الثغرات الأمنية فى مواقع الويب :
دراسة تطبيقية على مواقع أقسام المكتبات والمعلومات المصرية

إعداد
د. عماد عبد الستار طه زيدان
قسم المكتبات والمعلومات
كلية الآداب – جامعة كفر الشيخ
Emadzedan74@yahoo.com

ملخص الدراسة :

تتناول الدراسة إجراء اختبار تطبيقات الويب لمواقع أقسام المكتبات والمعلومات المصرية باستخدام برنامج Vega لتحديد الثغرات الأمنية الموجودة في مواقع الأقسام ومن ثم العمل على إصلاحها وتتضح مشكلة الدراسة فى وجود العديد من الثغرات الأمنية فى مواقع الويب وذلك لنقص الخبرات والكفاءات المؤهلة لذلك وأيضا لعدم وجود نظام أمنى رادع لمحاولات الاختراق وتكتسب الدراسة أهميتها من أهمية أمن المعلومات والحماية من الاختراق وأن توقع الأخطار واستباقها بأخذ الاحتياطات اللازمة أفضل طريقة للحماية من الاختراق، وتهدف الدراسة إلى تحديد أنواع الثغرات الأمنية، وطرق إصلاحها، التعرف على البرامج والأدوات المستخدمة فى عملية اختبار اختراق تطبيقات الويب والحماية من الثغرات وأهم نتائج الدراسة أن ثغرات المعلومات ٥٤ % النسبة الأكبر من المخاطر الأمنية بينما تحتل الثغرات الأمنية عالية الخطورة ٣٠ % والمتوسطة الخطورة ٦% والمنخفضة الخطورة ١٠ % ، أن ٩٤ % من مواقع أقسام المكتبات والمعلومات المصرية يوجد بها ثغرات أمنية ، ٦ % فقط لا يوجد به أى ثغرة أمنية ، ويوجد ٢٤ نوع من الثغرات فى مواقع أقسام المكتبات والمعلومات المصرية.

تمهيد

مع تطور أدوات معالجة البيانات والمعلومات ووسائل تخزينها وتبادلها بطرق مختلفة، أصبح النظر إلى أمن تلك البيانات والمعلومات أمر مهم للغاية، حيث أسهمت التقنية بشكل ملحوظ في انتهاك حقوق وخصوصيات المستخدمين وتعرضها للخطر، ويثير التزايد المستمر في كمية البيانات والمعلومات المتبادلة إلكترونيا، كثير من التساؤلات عن كيفية حماية تلك المعلومات من الوصول إليها واستخدامها الغير المشروع، وكذلك حول الاثار التي تحدثها هذه الأخطار على مخرجات نظم المعلومات.

فمن السهل الإدراك بأخطار أمن المعلومات بعد وقوع الضرر، ولكن من الصعب توقع الأخطار واستباقها بأخذ الاحتياطات اللازمة، ثم التعامل معها وتخفيف آثارها بعد وقوعها ويتحقق ذلك من خلال إجراء اختبار الاختراق، فأمن المعلومات موضوع فى غاية الأهمية، حيث يمس بشكل مباشر حياة كل المتعاملين مع الوسائط الإلكترونية، وينعكس على مصالحهم وسبل أدائهم أعمالهم.

تعطى أقسام المكتبات والمعلومات تصميم مواقعها على الويب اهتماما بالغا، ولكن يجب عليهم الاهتمام ببناء مواقع مؤمنة ولا يتحقق ذلك إلا من خلال إجراء اختبار الاختراق للمواقع بشكل مستمر ودوري وذلك من أجل اكتشاف الثغرات ونقاط الضعف الأمنية في المواقع في وقت مبكرا والعمل على إصلاحها، وذلك لأنه في حال احتواء الموقع على أي ثغرة أمنية يؤدي إلى اختراقه أو إلى تراجعه في الترتيب، فدائما الوقاية خيرا من العلاج فاكتشاف الثغرات الأمنية وإصلاحها خيرا من معالجة الاثار المترتبة على الاختراق من تدمير للبيانات أو تغيرها.

مواقع أقسام المكتبات والمعلومات المصرية مثل أى موقع ويب تحتوى على العديد من البيانات على تحتاج إلى تأمين وحمايتها من الاختراق مثل جداول الامتحانات والمحاضرات حيث يمكن لمخترقي

تاريخ استلام البحث : ٢٧ مارس ٢٠١٨ ، تاريخ القبول : ٢٣ يونيو ٢٠١٨

المواقع التعديل فى البيانات كتغير موعد الاختبار عن الموعد الذى تم وضعة من قبل القسم ما يسبب تخلف الطلاب عن حضور الاختبارات، ويمكن استغلال السير الذاتية لأعضاء هيئة التدريس فى جمع البيانات الشخصية عنهم مثل عنوان البريد الإلكتروني ورقم التليفون والرقم القومي وغيرها من المعلومات الشخصية حيث تستخدم هذه المعلومات فى عمليات اختراق خصوصيتهم مثل اختراق البريد الإلكتروني ، وتستخدم فى عمليات التجسس عليهم وفى عمليات النصب والاحتيال عليهم و يمكن انتهاك حقوق الملكية الفكرية بسرقة أبحاث أعضاء هيئة التدريس، وأيضا يمكن التلاعب وتغيير فى نتائج الطلاب .

علاقة أخصائي المكتبات والمعلومات بإجراء اختبار الاختراق لتطبيقات الويب

فرضت التطورات الحديثة في مجال تكنولوجيا المعلومات والاتصالات تغيرات جذرية على مهنة المكتبات والمعلومات وأبرز هذه التغيرات تمثل في حوسبة أقسام المكتبات والمعلومات وخدماتها ورقمنة مقتنياتها من المعلومات واستخدام الانترنت كمصدر للمعلومات وأداة للاتصال وذلك بهدف التجاوب مع متطلبات العصر وتحقيق معدلات رضا تعكس وتدلل على نجاح هذه المؤسسات.[١] ولذلك حظيت الكفاءات التقنية لأخصائي المكتبات والمعلومات باهتمام واسع، ومن الكفايات التقنية ذات الأهمية القصوى في الوقت الحاضر هي القدرة على التعامل مع الحاسب الآلي والإنترنت بكفاءة عالية وتسخيرهما لخدمة المهنة، والذي يستلزم التعرف على لغات و برامج تصميم مواقع الويب ويوكد ذلك توصية دراسة بإدراج مقرر تطوير صفحات الويب ضمن برامج اقسام المكتبات[٢]، وتتناول دراسة أخرى التوجهات الجارية لتطوير برامج المكتبات والمعلومات حيث تعرض الدراسة للوظائف التى يمكن أن تتوافق ومؤهلات وقدرات خريجي قسم المكتبات والمعلومات فى محاولة للربط بين مخرجات التعليم ومتطلبات سوق العمل، ومن هذه الوظائف : مصمم مواقع وبوابات الويب Web Designer، ومدير موقع وبوابة إلكترونية Web Master، ومدير إدارة قواعد البيانات Database Administrator ، ومدير إدارة المحتوى Content Management Administrator [٣] وأيضا دراسة تأكد أن " مهارة أساسيات تصميم مواقع الويب وإدارتها" من المهارات المتخصصة الضرورية من أجل النجاح فى الوظائف المتاحة داخل قطاع المكتبات ومراكز المعلومات فى مصر[٤]

مما سبق يمكن يتضح أن " تصميم وبناء مواقع الويب وإدارتها " من ضمن وظائف و ومهارات وكفاءات أخصائي المكتبات والمعلومات ونظرا لما تتعرض له مواقع الويب من التهديدات الأمنية فيجب على أخصائي المكتبات والمعلومات أن يتعلم كيف يصمم ويبنى موقع ويب آمن ولا يتحقق ذلك إلا من خلال إجراء اختبار تطبيقات الويب لتحديد الثغرات الأمنية ومن ثم العمل على إصلاحها بصفته مصمم ومطور مواقع الويب حيث أن كل صانع هو الشخص الأفضل لإصلاح ما بصناعته من عيوب ومشاكل، فأخصائي المكتبات والمعلومات المصمم والمطور لمواقع الويب هو الشخص الأفضل لإصلاح ما بها من ثغرات أمنية ويتحقق ذلك من خلال إجراء اختبار الاختراق لها .

١الحراصى، نبهان بن حارث بن ناصر. مدى توافق الخطط الدراسية الحديثة بقسم دراسات المعلومات بجامعة السلطان قابوس مع المعايير الدولية للكفايات المهنية المواكبة لمتطلبات العمل فى مجتمع المعرفة. المؤتمر الرابع والعشرون للاتحاد العربى للمكتبات والمعلومات "مهنة ودراسات المكتبات والمعلومات : الواقع والتوجهات المستقبلية" المدينة المنورة، السعودية،٢٠١٣.

٢ جاسم محمد جرجيس، خالد عتيق سعيد عبد الله .المهارات والكفاءات المهنية الواجب توافرها فى خريجى أقسام المكتبات والمعلومات فى الجامعات العربية. المؤتمر الرابع والعشرون للاتحاد العربى للمكتبات والمعلومات "مهنة ودراسات المكتبات والمعلومات : الواقع والتوجهات المستقبلية" المدينة المنورة، السعودية،٢٠١٣.

٣ أحمد، أحمد فرج ، عبد الرحمن العاصم .التوجهات الجارية فى تطوير برامج أقسام المكتبات والمعلومات : دراسة تقيميه لتجربة قسم دراسات المعلومات بجامعة الإمام محمد بن سعود الإسلامية . المؤتمر الرابع والعشرون للاتحاد العربى للمكتبات والمعلومات "مهنة ودراسات المكتبات والمعلومات : الواقع والتوجهات المستقبلية" المدينة المنورة، السعودية،٢٠١٣.

٤ اسماعيل رجب عثمان .الفرص الوظيفية المتاحة أمام خريجى أقسام المكتبات والمعلومات بالقطاع الخاص فى مصر: دراسة استكشافية . المؤتمر الرابع والعشرون للاتحاد العربى للمكتبات والمعلومات "مهنة ودراسات المكتبات والمعلومات : الواقع والتوجهات المستقبلية" المدينة المنورة، السعودية،٢٠١٣

وتدور الدراسة حول العناصر الاتية :
أولاً : الإطار المنهجي للدراسة **ثانيا : الإطار النظري للدراسة**
ثالثا : خطوات تطبيق الدراسة **رابعاً : تحليل النتائج**

أولاً : الإطار المنهجي للدراسة

١/١ مصطلحات الدراسة

يعتبر مجال أمن المعلومات من أكثر المجالات حيوية في قطاع تكنولوجيا الاتصالات والمعلومات ولذلك يوجد العديد من التعريفات المرتبطة بهذا المجال ولكن تعرض الدراسة المصطلحات الأساسية لموضوع الدراسة كما يأتي :

١/١/١ أمن المعلومات Information Security

يعرف أمن المعلومات من أكثر من زاوية :

- **من زاوية أكاديمية** ، هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن انشطة الاعتداء عليها.
- **ومن زاوية تقنية** ، هو الوسائل والادوات والاجراءات اللازم توفيرها لضمان حماية المعلومات من الاخطار الداخلية والخارجية.
- **ومن زاوية قانونية** ، فان أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة انشطة الاعتداء عليها او استغلال نظمها في ارتكاب الجريمة ، وهو هدف وغرض تشريعات حماية المعلومات من الانشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها (جرائم الكمبيوتر والإنترنت) [١]

يعد تخصص أمن المعلومات تخصصاً حيوياً متجدداً، حيوياً لارتباطه بأكثر من تخصص بشكل فعال ومؤثر، ومتجدد لتحديث معلوماته على فترات متسارعة تحتاج متابعتها ومتابعه غيرها من التخصصات ذات العلاقة بشكل مستمر، ويضاف لذلك الارتباط الوثيق بين الأمن بشكل عام وباقي نواحي الحياة وتخصصاتها العلمية وما يتبعها من جوانب تقنية، وهناك جانبان مهمان يجب التركيز عليهما:

الأول : تخصص أمن المعلومات علم قائم بحد ذاته له تفرعاته المختلفة التي هي أيضا علوم قائمة بحد ذاتها منها:

أمن الشبكات - البرمجة الآمنة - صلاحيات التحكم **- الاختراق الأخلاقي واكتشاف الثغرات الأمنية** - أمن قواعد البيانات - أمن نظم التشغيل **- أمن تطبيقات الويب -** الهندسة العكسية - التشفير

الثاني : تخصص أمن المعلومات يشترك مع عدة تخصصات متنوعة منها أمن المعلومات الصحي ، الأمن الفيزيائي، البصمة الحيوية الإلكترونية، أمن التعاملات المالية، الاحتيال المالي الإلكتروني، الأدلة الجنائية الرقمية، الخ[٢].

