبرى التي تستخدم قواعد البيانات لتخزين معلوماتها القيمة؛ ففي عام 2007م، أظهرت دراسة قامت بها إحدى شركات أمن المعلومات أن من بين كل خمسة مواقع إلكترونية هناك موقع إلكتروني واحد معرض لخطر «SQL injection» (jeremiah Grossman 2007). وفي عام 2008م أظهرت دراسة أخرى قامت بها إحدى الشركات المعنية بأمن المعلومات أن تَعرُّضَ المواقع الإلكترونية للـ «SQL injection» زادت عن عام2007 بنسبة 134 بالمائة، وأنه في نهاية عام 2008م أصبح الهجوم على المواقع غير المحصنة مائة ألف هجوم في اليوم الواحد (Lavon Peters 2009). وتعد هذه النسبة نسبة كبيرة ومقلقة، وعواقبها خطيرة للغاية حيث إنها تسبب خسائر كبيرة للشركات والأفراد والمؤسسات؛ حيث إن المهاجم يستطيع بمساعدة الإدخال قواعد البيانات اختراق قاعدة البيانات الخاصة بالموقع الإلكتروني فيقوم وبكل بساطة بالحذف، والإضافة، والسرقة والتعديل على المعلومات المخزنة في قاعدة البيانات تلك.

3ـ1 أصناف ثغرات الإدخال في قواعد البيانات (net_code 2010) :

يمكن تصنيف هذه الثغرة إلى نوعين حسب صعوبة الحصول على معلومات الجداول في قاعدة البيانات أو سهولتها، والنوعان هما:

أ. الطريقة العادية:

وهي أسهل طريقة للإدخال في قواعد البيانات، وفيها يكون الخطأ في النظام المعني هو أحد حالتين:

♦ الحالة الأولى: عدم استخدام دوال تصفية الأحرف والعلامات الخاصة في HTML، وبالتالي يمكن إدخالها بسهولة في الشفرة البرمجية للنظام، مما يؤدي إلى التلاعب بقاعدة بيانات النظام من قبل المخترق.ومثال ذلك:

statement = «SELECT×FROM users WHERE name ="" + ";'" + userName

هذه الشفرة البرمجية تقوم بسحب بيانات مستخدم محدد من قاعدة البيانات.وحال قام المخترق بوضع قيمة للحقل username هي عبارة عن شفرة برمجية تمثل استفساراً أو غيره، فإن هذه الشفرة ستقوم بتنفيذ الكثير؛ ومثال على ذلك إذا قام المخترق بتبديل قيمة حقل اسم المستخدم بأي من الآتي:

′or ′1′= ′1

′or ′1′=′1′––

′or ′1′=′1′ ([

′or ′1′=′1′ / ×

وبالتالي تصبح الشفرة البرمجية للاستعلام:

SELECT×FROM users WHERE name =′′′OR′1′=′1′;

وفي هذا الاستعلام تكون النتيجة صحيحة في الأحوال كلّها، وبالتالي يتمكن المخترق من تنفيذ الشفرة التي يريدها؛ على سبيل المثال يقوم بإضافة الشفرة الآتية:

DROPTABLE users; SELECT×FROM userinfo WHERE ‘t’=’t’;

وبالتالي تصبح الشفرة البرمجية النهائية:

SELECT×FROM users WHERE name =′a′; DROPTABLE users; SELECT×FROM userinfo WHERE ′t′=′t′;

♦ الحالة الثانية: عدم تقييد المتغير البرمجي بنوع محدد، وتحدث هذه الحالة عندما يقوم المبرمج بتعريف حقل معين في الشفرة البرمجية، ثم لا يقوم بتقييد محتوى هذا الحقل بنوع محدد من أنواع البيانات؛ أو لم يستخدم دوال تقييد قيمة الحقل بنوع معين من البيانات، وبالتالي يمكن وضع أي محتوى داخل هذا الحقل سواء كان قيمة رقمية أم قيمة حرفية، ومثال على ذلك:

statement:= «SELECT×FROM userinfo WHERE id =” + a_ variable + “;”