١ الحرايرى، صبرى محمد .أزمة أمن المعلومات. متاح على https://www.researchgate.net/publication/272506778 . في ٢٠١٨/٢/١١
٢ تخصص أمن المعلومات. متاح على http://sacmmedia.org/info/majors/information-security.html

١/١/٢ تهديدات أمن المعلومات Information Security Threats

تعرف تهديدات أمن المعلومات على انها الأشخاص والمؤسسات والآليات والأحداث التي يمكن أن تحمل تأثيرا سلبيا ومضرا على مصادر المعلومات، ونلاحظ من التعريف أن مصادر كثيرة للتهديدات لا تعتبر إلكترونية وانما يمكن ان تكون أحد افراد المؤسسة ، أو عملية قام بها احدهم تعرض المعلومات ومصادرها للخطر، أو حتى حادث يمكن ان يسبب ذلك(مثل انقطاع التيار الكهربائي وضياع المعلومات.)

١/١/٣ مخاطر أمن المعلومات Information Security Risks

تعرف مخاطر أمن المعلومات بانها اثر غير مرغوب به أو ضار بسبب اختراق أو خلل بأمن المعلومات ناتج عن تهديد أمنى محتمل أى يقصد بالخطر أنه الأثر الذي يقع نتيجة حدوث فعل التهديد، أي أنه حدث ما يقع نتيجة تهديد ما [١].

١/١/٤ نقاط الضعف أو الثغرات الأمنية : Vulnerabilities

تعني جزء من النظام (عنصر أو نقطة أو موقع) يحتمل أن يتحقق بسببه التهديد ليصبح خطرا، أي يعبر من خلاله منفذ التهديد ليقع بعد ذلك الخطر، فمثلا يعد الأشخاص الذين يستخدمون النظام نقطة ضعف إذا لم يكن تدريبهم كافيا لاستخدام النظام وحمايته، وقد يكون الاتصال بالإنترنت نقطة ضعف - مثلا -إذا لم يكن مشفرا، وقد يكون الموقع المكاني للنظام نقطة ضعفا كأن يكون غير مجهز بوسائل الوقاية والحماية، وأيضا قد يكون الثغرات فى البرمجيات أو شبكة المعلومات أو تهيئة الشبكة أو قواعد البيانات [٢] ومن خلال هذه الثغرات أو نقاط الضعف يمكن للمهاجمين أن يخترقوا شبكات المعلومات ويحدثوا فيها الأضرار أو حتى الاستيلاء على ما يريدوا منها، وعلى مدير النظام ومديرو الشبكة أن يقوموا بعمليات فحص باستمرار لشبكة المعلومات لكي يقفوا على أي نقاط ضعف أو ثغرات يمكن أن تحدث ويعملوا على الفور على معالجها وسد هذه الثغرات تجنبا لاكتشافها من قبل بعض العابثين.[٣]

يمكن العثور على نقاط الضعف فى : طوبولوجية الشبكة ونقاط الضعف فى نظام التشغيل ،أو المنافذ المفتوحة والخدمات التى تعمل، أو التطبيق وأخطاء إعداد الخدمات، أو ضعف التطبيق والخدمات.

١/١/٥ بحوث الثغرات الأمنية Research Vulnerability

هي تقنيات يستخدمها مختبري الاختراق لاكتشاف الثغرات وضعف التصميم التى يمكن من خلالها الهجوم على التطبيقات وأنظمة التشغيل وتشمل الدراسة الديناميكية للمنتجات والتقنيات والتقييم المستمر لإمكانية الاختراق. هذه البحوث تساعد كل من مسئولي الأمن والمهاجمين ويمكن تصنيفها على أساس مستوى الخطورة(منخفضة، متوسطة، عالية) ، استغلال النطاق(محلى ، عن بعد)

وتستخدم هذه التقنية

- لتحديد وتصحيح نقاط ضعف الشبكة
- لحماية الشبكة من التعرض للهجوم من قبل الدخلاء
- للحصول على المعلومات التى تساعد على منع المشاكل الأمنية
- لجمع المعلومات حول الفيروسات
- للعثور على نقاط الضعف فى الشبكة وتنبيه مدير الشبكة قبل حصول الهجوم

١ أبو شنب، عماد أحمد محمد. إدارة وتحليل مخاطر أمن المعلومات. مؤتمر أمن المعلومات والحكومة الإلكترونية كوالالمبور- ماليزيا. ابريل ٢٠٠٩
٢ الذنيبات، معاذ يوسف. مخاطر أمن المعلومات المحتملة في تطبيقات التعاملات الإلكترونية و أثرها في كفاءة نظام المعلومات :دراسة حالة للمديرية العامة للجوازات في محافظة الطائف . مجلة البحوث الأمنية(السعودية). مج٢٤،ع٦٠، فبراير ٢٠١٥. ص ص ١٣-٦٩.
٣ حسنين، رجب عبد الحميد .أمن شبكات المعلومات الإلكترونية : المخاطر والحلول.Cybrarian Journal .ع٣٠، ديسمبر ٢٠١٢.ص ص ٧٤-١٠١

١/٢ مشكلة الدراسة

ظهرت العديد من المشكلات الأمنية الرقمية وذلك بعد سهولة وانتشار استخدام الانترنت تتلخص بتعطيل وتدمير مواقع الويب، والتسلل إلى الشبكات المحلية وسرقة المعلومات الحساسة مثل كلمات المرور وأرقام الحسابات البنكية والمعلومات الشخصية وغيرها من الأسرار، وترويج برامج التخريب والتجسس والقرصنة ، وسرقة المواقع وانتهاك حقوق الملكية الفكرية، كما أنها تؤمن تربة مناسبة لنمو شبكات التجسس العالمية التي تمارس نشاطات جمع المعلومات وانتهاك الخصوصية على مدار الساعة،

ويرجع أساس هذه المشكلات الأمنية إلى وجود الثغرات الأمنية الخطرة في تصميم وإعداد مواقع الويب وبالتالي تتضح مشكلة الدراسة مما يأتي :

- انتشار اعتماد أقسام المكتبات والمعلومات المصرية على تطبيقات الويب فى تقديم خدماتها مما جعلها أكثر عرضة للاختراقات الخارجية.
- نقص الخبرات والكفاءات المؤهلة فى مجال أمن المعلومات حيث ينصب الاهتمام على مجرد بناء موقع للقسم على الويب فقد دون أن يهتموا بموضوع أمن المعلومات والحماية من الاختراق.
- عدم وجود نظام أمنى رادع لمحاولات الاختراق وتؤكد الشواهد فى الآونة الأخيرة ارتفاع معدلات جرائم الاختراق والتعدي على البيانات ودخول الحواسيب دون وجه حق بهدف قراءة البيانات ونسخها أو الاستيلاء عليها أو إتلافها.

ونلخص مشكلة الدراسة فى النقص الشديد فى أخصائي المكتبات والمعلومات المؤهلين لتصميم وبناء مواقع الويب المؤمنة

١/٣ أهمية الدراسة

تنبع أهمية الدراسة من أهمية أمن المعلومات، حيث يمس بشكل مباشر حياة كل المتعاملين مع الوسائط الإلكترونية، وينعكس على مصالحهم وسبل أدائهم أعمالهم، فتكتسب الدراسة أهميتها من أهمية أمن المعلومات والحماية من الاختراق بما يوفر من موثوقية ومصداقية وسرية وسلامة وتكامل البيانات والمعلومات. وتتضح أهميتها مما يأتي :

- اختبار اختراق تطبيقات الويب لاكتشاف الثغرات الأمنية يساعد على توقع الأخطار واستباقها بأخذ الاحتياطات اللازمة، ثم التعامل معها وتخفيف آثارها بعد وقوعها.
- تكتسب الدراسة أهميتها أيضا بتحقيق مبدأ " الوقاية خيرا من العلاج" حيث اكتشاف الثغرات ونقاط الضعف الأمنية فى مواقع أقسام المكتبات والمعلومات المصرية والعمل على إصلاحها خيرا من محاولة معالجة الآثار التدميرية لعملية الاختراق.
- ضرورة إجراء اختبار الاختراق لمواقع أقسام المكتبات والمعلومات المصرية لأنه يشبه فى أهميته تأمين المنازل والمصالح الحكومية والخاصة.

وتتجلى أهمية الدراسة من الناحية العملية والناحية النظرية كما يلى:

- **الأهمية العملية** : تقدم الدراسة تطبيق لبرنامج اختبار الاختراق لمواقع أقسام المكتبات والمعلومات المصرية واكتشاف الثغرات ومعالجتها
- **الأهمية النظرية** : تقدم الدراسة قائمة بأخطر الثغرات ونقاط الضعف الأمنية الموجودة فى مواقع أقسام المكتبات والمعلومات المصرية ومن ثم العمل على معالجتها.

١/٤ أهداف الدراسة

تسعى الدراسة إلى تحقيق الأهداف الآتية :

- تحديد أنواع الثغرات الأمنية التى تهدد مواقع أقسام المكتبات والمعلومات المصرية على الانترنت
- تحديد الاجراءات الضرورية لمعالجة وإصلاح الثغرات الأمنية التى تتعرض لها مواقع أقسام المكتبات والمعلومات المصرية .
- تحديد أخطر أنواع الثغرات الأمنية التى تهدد مواقع الويب على مستوى العالم.
- التعرف على البرامج والأدوات المستخدمة فى عملية اختبار اختراق تطبيقات الويب والحماية من الثغرات.