يتضح من الشفرة البرمجية السابقة أن المبرمج يقصد وضع قيمة رقمية في المتغير id، ولكنه لم يقم بتقييد هذا الحقل بنوع المتغير المطلوب، وبالتالي يمكن للمخترق أن يقوم بإضافة قيمة للمتغير هي سلسلة حرفية كالآتي:

1;DROP TABLE users

فتصبح الشفرة البرمجية النهاية كالآتي:

SELECT×FROM userinfo WHERE id=1; DROPTABLE users;

ب. الحقن الأعمى Blind sql injection (net_code 2010) :

وهنا تكون مهمة المخترق ازدادت صعوبة، حيث إن نتيجة الإدخال في قاعدة البيانات بالطريقة العادية تم تنفيذها، لكن لم تظهر نتيجة التنفيذ على الشاشة، وبالتالي لم يتأكد المخترق من وجود الثغرة، وبالتالي يقوم بالاعتماد على التخمين والتجارب حتى يتوصل لنتائج مرضية.

وللوصول لهذه النتائج المرضية، فإن المخترق يقوم باستخدام واحدة من ثلاث حيل هي:

- الاستجابة المشروطة Conditional responses:

هذه الحيلة تعتمد على التلاعب بالمتغيرات لتغيير الاستجابة الخاصة بالsql، فلمعرفة هل البرنامج مصاب بثغرةsql injection أم لا؟ يقوم المخترق بكتابة الآتي:

http:// site.com/ news.php?id=2 and 1=2

فإذا كانت الشفرة البرمجية مصابة بالثغرة ستتغير الاستجابة، وستظهر الصفحة بدون أي بيانات، وللتأكد من هذا يقوم بتغيير الشرط إلى 1=1، وإذا ظهرت بيانات هنا يتأكد أن الشفرة مصابة بsql injection.

- الأخطاء الشرطية Conditional errors:

و هذه الحيلة تعتمد على توليد خطأ عندما يكون الشرط صحيحاً مثلاً:

SELECT 1/ 0 FROM users WHERE username='netcode';

فإذا كان هناك بالفعل مستخدم بالاسم netcode فسيتم توليد الخطأ Division By Zero كنتيجة ل 1/ 0.

- تأخير الوقت Time delays:

وهذه الحيلة تعتمد على تأجيل الرد الخاص بقاعدة البيانات إذا كان الشرط صحيحاً، ومثال ذلك استخدام ألsql injection في عمل brute force لكلمة المرور.يستخدم المخترق هنا الدالة benchmark ولتنفيذ الدالة encode عدد كبير من المرات لتأخير تنفيذ ألsql إذا كان الشرط صحيحاً.

UNION SELECT IF (SUBSTRING (user_password،1،1) = CHAR (50) ،BENCHMARK (5000000،ENCODE ('MSG'،'by 5 seconds')) ،null) FROM users WHERE id = 1;

هنا استخدم الجملة if كشرط وقام بمقارنة أول حرف من كلمة المرور بأنه يساوي (char 50) أي الرقم 2، إذا حُملت الصفحة ببطء، إذاً الشرط صحيح، وأول حرف من كلمة المرور هو 2، وهكذا.

2_3 مقاومة الاختراق عبر ثغرات الإدخال في قواعد البيانات) وئام عبد المحسن 2014م) :

ولما لمعلومات الشركات والمؤسسات سواءً التجارية منها أو الحكومية من أهمية بالنسبة لها، فقد حاولت الشركات الأمنية مقاومة هذا النوع من الثغرات بابتكار طرق عديدة تساعد بقدر الإمكان من التقليل من هذا الاختراق الأمني الشديد الخطورة، والذي يهدد أمن معلومات هذه

الشركات والمؤسسات وسلامتها؛ فلذلك شرعت الشركات المعنية بأمن المعلومات بإيجاد طرق تساعد على الوقاية من هذه الثغرة الأمنية التي يتزايد انتشارها بشكل كبير يوماً بعد يوم.