١/٥ تساؤلات الدراسة

تسعى الدراسة إلى الإجابة عن الأسئلة الآتية :

١- ما هي أنواع الثغرات الأمنية التى تهدد أقسام المكتبات والمعلومات المصرية؟
٢- ما هي إجراءات إصلاح الثغرات الأمنية التى تهدد مواقع أقسام المكتبات والمعلومات المصرية؟
٣- ما هي البرامج والأدوات المستخدمة فى عملية اختبار اختراق تطبيقات الويب؟

١/٦ حدود الدراسة

تدور الدراسة حول تحليل الثغرات الأمنية لمواقع أقسام المكتبات والمعلومات المصرية على الويب باستخدام برنامج Vega لإجراء اختبار اختراق تطبيقات الويب ولتحديد أنواع الثغرات وعددها لكل موقع وتم تحليل ثغرات المواقع خلال المدة من ٢٠١٨/١/١ وحتى ٢٠١٨/٣/١٥

١/٧ مجتمع الدراسة

لكى تحقق الدراسة أهدافها، كان لابد اولا من حصر مجتمع الدراسة، والمجتمع هنا يتمثل في مواقع أقسام المكتبات والمعلومات المصرية على الأنترنت، ولتحقيق هذا الغرض قام الباحث بعمل مسح شامل على الإنترنت لمواقع أقسام المكتبات والمعلومات وتوصل البحث عن المواقع على الانترنت إلى وجود ثمانية عشر قسما لها مواقع على الانترنت(ملحق *) وتمت اختيار مواقع أقسام المكتبات والمعلومات المصرية على الانترنيت وفقا للشروط الآتية :

. البحث ضمن نطاق الموقع edu.eg
. الكلمات المفتاحية "أقسام +المكتبات +المعلومات"

١/٨ منهج الدراسة وأدواتها

اعتمد الباحث على المنهج الوصفي التحليلي لرصد وتجميع وتحليل الثغرات الأمنية لمواقع أقسام المكتبات والمعلومات المصرية على الانترنت؛ لكونه أفضل المناهج ملاءمة للدراسة معتمدا على مواقع أقسام المكتبات والمعلومات المصرية على الويب كمصدر رئيسي لجمع البيانات مستخدما برنامج vega لإجراء اختبار تطبيقات الويب لمواقع أقسام المكتبات والمعلومات المصرية.

* ملحق مواقع أقسام المكتبات والمعلومات المصرية

١/٩ الدراسات السابقة

تم مراجعة الانتاج الفكري فى كلا البيئتين العربية والأجنبية من خلال مجموعة من الأدوات وهى: دليل الانتاج الفكري فى مجال المكتبات والمعلومات ، وفهرس اتحاد مكتبات الجامعات المصرية، وبنك المعرفة المصري حيث تم البحث فى قواعد البيانات التالية ضمن بنك المعرفة المصري Arab world research complete database ، ودار المنظومة ، قاعدة إثراء المعرفية ، Library, Information Science & Technology Abstracts database ، Teacher Reference Center database وأيضا تم البحث في قاعدة بيانات الهادي للإنتاج الفكري في مجال المكتبات والمعلومات.

نتيجة البحث فى هذه القواعد لم يجد الباحث دراسة تناولت الثغرات الأمنية لمواقع الويب لأقسام المكتبات والمعلومات المصرية ، إلا أن بعضها قد تناول أبعاد من موضوع الأمن المعلوماتي فى المكتبات والمعلومات ، ويقسم الباحث الدراسات السابقة إلى المحاور الآتية:

١/٩/١ المحور الأول : أمن المكتبات ومراكز المعلومات
١/٩/٢ المحور الثاني : سياسة أمن المعلومات
١/٩/٣ المحور الثالث : الوعى بأمن المعلومات
١/٩/٤ المحور الرابع : أمن النظم الآلية وشبكات الحاسب فى المكتبات ومراكز المعلومات
١/٩/٥ المحور الخامس : الثغرات الأمنية لتطبيقات الويب

١/٩/١ المحور الأول : أمن المكتبات ومراكز المعلومات

- **أمن المعلومات فى المكتبات ومراكز المعلومات** [١] عرضت الدراسة لمكونات أمن المعلومات فى المكتبات وعناصر أمن المعلومات ، صور جرائم الحاسب الآلي والأنترنت
- **أمن المكتبات ونظم المعلومات دراسة حالة على مكتبة جامعة الملك عبدالعزيز بجدة** [٢]

تتناول الدراسة نواحي الأمن الرئيسية في المكتبات ومراكز المعلومات مع التركيز على أمن نظم المعلومات . فالمكتبات تتعرض عادة لمشاكل لها مساس بأمنها وسلامة محتوياتها مثل السرقة والتخريب والبعث والأخطار الطبيعية وفى الجانب التطبيقي قامت الدراسة بتناول نواحي الأمن في مكتبة جامعة الملك عبد العزيز بجدة من كافة الجوانب مركز على النظم الآلية مستخدمة منهج دراسة الحالة وذلك لكشف الإجراءات التى تتخذها المكتبة لمواجهة المخاطر الأمنية والسياسات التى تتبعها بهدف المحافظة على المكتبة ومقتنياتها. وقد بينت الدراسة غياب السياسات المكتوبة والخطط المعدة لمواجهة الطوارئ في المكتبة مجال الدراسة

- **أمن المجموعات الخاصة فى بعض المكتبات المصرية**[٣] تمثلت أهداف الدراسة في تقييم واقع عملية تأمين المجموعات الخاصة بعينة من المكتبات المصرية ، وتقديم المقترحات اللازمة لعلاج نقاط الضعف وتأكيد نقاط القوة بها، وقد اعتمدت الدراسة على المنهج الميداني وتم تصميم قائمة مراجعة من مئة و واحد عنصرا وتطبيقها على المكتبات موضوع الدراسة لتقييم وقياس أمن المجموعات الخاصة بها ، وكان من أبرز النتائج وجود نقاط عف مثل غياب سياسات أمن المجموعات الخاصة،

١ صالح، مشيرة أحمد. أمن المعلومات فى المكتبات ومراكز المعلومات. مكتبات نت. مج٨،ع٤، أكتوبر٢٠٠٧. ص ص ١٩-٢٨.
٢ السريحى، حسن بن عواد .أمن المكتبات ونظم المعلومات دراسة حالة على مكتبة جامعة الملك عبدالعزيز بجدة . المؤتمر الثاني عشر للاتحاد العربي للمكتبات والمعلومات . المكتبات العربية في مطلع الألفية الثالثة.مج٢.نوفمبر ٢٠٠١. الشارقة. ص ص٥٩١-٦٢٦
٣ الغلبان ، ثروت يوسف .أمن المجموعات الخاصة فى بعض المكتبات المصرية : دراسة ميدانية. المجلة الدولية لعلوم المكتبات والمعلومات. مج٢، ع٤،أكتوبر ٢٠١٥. ٧٤-١١٠

ونقص التسهيلات المادية والأنظمة الأمنية الآلية، ونقص عدد وقلة تدريب العاملين، كما أظهرت نقاط قوة مثل وعى العاملين بالموضوع، وجود أنظمة الحماية من الحريق، وقدمت الدراسة توصيات لتطوير مقومات أمن المجموعات الخاصة من سياسات وإجراءات ومقومات بشرية وتسهيلات مادية وأنظمة إلكترونية وغيرها.

١/٩/٢ المحور الثانى : سياسة أمن المعلومات

- **معيار المنظمة الدولية للتوحيد القياسى أيزو ٢٧٠٠٢ لسياسات أمن المعلومات [١]**

تهدف الدراسة إلى تحليل معايير آيزو ٢٧٠٠٢ لإدارة أنظمة أمن المعلومات والصادرة عن المنظمة الدولية للتوحيد القياسي) آيزو ,(والتعرف على السياسات والتوجيهات التي تتضمنها المعايير ومدى التزام أفضل الجامعات العربية بها.

- **سياسة أمن المعلومات في شبكة المكتبات بجامعة النيلين [٢]** يقدم البحث سياسة أمن المعلومات في ظل استخدامها لشبكات المعلومات وأهمية أمن المعلومات في المكتبات ويعرض أهم التهديدات التي تواجهها أنظمة المعلومات في المكتبات، والأخطار التي تجعل المكتبات أكثر عرضة للتهديدات، وتتناول تطبيق تلك السياسات على شبكة المكتبات بجامعة النيلين، ويخلص البحث إلى ضرورة وجود وثيقة لسياسة أمن المعلومات في المكتبات، متبوعة بمجموعة من الإجراءات والتعليمات، والتي بدونها يصبح الالتزام بعدم ارتكاب الجرائم الحاسوبية أخلاقيات قد لا يلتزم الكثيرون بها أو يختلف حولها باختلاف التربية والثقافة .كما يعرض هذا البحث وثيقة أمن المعلومات لإحدى المكتبات ومجموعة من التوصيات للتعرف على مدى كفاية تلك السياسات المتبعة لتحقيق أمن المعلومات.

١/٩/٣ المحور الثالث : الوعى بأمن المعلومات

- **أمن المعلومات وتطبيقاته فى أقسام علم المعلومات والمكتبات [٣]** يتعرف هذا البحث على **أمية أمن المعلومات** لدى طلبة أقسام المعلومات والمكتبات في الجامعات العراقية ومدى علاقتها بالمقررات الدراسية ، واعتمدت الدراسة المنهج المسحي لجمع البيانات وتحليلها، واستخدمت الاستبانة لجمع البيانات من الطلبة عينة البحث. وخرج البحث بمجموعة من النتائج أبرزها وجود وعى لدى الطلبة بأهمية حماية المعلومات وما المعلومات الواجب حاميتها، وافتقار مادة الحوسبة وفروعها الموضوعية المختلفة والتي تدرس في أقسام المعلومات والمكتبات إلى التغطية الجيدة لموضوع أمن المعلومات وتطبيقاته.
- **الوعي بأمن المعلومات لدى أعضاء هيئة التدريس في الجامعات [٤]** هدف الباحث إلي استعراض المفهومات العامة لأمن المعلومات، و معرفة مدي وعي أعضاء هيئة التدريس في الجامعات(دراسة حالة جامعة المجمعة) بمتطلبات تحقيق أمن معلوماتهم، و سبلهم لمواجهة عمليات الاختراق و التخريب.

---

١ العربى، أحمد عبادة . معيار المنظمة الدولية للتوحيد القياسى أيزو ٢٧٠٠٢ لسياسات أمن المعلومات : دراسة وصفية تحليلية لمواقع الجامعات العربية.مجلة جامعة طيبة للآداب والعلوم الإنسانية . س ٤، ع٧. ٢٠١٥ .ص ص٦٦١-٧٣٨

٢ حمودة ، بهاء الدين حمودة حسن .سياسة أمن المعلومات في شبكة المكتبات بجامعة النيلين : دراسة حالة . المجلة العربية الدولية للمعلوماتية. مج٣، ع٥، ٢٠١٤. ص ص ٥٥-٦٢

٣ العكيلى، هدى سليمان ، بشرى فاضل البياتى . أمن المعلومات وتطبيقاته فى أقسام علم المعلومات والمكتبات : دراسة مسحية. المجلة الأردنية للمكتبات والمعلومات.مج ٥٢،ع١ ،٢٠١٧.ص ص٣٧-٨٢

٤ العمران، حمد بن ابراهيم .الوعي بأمن المعلومات لدى أعضاء هيئة التدريس في الجامعات : دراسة حالة لجامعة المجمعة. اعلم –السعودية.ع٨، ابريل ٢٠١١.ص ص ١٠ -٤٤

١/٩/٤ المحور الرابع: أمن النظم الآلية وشبكات الحاسب فى المكتبات ومراكز المعلومات

- **تشفير المصادر الالكترونية باستخدام معيار مارك ٢١**[١] يهدف البحث إلى التعرف على الطريقة المثلى لتنظيم مصادر المعلومات الالكترونية في المكتبات ومراكز المعلومات باستخدام معيار مارك ٢١. واتبعت الدراسة المنهج الوثائقي القائم على الانتاج الفكري المنشور حول الموضوع. وقد توصل البحث إلى ضرورة تنظم هذه المصادر وفق قواعد الفهرسة الأنجلوا أمريكية وباستخدام شكل مارك ٢١ إذ يتعين تشفير المصادر الالكترونية باستخدام الفاتح ٠٦ الخاص بنوع التسجيلة والحقول ثابتة الطول ٠٠٦ الخاصة بنوع المصدر ونوع الملف و ٠٠٧ الخاص بالوصف المادي للمصدر والحقل ٨٥٦ لتوفير معلومات الموقع الإلكتروني ومعلومات تتعلق بالوصول إلى المصدر ضمن المجموعة

- **أمن شبكات المعلومات الإلكترونية : المخاطر والحلول** [٢] نحاول هذه الدراسة إيضاح أهمية أمن شبكات المعلومات وما هي المخاطر التي تهددها وكيفية مناهضة هذه المخاطر والحماية منها.