من هذه الطرق نذكر الأتي:

3-2-1 التحقق من صحة مدخلات المستخدم:

فإن أردنا السماح للمستخدم بإدخال جمل عن طريق مربع النص، فيجب علينا مراجعة جميع ما يدخله بدقة عن طريق:

- مراجعة طول الجملة ونوع المتغير:

فإذا كان طول الجملة التي أدخلها يزيد عن الطول المحدد داخل مربع النص، فإننا نتجاهل ما أدخله المستخدم، ولا نسمح لهذه الجملة باسترجاع أية نتيجة من قاعدة البيانات.أما بالنسبة لنوع المتغير، فإننا إذا كنا نتوقع أن يُدخل المستخدم حروفاً فإننا نراجع ما أدخله هل هو أحرف أم أرقام فإذا كانت أحرف نقبلها أما إذا كانت أرقام أو غيرها فإننا نتجاهلها ولا نسمح بها.

- مراجعة ما تتضمنه الجملة.

فإذا كانت تتضمن رموزاً معينة مثل: الفاصلة المنقوطة (;) ، الفاصلة (،) علامة التنصيص الفردية (') والرمز المستخدم للتعليق (--) ، أو البيانات الثنائية (0،1) ، فإننا لا نسمح بها مطلقاً؛ لأنها قد تكون إشارة لمحاولة الاختراق.

- استخدام العمليات المحفوظة في قاعدة البيانات:

ونقصد بذلك العمليات التي تكون موجودة مسبقاً في قاعدة البيانات، وتستخدم للتحقق من صحة المعلومات المدخلة.

- تدقيق وتنقيح الكلمات التي أدخلها المستخدم:

فإذا كانت تتضمن كلمات معروفة ومستخدمة في قاعدة البيانات، فإننا لا نسمح بها مثل: «UNION» ، « CREATE» ، «SELECT»،«DELET»

3-2-2 استخدام علامتي التنصيص الثنائية (″) :

ونقصد هنا باستبدال علامة التنصيص الفردية التي يدخلها المستخدم (') بعلامتي التنصيص الثنائية (″) ; لأن هذه العملية لها دور كبير بإفشال محاولة الاختراق باستخدام الإدخال في قواعد البيانات.

3-2-3 تحديد صلاحية المستخدم:

ونعني تجنب الدخول لقاعدة البيانات بالحساب الذي يعطي المستخدم كامل الصلاحيات للقيام بأي شي، ذلك أن المهاجم- وإن نجح في الدخول إلى قاعدة البيانات- فإنه لا يملك

الصلاحيات للقيام بأي شيء وهذا يساعد في تجنب إمكانية العبث بقاعدة البيانات.

3-2-4 استخدام رمز المساواة "=" بدلا من كلمة «Like».

حيث إن كلمة «like»عادة ما تستخدم في جمل الإدخال في قواعد البيانات، ويفضل استخدامها في محركات البحث فقط.

3-2-5 كتابة أسماء الأعمدة المستخدمة في الجداول:

يجب الانتباه لعدم كتابة الأسماء الواضحة والمتعارف عليها كتسمية العمود بالاسم، كلمة المرور، أرقام بطاقات الائتمان وغيرها، بل يجب تسميتها بأسماء يصعب على المهاجم التنبؤ بها.

3-2-6 الابتعاد عن وضع أي معلومات تخص قاعدة البيانات في رسائل الخطأ:

نقصد بذلك رسائل الخطأ التي تظهر للمستخدم; فهذه المعلومات قد تفيد المهاجم في اختراقه لقاعدة البيانات.

مثال على ذلك: عدد الأعمدة في قاعدة البيانات، أو حجم قاعدة البيانات، أو أسماء بعض الأعمدة والجداول.

3-2-7 الاهتمام بالحصول على آخر الإصدارات من البرمجيات التي تقوم بعمل مراجعة للأكواد البرمجية المستخدمة في مراجعة مدخلات المستخدم:

فهذه البرمجيات تقوم بمراجعة صحة الأكواد البرمجية ودقتها التي أُنشئت وعُملت مسبقاً في قاعدة البيانات كي تقوم بمراجعة مدخلات المستخدم، فكلما كانت هذه الأكواد البرمجية صحيحة ودقيقة، كانت مراجعتها للجمل التي يدخلها المستخدم أيضاً دقيقة للغاية، فبالتالي تمنع الجمل التي قد تكون خطرة على قاعدة البيانات

3ـ3 نموذج للثغرة:

الثغرة:

SELECT × FROM users WHERE name = ′ + userName + ′;

هذه الشفرة البرمجية تمثل استعلاماً عن اسم المستخدم في نظام ما، وهي تستدعي جميع السجلات الخاصة باسم المستخدم (userName) من جدول المستخدمين (users) .لكن إذا تم تغيير المتغير (userName) بشكل معين وباستخدام الرمز الخاص (') من قبل المستخدم المخترق، فمن الممكن لهذه الجملة أن تفعل أكثر مما هو منوي عليه.مثلاً يمكن استبدال قيمة المتغير (userName) بالجملة الآتية:

′a′ or 4>3

فتصبح الجملة كالآتي:

SELECT×FROM users WHERE name = ′a′ or 4>3;

وبما أن نتيجة الاستعلام ستكون صحيحة في كل الأحوال، فإن المخترق سيتمكن بكل سهولة من الحصول على ما يريد.ويمكن أيضاً استخدام هذه الطريقة لحذف جدول ما من قاعدة البيانات، ومثال ذلك إذا قمنا بإضافة الجزء التالي للشفرة البرمجية السابقة:

DROP TABLE users; SELECT × FROM data WHERE name LIKE ′%′;

وبما أن معظم خوادم لغة الاستعلام البنيوية (SQL SERVERS) تسمح بتنفيذ جمل عدة في آن واحد، وبالتالي يمكن إدخال أية جملة صحيحة عن طريق استخدام هذه الطريقة بإضافة الجملة إلى نهاية المدخل.وبالتالي تكون الجملة كالآتي:

SELECT×FROM users WHERE name =′a′; DROPTABLE users; SELECT×FROMDATAWHERE name LIKE ′%′;

وهذا يؤدي فعلياً لحذف جدول المستخدمين بالكامل من قاعدة البيانات.

كيفية الترقيع:

1. عدم السماح بوضع الحروف في المتغيرات، وجعلها فقط أرقاماً باستخدام الأمر هذا كمثال:

$id= (int) $_GET[‘id’];

2. منع الحروف الخاصة التي تحدث خللاً لقاعدة البيانات، مثل (– ،“.“_+/ ×) .

وخلاصة القول هو أن الإدخال في قواعد البيانات طريقة متداولة بين القراصنة; نظراً لأنها طريقة سهلة التعلم وغير مكلفة، وأيضاً صعوبة التعرف عليها من قبل المبرمجين يجعلها طريقة منتشرة فيما بينهم.وبما أن قواعد البيانات طريقة مهمة لا غنى عنها في حفظ المعلومات القيمة للشركات، والمؤسسات والأفراد، فيجب علينا المحافظة عليها بشتى الطرق من عبث القراصنة الذين يحاولون جاهدين سرقة هذه المعلومات أو تدميرها.

لذا فعدم معرفتنا بخطورة هذه الثغرة الأمنية يجعلنا لا نستطيع حماية قواعد البيانات التي نستخدمها بشكل أساسي في حياتنا.فالوعي بأهمية هذه المشكلة وبمدى ضررها أمر مهم للغاية للحماية منها.وإنه لمن المهم استخدام أكثر من طريقة لحماية قاعدة البيانات ففي حال استطاع المهاجم اختراق إحدى هذه الطرق، فلا يتمكن من اختراق الطرق الأخرى.

على الرغم من أن نظام موودل يعد من الأنظمة القوية في حماية بياناتها، فإن الباحث قد

وجد ضالته فيه، وذلك بعد الفحص والتدقيق الشديدين؛ حيث قام الباحث باستخدام خبرته في الفحص اليدوي وعثر عبرها على ثغرة واحدة، ومن ثم قام باستخدام أداة Acunetix Web Vulnerability Scanner وعثر عبرها على الثغرة الثانية والتي هي من النوع الأعمى.