- **إدارة أمن نظم المكتبات الآلية المتكاملة بطريقة أكثر فعالية :دراسة تطبيقية على المكتبات المصرية**[٣] تهدف الدراسة إلى التعرف على المخاطر التى تواجه نظم المكتبات الآلية المتكاملة المستخدمة فى المكتبات المصرية الحكومية، وتحديد أهم الأسباب التى تؤدى إلى حدوث تلك المخاصر والإجراءات التى تحول دون وقوع تلك المخاطر ، مستخدمة استبانة تحتوى على مجموعة المخاطر التى تهدد نظم المكتبات الآلية المتكاملة ، وأسبابها، وإجراءات الحماية المتبعة للتصدي لتلك التهديدات التى تتعرض لها، وتكونت عينة الدراسة من مديري المكتبات وأخصائي المكتبات ومشرفي النظم والشبكات، والمبرمجين، ومسؤولي الدعم الفني.

- **أساليب حماية وأمن المعلومات في النظم الآلية والشبكات في المكتبات ومراكز المعلومات بالقاهرة الكبرى** [٤] توصلت الدراسة إلى مجموعة من النتائج أهمها لا تهتم المكتبات ومراكز المعلومات موضوع الدراسة باستخدام أساليب متعددة لحماية أمن المعلومات وتفتقد بعض الأساليب الأمنية الضرورية ، مثل : البطاقات الذكية ، وتقنية التحقق بموجات الراديو الترددية ،الدوائر التلفزيونية المغلقة للمراقبة وذلك على الرغم من أهميتها ولم يتم تحديث برامج الحماية ضد الفيروسات بشكل منتظم لشبكة المكتبة وجميع محطات العمل.

- **حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى** [٥] هدفت الدراسة إلى قياس مدى كفاية الإجراءات الأمنية المطبقة على شبكة مكتبات جامعة أم القرى، والتعرف على مواطن القوة وجوانب القصور فيها وذلك في سبيل تطوير تلك الإجراءات وزيادة إحكامها.

وتركز الدراسة من الناحية الموضوعية على الجوانب المتعلقة بحماية أمن المعلومات في الشبكات ومدى تطبيقها على شبكة مكتبات جامعة أم القرى في زمن إجراء هذه الدراسة والمتمثل في عام ١٤٢٢ ه سواء كان ذلك في المكتبة المركزية للطلاب أم في المكتبة المركزية للطالبات.

---

١ الشمرى، رغد عبد الهادى جواد. تشفير المصادر الالكترونية باستخدام معيار مارك ٢١. المجلة الأردنية للمكتبات والمعلومات. مج٤٩،ع٣. ٢٠١٤. ص ص ٤١-٩٧

٢ حسنين، رجب عبد الحميد .أمن شبكات المعلومات الإلكترونية : المخاطر والحلول .Cybrarian Journal .ع٣٠، ديسمبر ٢٠١٢.ص ص ٧٤-١٠١

٣ إسماعيل ، نهال .إدارة أمن نظم المكتبات الآلية المتكاملة بطريقة أكثر فعالية :دراسة تطبيقية على المكتبات المصرية.أعلم ، السعودية.ع٧، اكتوبر ٢٠١٠.ص ص٢٤٠-٢٦٦

٤ محمد، مشيرة أحمد صالح . أساليب حماية وأمن المعلومات في النظم الآلية والشبكات في المكتبات ومراكز المعلومات بالقاهرة الكبرى : دراسة ميدانية.أطروحة(ماجستير) - جامعة عين شمس، ٢٠٠٧

٥ بامفلح، فاتن سعيد. حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى :دراسة حالة. المؤتمر العربى الثانى عشر للاتحاد العربى للمكتبات والمعلومات. المكتبات العربية في الألفية الثالثة. مج٢ ، ٢٠٠١نوفمبر.الشارقة .٥٥١-٥٩٠

١/٩/٥ المحور الخامس : الثغرات الأمنية لتطبيقات الويب

- **التدابير الوقائية لتجنب الثغرات الأمنية في شبكات الحاسوب المحلية** [١] هدفت الدراسة إلى إيجاد حلول لتجنب الثغرات الأمنية الخطرة في شبكات الحاسوب المحلية وتحديد التدابير اللازمة لتجنب حصول الثغرات وإزالة الموجود منها، للوصول إلى أفضل حماية ممكنة، وذلك بتطبيق الاستبانة كأداة لجمع البيانات على عينة الدراسة المكونة من خبراء في تقنية المعلومات من أساتذة جامعات ومهندسين وفنيين ومدراء يعملون في إدارات تقنية المعلومات في المؤسسات التعليمية في الرياض، وأظهرت نتائج التحليل الإحصائي عن وجود فروق ذات دلالة إحصائية بين درجة خطورة الثغرات الأمنية وبين التدابير الوقائية المتخذة لتجنبها، وذلك لصالح درجة خطورة الثغرات الأمنية، الأمر الذي يدل على عدم اكتمال التدابير الوقائية التي تتخذها المؤسسات التعليمية لتلافي الثغرات الأمنية، وأوصت الدراسة بضرورة زيادة الاهتمام بالكادر البشري العامل في حماية الشبكات المحلية، من حيث الكفاءة وكفاية العدد والتدريب والتحفيز لتمكينها من القيام بتدابير الحماية الفيزيائية وإعداد وتشغيل وتحديث أجهزة وبرامج الحماية، وكذلك تنفيذ الاختبارات الدورية لكشف الثغرات الأمنية، بالإضافة لضرورة توفير السياسات الأمنية اللازمة لتنفيذ أعمال الحماية..

١/٩/٦ الدراسات الأجنبية

1. **Analysis of Web Application Code Vulnerabilities using Secure Coding Standards** [2]

تتناول هذه الدراسة تقييم تطبيقات الويب من خلال التغطية الواسعة لتكنولوجيات الأكتف أكس والجافا اسكريبت وأيضا أشهر ثغرات تطبيقات الويب مثل(الخطأ في كتابة الكود البرمجي، وفى تهيئة السيرفر) والشاغل الرئيسي لمطورين تطبيقات الويب هو تعزيز وظائف تطبيق الويب وسهولة الاستخدام وقلقهم الثاني الثغرات الأمنية حيث يتعامل مطوري التطبيقات بفاعلية مع الثغرات من خلال الالتزام بمعيار سكيور .

2. **WEB APPLICATION SECURITY ANALYSIS USING THE KALI LINUX OPERATING SYSTEM** [3]

تتناول هذه الدراسة إمكانيات نظام كالي لينكس في تحليل أمن تطبيقات الويب وأنه يضمن مجموعة من أدوات الاختبار مع إمكانية تثبيت أدوات أخرى عليه وتقدم الدراسة اختبار عملي لتطبيقات الويب باستخدام أدوات من نظام كالي لينكس.

3. **SQLiDDS: SQL injection detection using document similarity measure** [4]

١ عمار، زكريا أحمد، ياسر عامر الكبيسى . التدابير الوقائية لتجنب الثغرات الأمنية في شبكات الحاسوب المحلية : دراسة مسحية تحليلية. المجلة العربية الدولية للمعلوماتية. مج١، ع١، يناير ٢٠١٢.ص ص ٣٥-٤١.

2 Sahu, Divya; Tomar, Deepak.Analysis of Web Application Code Vulnerabilities using Secure Coding Standards. Arabian Journal for Science & Engineering (Springer Science & Business Media B.V.).2017.available at http://0811lbvgc.1106.y.http.web.b.ebscohost.com.mplbci.ekb.eg

3Babincev, Ivan M.; Vuletić, Dejan V .WEB APPLICATION SECURITY ANALYSIS USING THE KALI LINUX OPERATING SYSTEM. Military Technical Courier / Vojnotehnicki Glasnik .2016 available at http://0811lbvls.1106.y.http.web.a.ebscohost.com.mplbci.ekb.eg/ehost

4 Kar, Debabrata; Panigrahi, Suvasini; Sundararajan, Srikanth.SQLiDDS: SQL injection detection using document similarity measure. Journal of Computer Security.2016 available at http://0811lbvls.1106.y.http.web.a.ebscohost.com.mplbci.ekb.eg/ehos

تقدم هذه المقالة طريقة جديدة للكشف عن هجمات حقن قواعد البيانات وذلك من خلال بناء أداة تعمل على الويب ومنصات تشغيل أخرى وتستطيع هذه الأداة الكشف عن جميع أنوع هجمات حقن قواعد البيانات

4. Extraction of Web Applications Vulnerabilities [1]

تهدف هذه الدراسة تقديم نهج جديد لاستخراج الثغرات الأمنية في أكواد تطبيقات الويب مثل: SQL Injection، Cross-Site Scripting، Cookie Poisoning واعتمد النهج المقدم على أحد نظم اكتشاف الثغرات الأمنية هو " white box code" وقد طبق النظام نهجا استباقيا لتقديم النصائح لإصلاح نقاط الضعف المحتملة في الشفرة البرمجية، وتجنب العواقب المحتملة، والهجمات.

5. METHODS TO TEST WEB APPLICATION SCANNERS[2]

تتناول الدراسة طرق مختلفة لفحص تطبيقات الويب من خلال اختيار مجموعة من أدوات الفحص وتطبيقها على مواقع الويب لاكتشاف الثغرات الأمنية فى مواقع الويب وتكون النتائج عبارة عن كشف الثغرات الأمنية فى مواقع الويب وقامت الدراسة بالمقارنة بين العديد من نتائج الدراسات ، وقدمت الدراسة مجموعة من الاقتراحات لتحسين اكتشاف الثغرات الأمنية .

6. SECURITY TESTING OF WEB APPLICATIONS [3]

تقدم هذه المقالة منهجية مختصرة للاختبار الأمني لتطبيقات الويب وذلك لأن تطبيقات الويب تحظى بشعبية كبيرة في السنوات الأخيرة، حيث بدأت تحل محل تطبيقات سطح المكتب. ومع ذلك يؤكد مطوري تطبيقات الويب أنه ليس هناك طريقة واحدة لأجراء الاختبار الأمني الكامل لتطبيقات الويب، تجمع هذه المقالة المنهجية وأفضل الممارسات لتطبيقات الاختبار الأمني لتطبيقات الويب.

7. Web vulnerability study of online pharmacy sites[4]

تهدف هذه الدراسة إلى تقديم طريقة جديدة لتحديد الثغرات الأمنية فى مواقع الصيدليات على الانترنت ، وتقدم التوصيات التقنية والإدارية والقانونية بشأن كيفية التخفيف من حدة الثغرات الأمنية وتوصلت الدراسة إلى أن غالبية الثغرات الأمنية هي (البرمجة النصية عبر المواقع أو الإصدارات القديمة من البرامج التي لم يتم تحديثها) وتقدم طريقة لتأمين مواقع الصيدليات على شبكة الإنترنت.