4ـ الدراسات السابقة:

1.4 دراسة ميرال تاج الدين محمد (2009م) :

عنوان الدراسة: تصميم إطار عمل أمني لنظم التعليم الالكتروني، دراسة حالة نظام موودل بجامعة السودان للعلوم والتكنولوجيا

أجريت هذه الدراسة بجامعة السودان للعلوم والتكنولوجيا لنيل درجة الماجستير.تركز هذه الدراسة على الأسس الأمنية في التعليم الالكتروني وأهمية ضمان سلامة المعلومات التي تتم حمايتها بشكل صحيح ضمن التعليم الالكتروني، وذلك من خلال معالجة المتطلبات الأمنية للعمليات الثلاث الرئيسة في أنظمة التعليم الالكتروني وهي عملية إنشاء المحتوى التعليمي، وعملية التدريس والتعلم والعملية التنظيمية.قدمت هذه الدراسة إطار عمل لأمن نظم التعليم الالكتروني لتحقيق متطلبات السرية؛ في هذه الدراسة اختير نظام إدارة العملية التعليمية موودل (MOODLE) كدراسة حالة لتطوير أنظمته الأمنية، وهي التحكم في الوصول (الأدوار والأذونـات) ، التوثيق والنسخ الاحتياطي والاسترجاع.وبعد ذلك قدمت الدراسة إطاراً للحلول الأمنية؛ وطُبِّق نظام إدارة العملية التعليمية في جامعة السودان للعلوم والتكنولوجيا.

اتفقت الدراستان على ضرورة التركيز على الأسس الأمنية في التعليم الالكتروني وأهمية ضمان سلامة المعلومات التي تحمي بشكل صحيح ضمن التعليم الالكتروني.كما اتفقتا على اختيار نظام إدارة العملية التعليمية موودل (MOODLE) كدراسة حالة لتطوير أنظمته الأمنية.

2.4 دراسة مصعب محمد الفاتح يوسف (2010م) :

عنوان الدراسة: SQL Injection طرق اكتشافها والحماية منها تطبيقاً على Php and My Sql

أجريت هذه الدراسة بجامعة النيلين لنيل درجة الماجستير.وهدفها التعرف إلى أهمية أمن البرمجيات والأضرار التي يمكن أن تحدث من جراء ضعف الأمن، والتعرف إلى المشكلات الأمنية في البرمجيات وأسباب نموها، والتعرف إلى نقاط ضعف البرمجيات، وكيف يتم التعامل معها؟ ، والتعرف على الترتيبات التي يجب أن تتبع في مراحل تطوير البرمجيات لسد نقاط الضعف

التي تمكن المهاجمين من شن هجومهم عليها، والتعرف إلى المشكلات الأمنية التي تتعرض لها الأنظمة التي تعتمد في عملها على الانترنت، ومساعدة المطورين والمبرمجين لصفحات الانترنت خاصة الذين يستخدمون لغة php and my sql في إنشاء صفحاتهم الالكترونية على اكتشاف نقاط الضعف في جملة sql (sql injection) تمهيداً لعملية حلها.وتوصل الباحث إلى إنشاء خوارزميتين تقومان باكتشاف نقاط الضعف في جمل sql، وتحديد موقعها داخل الشفرة الممثلة للصفحة التي كتبت بلغة php and my sql، فالخوارزمية الأولى تعنى بعملية استخراج القيم الممرَّرة إلى الصفحة وتحليلها، والتأكد من أنها جملة php، ثم تستخرج اسم القيمة الممرَّرة ونوعها، أما الخوارزمية الثانية فتعنى بعملية تتبع القيم الممررة المستخرجة من الخوارزمية الأولى والبحث عنها داخل أسطر الشفرة من أجل اتخاذ القرار المناسب.ثم قام الباحث بإنشاء برنامج يطبّق الخوارزميتين باستخدام لغة vb.net 2008 and sql server 2008، ومن ثم تنفيذ البرنامج على شفرة موقع www.ntcysudan.com والذي أعطى نتائج دقيقة للغاية.