١/٩/٧ تعليق على الدراسات السابقة

يلاحظ الباحث أن الدراسات السابقة عالجت موضع الأمن المعلوماتي فى مجال المكتبات والمعلومات من زوايا مختلفة مثل الأمن فى المكتبات وشبكات المعلومات والنظم الآلية فى المكتبات وسياسة أمن المعلومات والوعى بأمن المعلومات وركزت الدراسات الأجنبية على تحليل واكتشاف الثغرات الأمنية فى تطبيقات الويب ويستنتج الباحث من ذلك أن ندرة الدراسات العربية فى أمن تطبيقات الويب و على حد علم الباحث لا توجد دراسة تتناول أمن مواقع أقسام المكتبات والمعلومات المصرية على الرغم من أهمية

1 El-Licy ,Fatma A. Extraction of Web Applications Vulnerabilities. Egyptian Computer Science Journal Vol. 39 No. 4 September 2015 . available at http://0811lbvgc.1106.y.http.web.b.ebscohost.com.mplbci.ekb.eg

2 Muñoz, Fernando Román .METHODS TO TEST WEB APPLICATION SCANNERS\Fernando Román Muñoz, Luis Javier García Villalba. The 6th, International Conference on Information Technology, 2013

3 Vala, Radek; Jasek, Roman.SECURITY TESTING OF WEB APPLICATIONS. Proceedings of the 22nd International D AAAM Symposium, Volume 22.DAAAM International: Vienna, Austria,2011.available at http://0811lbvls.1106.y.http.web.a.ebscohost.com.mplbci.ekb.eg/ehost/

4 Kuzma, Joanne.Web vulnerability study of online pharmacy sites. Informatics for Health & Social Care. January 2011; 36(1): 20–34 available at http://0811lbvgv.1106.y.http.web.b.ebscohost.com.mplbci.ekb.eg/ehost/

حماية أمن مواقع أقسام المكتبات والمعلومات للحافظ على ما بها من معلومات، وبينما الدراسات الأجنبية تناولت أمن تطبيقات الويب ولكن لم تتناول أمن مواقع ويب أقسام المكتبات والمعلومات.

ثانياً : الإطار النظري للدراسة

يتناول الإطار النظري للدراسة أهمية أمن المعلومات والاختراق ومراحلة ثم يعرض أنواع الثغرات الأمنية لتطبيقات الويب وفقا لخطورتها ثم يتناول برامج ومواقع اختراق تطبيقات الويب و تقسم إلى ثلاثة محاور(البرامج والمواقع المختصة بالفحص واكتشاف الثغرات الأمنية، المواقع المختصة بالثغرات الأمنية، المواقع المختصة بتعليم الاختراق)

٢/١ أولاً : أهمية أمن المعلومات

بعد ما أصبح العمليات الإلكترونية هي الحل الأمثل لأغلب سكان الكرة الأرضية لا يمكن إنكار أهمية أمن المعلومات بما أنه يلعب دور حارس القلعة التي إن سقطت اليوم، أصبح العالم متخلفاً وعاد عقوداً من السنين إلى الوراء وتتضح أهمية أمن المعلومات مما يأتي :

- **١/١ سرية البيانات**: يحافظ على سرية البيانات المنقولة عبر الوسائط الإلكترونية حيث هذه الخدمة تمنع الهكر من إنشاء هجمات من نوع التجسس و تحليل البيانات المرسلة حيث يضمن المُرسل أن بياناته قد وصلت إلى المستقبل بسرية تامة، بل يجعل مهمة الهكر الراغب في الوصول إلى المعلومة من الاستحالة بحيث إما أن يستسلم أو يصل إلى المعلومات بعد زمن تفقد فيه المعلومة قيمتها.
- **١/٢ سلامة البيانات من أى تغيير أو تشوية فمثلا** استلمت راتبك أقل مما يجب بـــــ ٨٠% في لحظة أنت في حوجه ماسة لهذا الراتب و هذا قد حدث رغم أن مديرك قد قدم طلباً إلكترونياً بتسليمك الراتب كاملاً، هذا هو ما يدعى بهجمات التعديل على البيانات و التي يمنعها استخدام أمن المعلومات، فالرسالة تصل كما أُرسلت تماماً لحماية الطرفين.
- **١/٣ عدم الإنكار** : هل تتصور أن تُرسل رسالة من هاتفك إلى شخصٍ ما ثُم تستطيع إنكار ذلك؟، إن لم تستطع فعل ذلك رغم محاولاتك الحثيثة فهذا بسبب تطبيق مفاهيم أمن المعلومات، و بدونه لن توجد مصداقية في المحادثة بين أي طرفين، و بغياب المصداقية تنهار كُل المراسلات التقنية.
- **١/٤ المصادقة** : لكل شخص يرغب بالانضمام إلى محادثة مع صديق مثلا، فلا بد أن يكون مُطمئناً أنه يتحدث مع صديقه فعلاً، من الخدمات التي يقدمها أمن المعلومات هي ضمان أن الطرف الآخر هو الشخص الذي اخترته فعلاً و ليس شخصاً آخر، فلا يمكن إرسال رسالة إلى البنك لتحويل الرواتب و تصل إلى مخبز! أمن المعلومات متوفر لضمان الإيصال.
- **١/٥ التحكم بالوصول**:هذه الخدمة يعشقها محبوا الخصوصية، وهي تعني حماية البيانات من الوصول غير المسموح به، فما يوجد بهاتفك من نظام بصمة أو كلمة مرور أو أي طريقة حماية أخرى ما هي إلا تطبيق لإحدى خدمات أمن المعلومات، كما أن نظام كلمة المرور بحاسبك و غيرها من نظم حماية البيانات و/أو الأنظمة تُعد تطبيقاً لخدمات أمن المعلومات.

مما سبق يتضح أننا لا تستطيع الحياة بدون أمن المعلومات طالما أن التعاملات الإلكترونية في ازدياد[١]

1 https://www.oolom.com/1105/%D9%84%D9%85%D8%A7%D8%B0%D8%A7-%D8%A3%D8%B5%D8%A8%D8%AD-%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA-%D8%A8%D9%87%D8%B0%D9%87-%D8%A7%D9%84%D8%A3%D9%87%D9%85%D9%8A%D8%A9

٢/٢ ثانياً : الاختراق Hacking

تسمى الاختراق بالإنجليزية (Hacking) و تسمى باللغة العربية عملية التجسس أو الاختراق حيث يقوم أحد الأشخاص الغير مصرح لهم بالدخول نظام المعلومات بطريقة غير شرعية ولأغراض غير سوية مثل التجسس أو السرقة أو التخريب حيث يتمكن الشخص المخترق للنظام أن ينقل أو يمسح او يضيف ملفات أو برامج

- **٢/٢/١ الكراكرز: crackers** هي كلمة مأخوذة من الفعل Crack بالإنجليزية وتعنى الكسر أو التحطيم ، وهم أفراد لديهم مهارات استثنائية فى علم الحوسبة ، اللجوء إلى أنشطة ضارة أو مدمرة، كما أنهم معروفين أيضا باسم المخترقون ذو القيعة السوداء Black Hats هؤلاء الأفراد دائم ما يستخدمون مهاراتهم فى الأنشطة التدميرية والتي تسبب ضرر كبير للشركات والمؤسسات والأفراد. هؤلاء يستخدمون مهاراتهم فى إيجاد الثغرات فى الشبكات المختلفة والتي تشمل أيضا المواقع الحكومية ومواقع الدفاع والبنوك هكذا بعضهم يفعل ذلك من أجل أحداث ضرر أو سرقة معلومات أو تدمير بيانات أو كسب المال بطريقة سهل.
- **٢/٢/٢ الهاكر Hacker: شخص عبقري فى البرمجة ويقوم بتصميم أسرع البرامج والخالية من** المشاكل والعيوب التى تعيق البرنامج عن القيام بدوره المطلوب منه.
- **٢/٢/٣ الهاكر الأخلاقى Ethical Hacker**

هو عملية فحص واختبار الشبكة الخاصة بك من أجل إيجاد الثغرات ونقاط الضعف والتي من الممكن أن يستخدمها الكراكز . الشخص الذى يقوم بهذه العملية هو الهاكر الأبيض (white hacker) الذى يعمل على الهجوم على أنظمة التشغيل بقصد اكتشاف الثغرات بها بدون الحاق أى ضرر. وهذا من الطبيعي يؤدى إلى زيادة معدلات الأمن لدى النظام الخاص بك . أو بمعنى أخر هو أنسان له مهارات تعطيه إمكانية الفهم والبحث عن نقاط الضعف فى أنظمة التشغيل المختلفة، وهذا الشخص يعتبر نفسه هاكرز حيث يستخدم نفس معرفته ونفس أدواته ولكن بدون أن يحدث أى ضرر. ويستخدمها فى تحسين الوضع الأمن، **ويعتبر الهاكر الأخلاقي ضروري ولذلك لأن هناك نمو سريع فى مجال التكنولوجيا ، لذلك هناك نمو فى المخاطر المرتبطة بالتكنولوجيا.**

- **٢/٢/٤ اختبار الاختراق penetration testing**

هو طريقة من أجل تقييم النظام الأمني للنظام الحاسوبي أو الشبكة الحاسوبية، وذلك لاستهداف الحواسيب عبر مجموعة من الهجمات المختلفة لرؤية فيما إذا كان الحاسوب قادر على التعامل مع هذه الهجمات بدون أى تأثير على أداءه، والهجمات المختلفة في اختبار الاختراق تتضمن تحديد واستغلال نقاط الضعف المعروفة في مختلف التطبيقات البرمجية وأنظمة التشغيل وتحديد قوة الاتصال في الشبكة ويعتبر اختبار الاختراق مجال مستقل في دراسة علوم الحاسب[١]

- **٢/٢/٥ أهمية اختبار الاختراق**
  - تحديد التهديدات التى تواجه أصول المعلومات فى المؤسسة
  - تخفيض تكاليف أمن المعلومات للمؤسسة وتوفير أفضل عائد من الاستثمار الأمن حسب تحديد وحل نقاط الضعف

١ كيالى، اسماعيل محمد. نظام التشغيل KALI LINUX : الدليل السريع.[د.م : د. ن]،٢٠١٤

- توفير المنظومة مع الضمان من خلال تقييم شامل للمنظومة الأمنية و التى تغطى السياسة والإجراءات والتصميم والتنفيذ
- الاختبار والتحقق من صحة وكفاءة الحماية الأمنية والضوابط
- تغيير أو ترقية البنية التحتية من البرمجيات او الأجهزة أو تصميم الشبكات
- التركيز على نقاط الضعف الأكثر شدة والتأكد من الأمن على مستوى التطبيق
- توفير منهج شامل لخطوات إعداد يمكن اتخاذها لمنع الاستغلال
- تقييم كفاءة أجهزة أمن الشبكات مثل الجدران النارية و الراوتر وخوادم الويب

- **٢/٦ /٢ مراحل الاختراق : تمر عملية الاختراق بعدة مراحلة هى :**

٢/٦/١ /٢ عملية جمع المعلومات (الاستطلاع) Reconnaissance

حيث يقوم المهاجم بجمع أكبر قدر ممكن من المعلومات عن الهدف لتقيمه قبل تنفيذ هجمته و يضع استراتيجيات الهجوم والتي من الممكن أن تأخذ بعض الوقت حتى يصل على المعلومات المهمة ويستخدم الوسائل التالية في جمع المعلومات :

- فحص الشبكة سواء من الداخل أو الخارج بدون دخول على النظام.
- الهندسة الاجتماعية social engineering او ما يعرف بفن اختراق العقول وهو عبارة عن مجموعة من التقنيات المستخدمة لجعل الناس يقومون بعمل ما أو يفصحون عن معلومات سرية وتستخدم فى المرحلة الأولى (مرحلة جمع المعلومات) حيث أن الهدف الأساسي للهندسة الاجتماعية هو طرح أسئلة بسيطة أو تافهة عن طريق الهاتف أو البريد الإلكتروني مع انتحال شخصية ذو سلطة أو ذات عمل يسمح له بطرح هذه بطرح هذه الأسئلة دون إثارة الشبهات.
- الغوص فى سلة المهملات: وهى عبارة عن عملية النظر فى سلة مهملات بعض المنظمات من أجل الوصول إلى بعض المعلومات الحساسة المستبعدة مثل اسم المستخدم والرقم السرى وأرقام الكريديت كارد والحالة المالية ورقم الائتمان وغيرها من المعلومات الحساسة
- استخدام شبكة المعلومات الانترنت للحصول على بعض المعلومات مثل معلومات الاتصال والشركاء فى العمل والتكنولوجيا المستخدمة وبعض المعلومات الحساسة الأخرى .