الإطار العملي للبحث:

1ـ الشيفرات البرمجية للملفات المصابة وترقيعها:

فيما يأتي يستعرض الباحث الشفرات البرمجية التي تمثل الثغرات التي عثر عليها الباحث، ومن ثم يبين مكمن الثغرة وكيفية ترقيعها.

1. Blind SQL Injection

عثر الباحث على هذه الثغرة في الملف sys/ email.php، وفيما يأتي جزء من الشفرة البرمجية للملف والتي يمثل موضع الإصابة فيها بالجزء الذي تحته خط:

```
؟>php
if(isset($_GET['type']))﴿$type=$_GET['type'];﴾else﴿$type='NO';﴾
$link=mysql_connect('localhost','elearn_kh','﴿^J#LfGXbmQo') or
die (mysql_error ()) ;
$db=mysql_select_db ('elearn_main_kh؛)'
// if ($db) ﴿echo 'don connecy﴿:'
if ($type=="SEND﴾("
    if (isset ($_POST['forgetemail'﴾))['
      if (! empty ($_POST['forgetemail'﴾(([
```

```
$myemail=$_POST['forgetemail'];
$x/sql=mysql_query ("SELECT x FROM mdl_user
WHERE email='$myemail' LIMIT 1") or die (mysql_error () ;
if ($row=mysql_fetch_array ($sql))(
echo $row['username'];echo»</ br": "<
// echo $row['email'];echo"</ br/x: "<
$sql=mysql_query ("SELECT x FROM ous_students WHERE
user_email='$myemail' LIMIT 1") or die (mysql_error (() ;
if ($row=mysql_fetch_array ($sql))(
echo $row['user_name'];echo"</ br:"<
echo $row['user_email'];echo"</ br:"<
$to =$row['user_email';['
$subject = "إرسال كلمة المرور المفقودة";
$body.="معلومات دخولك المفقودة <br/ >";
$body.= $row['user_name'].' اسم المستخدم: <br/ >";
$body.= $row['pass'].' كلمة المرور: <br/ >";
```

تكمن الثغرة هنا في أن محتوى المتغير $myemail يُضاف إلى قاعدة البيانات قبل تنقيح المدخل فيه عبر دالة $POST.ولترقيع هذه الثغرة أضاف الباحث دالة التنقيح _mysql real_escape_string () لتنقيح المدخل للمتغير $myemail من كل الحروف الخاصة، والتي يمكن أن تشكل خطراً على النظام.

```
?>php
if(isset($_GET['type']))$type=$_GET['type';)else$type='NO';
$link=mysql_connect('localhost','elearn_kh','^J#LfGXbmQo')
or  die (mysql_error());
$db=mysql_select_db ( 'elearn_main_kh');
// if ($db) {echo 'don connecy';}
if ($type=="SEND") {
```

```
if (isset ($_POST['forgetemail'])){
    if (! empty ($_POST['forgetemail'])){
$myemail=mysql_real_escape_string ($_POST['forgetemail']);
/*$sql=mysql_query ("SELECT × FROM mdl_user
WHERE email='$myemail' LIMIT 1") or die (mysql_error());
if ($row=mysql_fetch_array ($sql)){
echo $row['username'];echo"</ br>";
// echo $row['email'];echo"</ br>";*/
$sql=mysql_query ("SELECT × FROM ous_students
WHERE user_email='$myemail' LIMIT 1") or die (mysql_
error());
if ($row=mysql_fetch_array ($sql)){
echo $row['user_name'];echo"</ br>";
echo $row['user_email'];echo"</ br>";
$to =$row['user_email'];
$subject = "إرسال كلمة المرور المفقودة";
$body.="معلومات دخولك المفقودة <br/ >";
$body.= $row['user_name'].» اسم المستخدم: <br/ >";
$body.= $row['pass'].» كلمة المرور: <br/ >";
```