٢/٢/٦/٢ فحص الشبكة Scanning:

فحص الشبكة للحصول على معلومات محددة على اساس المعلومات التى تم جمعها من خلال عملية الاستطلاع، ويستخدم القراصنة المسح للحصول على نقطة دخول (الثغرة) للبدء فى الهجوم ، وتتضمن عملية المسح مسح المنافذ، خرائط الشبكة الضعف الأمني ، وما إلى ذلك والمهاجم دائما ما يستخدم الأدوات الجاهزة مثل war dialers - network host scanner لإيجاد النظام واكتشاف الثغرات الى يحتويها

٢/٦/٣ /٢ مرحلة الاختراق Gaining Access

المخترق يستغل الضعف فى النظام ، حيث يمكن أن يحدث ذلك على مستوى شبكة محلية أو الأنترنت أو على مستوى نظام التشغيل أو على مستوى التطبيقات

٢/٢/٦/٤ مرحلة الوصول والحفاظ على الوصول Maintaining Access

وتشير إلى المرحلة التى يحاول فيها المخترق حفظ ملكية الدخول مجددا إلى النظام، من خلال وصول حصري باستخدام Backdoor أو Rootkite أو Trojans مما يسمح للمخترق بتحميل ورفع الملفات، والتعامل مع البيانات والتطبيقات على النظام المخترق.

٢/٢/٦/٥ مسح الأثر Clearing Tracks

تشير إلى الأنشطة التى يقوم بها المحترق لإخفاء دخوله إلى النظام ، بسبب الحاجة للبقاء لفترات طويلة، ومواصلة استخدام الموارد، وتشتمل إخفاء بيانات الدخول والتغيير فى ملف Log

٢/٣ ثالثاً : أنواع الثغرات الأمنية لتطبيقات الويب

يتم تحديد أنواع الثغرات وفقا لما ورد في مشروع **Owasp**[١] عام٢٠١٧ وتم الاعتماد على ترجمة المصطلحات على ما ورد فى ملف مشروع **Owasp** المعرب لعام ٢٠١٣ والذى يحدد أشهر عشرة أنواع ثغرات تطبيقات الويب انتشارا على مستوى العالم ويرتبها وفقا لخطورتها

٢/٣/١ النوع الأول : الحقن [Injection]

أن عملية "حقن قواعد البيانات" SQL Injection تعني قدرة المستخدم على إرسال نصوص برمجية Queries إلى قاعدة بيانات الموقع الإلكتروني، بهدف الحصول على معلومات غير متاحة لعامة المستخدمين حيث يمكن للمهاجم التعامل مباشرة مع قاعدة البيانات و إجراء استعلامات غير متوقعة من طرف المبرمج ، كالولوج و سرقة البيانات ، و إدخال بيانات جديدة أو تعديل البيانات السابقة أو حذفها . أما من الناحية البرمجية، فهي تعني فشل الموقع في فحص البيانات القادمة إليه فيما إذا كانت تلك البيانات نصوصًا برمجيةً أو نصوصًا عاديةً مسموحًا بها.

ويمكن القول بأن قاعدة البيانات هي قلب المواقع الديناميكية، والحصول على معلومات منها يُعتبر تهديد لمستخدمي الموقع الإلكتروني والقائمين عليه.[٢] والعثور على هذه الثغرة في تطبيق ما واستغلالها أمر لا يحتاج إلا لمعرفة بسيطة بكيفية التعامل مع قواعد البيانات ، ويعود سبب وجود هذه الثغرة إلى عدم حماية البيانات أثناء التعامل مع قاعدة البيانات إما عن غير قصد ، و غالبا عن الجهل الذي يخيم على "المبرمج" . فلا غرابة أن نجد هذه الثغرة في الكثير و الكثير من المواقع . رغم أنها من أقدم الثغرات ، و طرق حمايتها لا يتطلب جهدا و خاصة أثناء إنجاز المشروع[٣] ويتم منع ثغرات حقن قواعد البيانات عن طريق عزل البيانات الغير موثوق بها عن الأوامر والاستعلامات الموجهة لقاعدة البيانات.[٤]

٢/٣/٢ النوع الثانى : ضعف الهوية وإدارة جلسة الاتصال Broken Authentication and Session Management

في غالب الأحيان، يتم تطبيق البرامج المسئولة عن التحقق من الهوية أو إدارة جلسات الاتصال بطريقة غير صحيحة، مما يسمح ذلك للمخترقين بسرقة كلمات المرور، أو المفاتيح، أو معرّف جلسة الاتصال، أو بالإمكان كذلك استغلال ثغرات أخرى بانتحال هويات مستخدمين آخرين

1 https://www.owasp.org

٢ ما هي عملية "حقن قواعد البيانات. متاح على http://keefwiki.com/tech/ -sql-injection/

٣ ثغرة حقن قاعدة البيانات.https://www.dorossinet.com/news/sql-injection

٤https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet

، ويمكن التغلب على هذه الثغرة بتوفير برامج قوية لتحقق من الهوية والتحكم في إدارة جلسات الاتصال وذلك بتطبيق المعايير الخاصة بذلك [١]

٢/٣/٣ النوع الثالث - البرمجة عبر الموقع Cross-Site Scripting – XSS

تظهر ثغرات البرمجة عبر الموقع عندما يقوم التطبيق باستلام بيانات غير موثوقة وإرسالها إلى المتصفح من دون التحقق منها أو تخطيها ." escaping " تسمح ثغرات البرمجة عبر الموقع أن يقوم المخترق بتنفيذ نصوص برمجية "scripts" في متصفح الضحية وتكون بلغة javascript أو html و يتم إدخالها غالبا في صندوق التعاليق أو في مربع البحث، ويرجع سببها إلى أن المبرمجين لا يقومون بوضع أكواد تمنع من إدخال هذه الثغرات من طرف المخترقين[٢] ، ويسهل الاختراق من خلال هذه الثغرة وينتج عن الاختراق ما يلى :

- سرقة الكوكيز والدي يسمح لك بالدخول إلى لوحة التحكم للموقع بدون معرفة كلمة السر
- تحويل زوار الموقع المخترق إلى موقع أخر خبيثة ويطلبون منهم تحميل ملفات أو برامج يوهمون الضحية بأنها من صاحب الموقع المخترق وبالتالي تكون هده البرامج عبارة عن فيروسات تؤدي إلى اختراق أجهزتهم.
- تشوية الموقع بتغيير محتوى الصفحة بادحال أكواد html

يمكن التغلب على هذه الثغرة باتياع ما يلى :

- تفعيل خاصية No-Script Add on في متصفحات الانترنت
- عدم الوثوق في الروابط القصيرة
- مسح كل الكوكيز من على متصفحك ومن ثم تصفحها من خلال بروكسي لكي لا يلتقط المخترق الأيبي الخاص بك [٣]

٣/٤ /٢ النوع الرابع : لإحالة المباشرة الغير أمنة Insecure Direct Object References

تظهر ثغرة الإحالة المباشرة الغير آمنة عندما يقوم المبرمج بتعريض مراجع لمكونات داخلية مثل الملفات أو قائمة المجلدات أو مفاتيح قواعد البيانات من دون تطبيق أدوات التحكم بالوصول أو غيرها من أساليب الحماية، يمكن للمخترق أن يتلاعب بهذه المراجع للوصول إلى بيانات من دون صلاحيات مناسبة .ويمكن الوقاية من هذه الثغرة باختيار طريقة لحماية كل كائن يمكن للمستخدم الوصول إلية مثل (رقم الكائن ، واسم الملف) وذلك باستخدام إحالات غير مباشرة للكائنات خاصة لكل مستخدم أو لكل جلسة وأيضا التحقق من صلاحية الوصول لضمان أن المستخدم مصرح له بالكائن المطلوب [٤]

٣/٥ /٢النوع الخامس : الإعدادات الأمنية الخاطئة Security Misconfiguration

التأمين الجيد يتطلب أن يتم تحديد وتطبيق الإعدادات الأمنية للتطبيقات، إطارات العمل، خوادم التطبيقات، خوادم الويب، خوادم قواعد البيانات، و منصات التشغيل، ويجب تحديد الإعدادات الأمنية وتطبيقها والمحافظة عليها، حيث أن غالب الإعدادات الافتراضية لا تكون آمنة بالإضافة إلى ذلك، يجب أن تحدث البرمجيات أولاً بأول، ويمكن التغلب على هذه الثغرة باتباع ما يلى :

١. إجراءات تأمين قابلة للتكرار مما تسهل من مهمة إنشاء بيئة جديدة وآمنة .

1 https://www.owasp.org/index.php/Authentication_Cheat_Sheet
2 http://cwe.mitre.org/data/definitions/79.html
3 http://hack4s3c.blogspot.com.eg/2012/06/cross-site-scripting-xss.html
4https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

٢. تحديث لجميع البرامج المستخدمة في مختلف البيئات لضمان إدراج جميع المكتبات البرمجية
٣. بنية تطبيق قوية بحيث توفر فصل أمن وفعال بين المكونات [١]

٢/٣/٦ النوع السادس : كشف البيانات الحساسة Sensitive Data Exposure

الكثير من التطبيقات لا تقوم بحماية البيانات الحساسة مثل بطاقات الائتمان، ومعرفات الضرائب، وبيانات التحقق من الهوية بشكل مناسب، يمكن للمخترقين سرقة أو تغيير مثل هذه البيانات الغير محمية بالشكل المطلوب لإجراء احتيالات مالية، أو سرقة الهوية، أو جرائم أخرى .إن البيانات الحساسة تتطلب مزيد من الحماية، مثل تشفيرها عند الحفظ أو النقل، كذلك تطبيق احتياطات خاصة عند تبادل هذه البيانات مع المتصفح.

الوقاية من هذه الثغرة نتبع ما يلى :

- التأكد من تشفير جميع البيانات الحساسة سواء في حالة التخزين او الإرسال
- التخلص من تخزين البيانات الحساسة الغير مطلوبة
- التأكد من استخدام خوارزميات قياسية وقوية ومفاتيح تشفير قوية والإدارة الجيد لها
- التأكد من تخزين الكلمات السرية باستخدام خوارزمية مخصصة لتخزين الكلمات السرية
- قم بتعطيل خاصية الإكمال التلقائي عند تعبئة البيانات الحساسة وتعطيل خاصية الاحتفاظ بنسخة للوصول السريع للصفحات التى تحتوى على بيانات حساسة[٢]

٢/٣/٧ النوع السابع : إهمال التحكم بالوصول الوظيفى Missing Function Level Access Control

تقوم أغلب التطبيقات بالتحقق من صلاحيات الوصول الوظيفية قبل إظهار تلك الوظائف عبر واجهات المستخدم في كل الأحوال، تحتاج التطبيقات لتطبيق نفس إجراءات التحقق من صلاحيات الوصول لكل وظيفة. حيث إذا لم يتم التحقق من صلاحيات الوصول لكل وظيفة ، فعندها يمكن للمخترقين أن يقوموا بتزوير طلبات من أجل الوصول إلى وظائف من دون صلاحيات مناسبة.