2. SQL injection (AS) :

عثر الباحث على هذه الثغرة في الملف email.php، وفيما يأتي جزء من الشفرة البرمجية للملف، والتي يُمثَّل موضع الإصابة فيها بالجزء الذي تحته خط:

```
<?php
if(isset($_GET['type']))«$type=$_GET['type'];»else«$type='NO'»;
$link=mysql_connect('localhost','elearn_kh','«^J#LfGXbmQo') or
die (mysql_error :(()
```

```
$db=mysql_select_db (‘elearn_main_kh’) ;
// if ($db) {echo ‘don connecy’};
if ($type==”SEND”) {
    if (isset ($_POST[‘forgetemail’])) {
        if (! empty ($_POST[‘forgetemail’])) {
            $myemail=$_POST[‘forgetemail’] ;
/×$sql=mysql_query (“SELECT × FROM mdl_user WHERE email=’$myemail’ LIMIT 1”) or die (mysql_error : ())
    if ($row=mysql_fetch_array ($sql)) {
        echo $row[‘username’];echo”</ br:”<
        // echo $row[‘email’];echo”</ br:”<
$sql=mysql_query (“SELECT × FROM ous_students WHERE user_email=’$myemail’ LIMIT 1”) or die (mysql_error ; ())
    if ($row=mysql_fetch_array ($sql)) {
        echo $row[‘user_name’];echo”</ br:”<
        echo $row[‘user_email’];echo”</ br:”<
        $to =$row[‘user_email;[‘
                $subject = ”إرسال كلمة المرور المفقودة”;
                $body.=”معلومات دخولك المفقودة </br> <”;
                $body.= $row[‘user_name’].” اسم المستخدم: </br> <”;
                $body.= $row[‘pass’].” كلمة المرور: </br> <”;
```

تكمن الثغرة في الملف المذكور في السطر البرمجي رقم (1) ، وذلك بسبب استقبال المتغير $type لقيمة ما دون تنقيح هذه القيمة، والمتغير $type من المتغيرات التي تدخل إلى قاعدة البيانات مباشرة، وبالتالي يمثل خطورة كبيرة لأنه يمكن استغلاله من قبل القرصان لإدخال شفرة برمجية مضرة.ولترقيع هذه الثغرة استبدل الباحث السطر البرمجي المحتوي على الثغرة بسطر برمجي جديد مضاف إليه دالة التنقيح mysql_real_escape_string () .

```
؟>php
$type= (isset ($_GET['type'])) ?
Mysql_real_escape_string ($_GET['type']) :$type='NO';
$link=mysql_connect ('localhost','elearn_kh','^J#LfGXbmQo') or
die (mysql_error ()) ;
$db=mysql_select_db ('elearn_main_kh') ;
// if ($db) {echo 'don connecy';}
if ($type=="SEND") {
        if (isset ($_POST['forgetemail']) ) {
          if (! empty ($_POST['forgetemail']) ) {
$myemail=mysql_real_escape_string ($_POST['forgetemail']) ;
/ ×$sql=mysql_query ("SELECT × FROM mdl_user WHERE
email='$myemail' LIMIT 1") or die (mysql_error ()) ;
        if ($row=mysql_fetch_array ($sql) ) {
         echo $row['username'];echo"</ br>";
         // echo $row['email'];echo"</ br>";×/
$sql=mysql_query ("SELECT × FROM ous_students WHERE
user_email='$myemail' LIMIT 1") or die (mysql_error ()) ;
        if ($row=mysql_fetch_array ($sql) ) {
        echo $row['user_name'];echo"</ br>";
        echo $row['user_email'];echo"</ br>";
        $to =$row['user_email'];
                                $subject = "إرسال كلمة المرور المفقودة";
                                $body.="معلومات دخولك المفقودة <br/ >";
                        $body.= $row['user_name'].' اسم المستخدم: <br/ >";
                                $body.= $row['pass'].' كلمة المرور: <br/ >";
```