ويمكن التغلب على هذه الثغرة باتباع ما يلى :

- تصميم تطبيق الويب بطريقة تسهل عملية التحقق من صلاحيات الوصول في أجزاءه
- عدم تحديد صلاحيات بعينها فى النص البرمجي
- يجب عدم وضع صلاحيات الوصول لوظائف التطبيق افتراضيا ، إلا بعد إذن بالسماح للوصول للوظيفة [٣]

٢/٣/٨النوع الثامن : تزوير الطلبات عبر الموقع Cross-Site Request Forgery – CSRF

ثغرات تزوير الطلبات عبر الموقع تجبر مُتصفح الضحية على إرسال طلبات (HTTP) مزورة تتضمن ملف جلسة الاتصال و أي معلومات تستخدم للتحقق من هوية المستخدم إلى تطبيقات ويب أخرى مصابة، وهذا يسمح للمخترق بإجبار متصفح الضحية من إنشاء طلبات تظهر بأنها صادرة من الضحية ومشروعة في التطبيق المصاب

1 https://www.pcmag.com/article2/0,2817,11525,00.asp
2https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project
3 https://www.owasp.org/index.php/Category:Access_Control

للوقاية من هذه الثغرة نتبع ما يلى :

- تضمين معرفات غير قابلة للتخمين في جميع طلبات بروتوكول نقل النصوص (HTTP) بحيث تكون هذه المعرفات فريدة على الفل لكل جلسة اتصال للمستخدم .
- إضافة المعرف الفريد فى حقل مخفى بحيث يتم إرسال القيمة عبر جسد الطلب بدلاً من إرسالها عبر عنوان URL مما يجعلها أقل عرضة للانكشاف .

٢/٣/٩ النوع التاسع : استخدام مكونات معروفة الضعف Using Components with Known Vulnerabilities

المكونات، مثل المكتبات وإطارات العمل والوحدات البرمجية الأخرى، تعمل في غالب الأمر بصلاحيات كاملة في حال استغلال إحدى المكونات فإن مثل هذا الهجوم قد يؤدي إلى فقد البيانات بصورة خطيرة أو الاستحواذ على الخادم إن استخدام مكونات معروف إصابتها بثغرات أمنية قد يعرض دفاعات التطبيق للخطر ويعرضه لمجموعة من الاختراقات والأضرار.

للوقاية من هذه الثغرة نتبع ما يلي

- ترقية المكونات إلى الإصدارات الجديدة حتى نتجنب الثغرات الموجودة في الإصدارات القديمة
- متابعة الحالة الأمنية لهذى المكونات في قواعد البيانات العامة والقوائم البريدية للمشروع، و القوائم البريدية الأمنية ، مع مراعاة تحديثها دوريا .
- أضافة طبقة أمنية حول المكونات وذلك لتعطيل الوظائف الغير مستخدمة ولتأمين جوانب من المكونات المصابة بثغرات أمنية

٢/٣/١٠ النوع العاشر : الارسال وإعادة التوجيه الغير محقق Unvalidated Redirects and Forwards

تقوم تطبيقات الويب بإعادة توجيه المستخدمين إلى صفحات أو مواقع ويب أخرى، وتستخدم بيانات غير موثوقة لتحديد صفحات الوجهة من دون إجراءات التحقق المناسبة قد يتمكن المخترقين من إعادة توجيه الضحايا إلى مواقع مزورة (إصطياد إلكتروني)أو مواقع مصابة ببرمجيات خبيثة، أو التوجيه للوصول إلى صفحات غير مصرح له فيها.

للوقاية من هذه الثغرة نتبع ما يلى :

الاستخدام الآمن لعمليات إعادة التوجيه أو الإرسال تتم بعدة طرق :

- تجنب استخدام عمليات إعادة التوجيه أو الإرسال و في حالة استخدامها، لا تقم بالاعتماد على متغيرات المستخدم لتحديد صفحات الوجهة .
- عند عدم إمكانية تجنب استخدام متغيرات الواجهة تأكد من أن القيمة المرسلة تم التحقق منها وأنها مخولة للمستخدم .
- مما ننصح به في حالة استخدام متغيرات الوجهة ، أن لا يتم استخدام القيم الحقيقية لعناوين الصفحات أو جزء منها ، بل يستعاض عنها بقسم بديلة يتم مطابقتها وترجمتها لاحقا من جانب الخادم .

٢/٤ رابعاً : برامج ومواقع اختراق تطبيقات الويب

"الوقاية خيرا من العلاج" معظم مشرفي المواقع يولون الاهتمام الأكبر و الجزء الأكبر من وقتهم لأمور تتعلق بتصميم الموقع و تحديث المحتوى ، ولكن يجب إعطاء أمن الموقع الاهتمام المطلوب ، إذا

كان بالإمكان تفحص الموقع يومياً فهذا أفضل ، إذا كانت الميزانية المرصودة للموقع تسمح بتوظيف شخص مختص بأمن المواقع أو باللجوء إلى أحد الشركات التي تقدم خدمات حماية المواقع فلا تتردد.

ونقسم برامج ومواقع اختراق تطبيقات الويب إلى ثلاثة محاور

٢/٤/١ المحور الأول : يتناول البرامج والمواقع المختصة بالفحص واكتشاف الثغرات الأمنية
٢/٤/٢ المحور الثاني : يتناول المواقع المختصة بالثغرات الأمنية
٢/٤/٣ المحور الثالث : يتناول مواقع المختصة بتعليم الاختراق

٢/٤/١ المحور الأول : يتناول البرامج والمواقع المختصة بالفحص واكتشاف الثغرات الأمنية

تستخدم هذه البرامج لفحص تطبيقات الويب من أجل اكتشاف الثغرات الأمنية سواء للمواقع العادية أو للشركات، وأصبحت تستخدم بشكل واسع خلال السنوات الأخيرة من قبل المهتمين بمجال أمن المعلومات واختبار اختراق تطبيقات الويب، وأشارت التقارير في السنوات القليلة الأخيرة أنه تم إيجاد ثغرات خطيرة بمواقع لشركات كبيرة عن طريق استخدام هذه البرامج وتشترك هذه البرامج فى كل أو بعض الوظائف التالية[١] :

- فحص تطبيقات الويب والبحث عن الثغرات الأمنية الموجودة
- تصنيف الثغرات الأمنية وفقا لدرجة خطورتها (حرجة، مرتفعة، متوسطة، منخفضة، معلومات) أو وفقا لأنواع الثغرات أو وفقا لمكان وجودها
- يعرض نقاط الضعف والدليل عليها وكيفية إصلاحها
- تعمل على بيئات تشغيل مختلفة
- يدعم مجموعة من صيغ التقارير(plain text, XML, HTML, NBE or CSV) عن نتيجة الفحص فضلا عن تصميم تقرير خاص بك وامكانية تبادلها من الزملاء
- تستطيع تحديد نقاط الضعف المشتبه بها
- إمكانية إجراء الفحص يدويا حيث يتيح أمكانية ضبط استراتيجية الفحص لتناسب ما تريد
- إمكانية استغلال الثغرات الموجودة .
- المرونة حيث يمكن فحص جزء معين من تطبيقات الويب وليس التطبيق كاملا فقط
- التكامل مع أدوات الفحص الأخرى.
- يوجد برامج تتاح بالمجان وأخرى بمقابل مادى ويجد برامج منها نسخ مجانية محدودة الإمكانيات و أخرى بمقابل مادى

مجال أمن المعلومات واختبار اختراق تطبيقات الويب يشمل العديد من البرامج ومواقع الويب ونعرض لأشهر البرامج ومواقع الويب والأكثر استخداما فى مجال اختبار تطبيقات الويب .

٢/٤/١/١ أولاً : برامج اختبار تطبيقات الويب الأشهر والكثر استخداماً

١- كالي لينكس لاختبار واختراق مواقع الويب[٢]

نظام Kali Linux مبنى على أساس نظام التشغيل Linux ومصمم بهدف استخدامه فى اختبار الاختراق وهو مجموعة من البرمجيات مفتوحة المصدر والتي يستخدمها المحترفون والخبراء أثناء التعامل مع الحالات العملية لاختبار الاختراق وهي متخصصة في الأمن والحماية المعلوماتية واختبار

١ قام الباحث بتحديد هذه الوظائف عن طريق العديد من برامج الاختراق

2 http://ar.codexait.com/2016/03/top-web-tools-in-kali-linux.html

الاختراق Penetration Testing تم الإعلان عن صدورها في ١٣ مارس ٢٠١٣ ، وتحتوي مسبقا على عدة برامج وأدوات موجهة لاختبار الاختراق بكل مراحلة بداية من مرحلة جمع المعلومات ثم اكتشاف الثغرات الأمنية ثم الاختراق ثم الوصول والمحافظة على الوصول وفى النهاية مسح اثر الاختراق ، وبعض مميزاته :

- يحوى أكثر من ٣٠٠ أداة للاختراق والتقديرات الأمنية
- يدعم العديد من التجهيزات الخارجية مثل المستقبلات اللاسلكية وتجهيزات pci
- يؤمن بيئة متكاملة للتطوير بعدة لغات برمجية مثل Ruby ,Python,C
- نظام مفتوح المصدر وقابل للتطوير
- كالى لينكس هو نظام مجانى : وقد اعلنت الشركة المطورة والمصممة له بذلك انه سيظل مجانى الى الابد
- متعدد اللغات : بالرغم من ان معظم الكثير من ادوات اختبار الاختراق باللغة الانجليزية، الا ان الشركة قامت بدعمها مع بعض اللغات التى تسمح للمستخدم بالتعديل غيره بلغته.[١]

أدوات نظام كالى لينكس

يوجد عدد كبير من الأدوات المخصصة لدعم تطوير انظمة الحماية والاختراق واذا استخدم هذه الادوات الهاكرز الغير أخلاقيّن فان كثير من حالات السرقة والاختراق قد تحدث فهذه الادوات مخصصة لدعم الحماية ولكن من يدعمك يستطيع ان يكسرك أما بالنسبة للأدوات التي يحتويها كالي لينكس كثير ة لكن اهمها:

- برامج لتحليل الحزم المتبادلة على الشبكات
- ماسح للنوافذ المفتوحة والمغلقة على الشبكة
- كاسر لكلمات المرور كلمات السر
- إمكانية تشغيل نظام وهمي
- برنامج الـ wireshark وهو يعد من اقوى البرامج في مراقبة الحزم الصادرة والواردة[٢]

أشهره هذه الأدوات

- **Whatweb** :تقوم باستكشاف معلومات عن السرفر وعنوان الأنترنت ومعلومات إضافية خاصة بالسيرفر
- Maltego : خاصة بالاستطلاع ومعرفة معلومات عميقة عن الموقع مثل نطاق الدومين وايميلات خاصة بمالك الموقع وأرقام هواتف وغيرها من المعلومات وهى ذات واجهة رسومية وبلغة الجافا ومتوفرة أيضا على الويندوز فقط تحتاج تسجيل حساب فى موقع الأداة
- Wapiti :أفضل أداة لفحص الثغرات فهى تقوم بعمل فحص دقيق للموقع وتعطيك مكان وروابط استغلال الثغرة
- Httrack :هذه الأداة خاصة بتحميل ملفات الموقع فمن الرائع الحصول على ملفات الموقع وقراءة الأكود والتعرف على بنية الموقع أكثر
- Sqlmap :خاصة باستغلال ثغرات قواعد البيانات وتنفيذ هجوم حقن قواعد البيانات