الخلاصة والنتائج والتوصيات:

1ـ الخلاصة:

بين الباحث خلال دراسته هذه ثغرات الإدخال في قواعد البيانات في نظام التعليم الإلكتروني مفتوح المصدر موودل؛ وفي سبيل ذلك تحدث عن نظام موودل بصورة تفصيلية، ثم بين ماهية ثغرات الإدخال في قواعد البيانات.واستخدم الباحث خلال دراسته أدوات الدراسة المتمثلة في لغة البرمجة PHP، ونظام Acunetix Web Vulnerability Scanner، وخبرته الشخصية للوصول للثغرات المعنية في النظام قيد الدراسة، وهو النسخة 1.9.5.استخدم الباحث في دراسته المنهج التطبيقي وتوصل من خلاله لوجود ثغرتين في الشفرة البرمجية للنظام، وقام بتحليلهما وكتابة الشفرة البرمجية للترقيع العلمي المناسب لهما.

2ـ النتائج:

خلص البحث للنتائج الآتية:

1. وجود ثغرتين من نوع ثغرات الإدخال في قواعد البيانات في الملف email.php.
2. عُدِّلت الشفرة البرمجية للملف المصاب لحمايتها من الاختراق.

3ـ التوصيات:

1. إجراء فحص دقيق للشفرة البرمجية لنظام موودل قبل استخدامه بصورة رسمية للتعليم الإلكتروني للمؤسسة.
2. إجراء فحص شامل للشفرة البرمجية لملفات نظام موودل في جامعة السودان المفتوحة مع كل تعديل أو تطوير للنظام.
3. تطبيق النتائج العملية للبحث على نظام موودل للمناطق التعليمية الأخرى – غير منطقة الخرطوم– في جامعة السودان المفتوحة.

المصادر والمراجع:

أولاً- الكتب:

1. جميل أحمد اطميزي، دليل استعمال المدرسين لنظام إدارة التعليم مفتوح المصدر MOODLE، (ديسمبر 2012م) ، متوفر على موقع التعليم الالكتروني لجامعة بوليتكنك فلسطين http:// elearning. ppu. edu.

ثانياً- منشورات حكومية:

1. دليل مركز التعليم الالكتروني، منشورات جامعة السودان المفتوحة، 2011م.
2. تقرير اللجنة الإدارية لجامعة السودان المفتوحة – 2013م

ثالثاً- مواقع الإنترنت:

1. نظام التعليم الإلكتروني موودل، بالنس قروب للاستشارات الإدارية وحلول الأعمال، (سبتمبر 2010م) ، متوفر على: http:// www. balance- group. net/

2. خصائص موودل، الموقع الخاص بالدكتور محمد محمد عبد الهادي، (سبتمبر 2012م) ، متوفر على: http:// kenanaonline. com

3. بيئة التعلم الإلكتروني، عبد المجيد الدائل وعبد الرحمن بن علي العثمان، (ديسمبر2012م) ، متوفر على: http:// faculty. ksu. edu. sa

4. ال sql injection بالتفصيل، موقع الفريق العربي للبرمجة، كتبت بواسطة net_code، (نوفمبر 2010م) ، تم أخذ المعلومات يوم 10/ أبريل 2014. متوفر على
http:// arabteam2000- forum. com

5. Jeremiah Grossman, WhiteHat Website Security statistic report, (October 2007).
www. whitehatsec. com/ home/ assets/ WPStatsreport_100107. pdf

6. Lavon Peters, SQL Injection Attacks on the Rise, (Feb 2009).
http:// sqlmag. com/ sql- server/ sql- injection- attacks- rise

7. الحماية من حقن قواعد البيانات، وئام عبد المحسن الراشد، مركز التميز لأمن المعلومات، (أبريل 2014م) ، أخذت المعلومات يوم الأربعاء 2/ 4/ 2014م الساعة 12:17. متوفر على https:// coeia. ksu. edu

8. موقع نظام موودل على الشبكة العنكبوتية www. moodle. org

9. www. acunetix. com (Dec 2013)