١ ما هو نظام كالى لينكس . ٢٠١٦ متاح على https://www.matrix219.com/eg/2016/09/10/kali-linux/ في ٢٠١٨/٣/١

2 https://touch-tech.net/2017/03/20/kali-linux

٢- **برنامج Netsparker**[47] : يعتبر **برنامج Netsparker** من أهم الأدوات المستخدمة في عملية **Web Application Security Scanner** حيث يساعد المهتمين بمجال **اختبار اختراق تطبيقات الويب** بالكشف عن الثغرات الأمنية في المواقع الخاصة بك وتطبيقات الويب وخدمات الويب يوجد منه نسخة كتطبيق ويندوز ويوجد امكانية الفحص عبر الموقع من خلال اختيار Cloud Scanner ، ويتميز بسهولة الاستخدام ، ، ويحدد نقاط الضعف والدليل عليها ، التدعيم الكامل لغة HTML5 التى تجعل تطبيقات الويب أكثر ثراء وتفاعلية وديناميكية، ويعرض فى موقع البرنامج كشاف[١] بالثغرات الأمنية لتطبيقات الويب مصنفة وفقا لدرجة خطورتها إلى (حرجة، مرتفعة، متوسطة، منخفضة، معلومات)، ويتيح لك استغلال الثغرات الموجودة عن طريق خاصية.**Integrated Exploitation Engine**

٣- **برنامج Burp Suite** [٢] مكتوب بلغة البرمجة Java ويعمل من خلال برتوكول نقل الصفحات http وذات واجهة رسومية ويدعم نظام الويندوز، ويعد من البرامج والأدوات المستخدمة بكثرة للكشف عن الثغرات الأمنية بتطبيقات الويب، ويحتوي مجموعة متنوعة من الأدوات المصممة لتسهيل عملية فحص وتحليل واختراق تطبيقات الويب، يتوفر من البرنامج نسخة مجانية محدودة الإمكانيات ونسخة مدفوعة بقيمة $٢٩٩ ، ويعل هذا البرنامج بشكل مستقل ويمكن أن يعمل كأحد أدوات نظام كالي لينكس.

٤- **أداة Vega Scanner**[٣]**:**

أداة مفتوحة المصدر وذات واجهة رسومية، وتعد أداة رائعة جدا لفحص واكتشاف الثغرات فى مواقع الويب وتستخرج الثغرات البرمجية الموجودة بها مثل **SQL Injection - XSS - Cross-Site Scripting** وتعمل هذه الأداة على عدة أنظمة تشغيل ومكتوبة بلغة الجافا وتمتاز بأنها مجانية وقوية وسهلة الاستعمال، **و يمكن إجراء اختبار الأمن أليا أو يدويا أو مختلط**

٢/٤/١/٢ ثانيا : أشهر مواقع الويب للكشف عن الثغرات الأمنية فى تطبيقات الويب

١. **أداة الفحص من جوجل** [٤] أداة مقدمة من جوجل تقوم بفحص موقعك و التأكد من عم وجود أي محتوى غير آمن على موقعك ، الأداة سهلة و لا تحتاج إلى شرح ، كل ما تحتاجه هو وضع رابط الموقع و ستحصل على النتيجة.

٢. **Scan My Server** [٥]موقع ممتاز يقوم بفحص موقعك من كل الثغرات و يرسل لك تقرير أمني عن كافة الثغرات الموجودة في موقعك.

٣. **SSL Labs** [٦] موقع ممتاز يفحص المواقع التي تعمل ببروتوكول HTTPS و يعطيك معلومات عن شهادة الموقع و الثغرات المتعلقة ببروتوكول SSL من المهم جداً أن تتفحص موقعك باستخدام هذه الأداة.

٤. **Detectify** [١] تقوم هذه الأداة بإجراء أكثر من ١٠٠ اختبار أمني على موقعك بحثاً عن ثغرات متواجدة فيه.

1https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/
2https://portswigger.net/burp/communitydownload
3 https://subgraph.com/vega/
4 https://transparencyreport.google.com/safe-browsing/search
5 https://www.scanmyserver.com/
6 https://www.ssllabs.com/ssltest/

٥. **Web Inspector** [٢] أيضاً أداة أخرى تقوم بالفحص بحثاً عن الأكواد الضارة و البرمجيات الضارة التي يمكن أن تتواجد في موقعك.

٢/٤/٢ المحور الثاني : يتناول المواقع المختصة بالثغرات الأمنية

تقدم هذه المواقع معلومات كاملة عن الثغرات وطرق علاجها ومن أهم وأشهر هذه المواقع ما يلى :

١- OWASP [٣]

مشروع أمان تطبيقات الويب مفتوح المصدر وهى منظمة خيرية غير هادفة للربح مهمتها جعل أمن البرمجيات مرئي بحيث تجعل الأفراد والمنظمات قادرون على اتخاذ قرارات مستنيرة، ويهدف المشروع إلى نشر الوعي عن أمن التطبيقات وذلك بتحديد أبرز المخاطر الأمنية الحرجة التي قد تواجهها المنظمات وطرق التغلب على هذه المخاطر، ويمكنك الحصول مجاناً وبشكل مفتوح على ما يلي : أدوات ومعايير أمن التطبيقات، و كتب متكاملة في اختبار أمن التطبيقات، والتطوير الآمن للنصوص البرمجية، والمراجعة الأمنية للنصوص البرمجية، ومكتبات وأدوات تحكم أمنية معيارية ، وأبحاث متطورة ، ويحدد هذا المشروع أخطر عشرة ثغرات لتطبيقات الويب حيث يجمع بيانات **تتجاوز ال 500,000 ثغرة أمنية خلال مئات المنشآت وآلاف التطبيقات، و تم اختيار وترتيب العشرة ثغرات الأوائل** وفقا لدرجة الخطورة وليس وفقا لمدى انتشارها فقط .

١. **SecurityFocus** [٤]: موقع أمريكى تأسس عام ١٩٩٩ وكانت فكرة الموقع أن المجتمع يحتاج إلى مكان للالتقاء وتبادل الحكمة والمعرفة التي تم جمعها ويركز على عدد قليل من المجالات الرئيسية ذات الأهمية القصوى للمجتمع الأمني يوفر الموقع ٣١ قائمة بريدية لمناقشة جميع المسائل الأمنية ، ويهدم إعلانات مفصلة عن الثغرات الأمنية ، وقاعدة بيانات نقاط الضعف لجميع المنصات والخدمات.

٢. **SecuriTeam** [٥] موقع يحمى ويكشف عن الثغرات في المواقع والبرامج وأنظمة التشغيل ويقدم أحدث الأخبار والمرافق في أمن الكمبيوتر.

٣. **jaascois** [٦]موقع عربى متخصص في أمن المعلومات والمسح الأمني للمواقع وتحليل الثغرات وتعليم فنون الاختراق

٥- **SecurityReason** [٧]: موقع بولندي موقع يهتم بذكر أخر الثغرات والفيروسات والتركيز على أهداف الثغرة

٦- **The Linux Kernel Archives**[٨] :موقع أمريكي متخصص في ثغرات وبرمجيات نظام Linux

٢/٤/٣ المحور الثالث : يتناول مواقع المختصة بتعليم الاختراق

مجال الاختراق يحتاج إلى تدريب مكثف، ولا يمكنك إجراء تجارب الاختراق على مواقع أو برامج أو تطبيقات فعلية وإلا لن تصبح مخترق أخلاقي ان صح التعبير ، إنما ستتحول من شخص يختبر اختراق

1 https://detectify.com/
2 https://app.webinspector.com/public/tasks/80128203
3 https://www.owasp.org
4 http://www.securityfocus.com
5 http://www.securiteam.com
6 www.jaascois.com
7 http://securityreason.com
8 http://www.kernel.org/

المواقع من أجل حماية أفضل الى شخاص يختبر اختراق المواقع من أجل استغلالها، و هو ما لا يجوز فعله ، ونجد أن اكتشاف الأخطاء Exploits أو الثغراتVulnerability في أحد المواقع و مراسلتهم ، فأنت تحصل على الألاف من الدولارات من أجل ذلك ، و الاف اخرى من أجل تصحيحها، ولذلك يوجد العديد من المواقع التى تمكنك من التدريب المكثف على الاختراق ونعرض أمثلة لأشهر هذه المواقع.

١. CTF365[1]:

يرمز لل CTF ب (Catch The Flag) و هي نمط بسيط يتبارز فيه مجموعة من الهاكرز إذ يجب على كل مجموعة محاولة اختراق السيرفر الخاص بالمجموعة الأخرى و أيضا حماية السيرفر الخاص بها ، تم تصميمه باحترافية تامة وكما انه مخصص لمحبي هذا العالم و الذين يريدون تطوير مهاراتهم في الاختراق بشكل عام، يمكن الدخول الى الموقع والتسجيل فيه بشكل مجاني كمبتدئ و البدئ بالتدرب على اختراق بعض السيرفرات

٢. OverTheWire:[2]

موقع Overthewire هو موقع صمم لجميع المستخدمين من جميع المستويات و الخبرات ، سواء للمبتدئين أو المحترفين وهو مختص لتعلم المبادئ الأساسية في الحماية ، و يقدم أيضا مجموعة من الاختبارات الخاصة بالاختراق والحماية ، الجميل في الموقع انه ستمر بمراحل متعددة، اي يجب عليك اولا اتمام مهام بدائية في الأول بسيطة بالنسبة لك ان كنت مختصا في المجال ، و صعبة قليلا على المبتدئين ، و تجتاز مستويات اخرى بعدها حتى تتقن مجموعة من مبادئ الاختراق والحماية .

٣. Hacking Lab[3]

كما يدل إسم الموقع على خدماته ، موقع Hacking Lab يقدم لك مختبر اختراق جاهز للبدئ في تحديات الحماية الخاص بك ، ايضا يقدم الموقع تحدي CTF الذي شرحناه من قبل ، ما يميز هذا الموقع ، انه ينظم مسابقات محلية و دولية خاصة بالحماية و الاختراق و لك كامل الحرية للاشتراك و التسجيل فيها ، لكن يجب عليك اولا ان تتقن المبادئ المطلوبة ، كل ما يجب عليك فعله هو الدخول الى الموقع و تسجيل حساب مجاني.

٤. Hack This Site:[4]

هل انت قادر على اختراق هذا الموقع ؟ حسنا ، موقع Hack This Site هو موقع يمكنك التسجيل فيه بشكل مجاني من اجل توسيع مداركك في مجال الاختراق ، يضم العديد من التحديات و المهمات الخاصة بالاختراق في مجموعة من الأقسام منها اختراق البرامج او اختراق المواقع و الForensic (و التي سأكتب عنها مقالا المرة المقبلة لأهميتها) ، و أيضا بعض الدروس في البرمجة ، و لأكون واقعيا معك ، فأنت تحتاج البرمجة في جميع الأحوال من أجل اجتياز تلك المهام ، من جهة أخرى ، فهذا الموقع يضم أيضا مجموعة من المواضيع و المقالات و الشروحات في مجال الاختراق و الحماية ، و منتدى خاص بالموقع أيضا من اجل مشاركة مواضيع الاختراق و الحماية ، كما ان الموقع قد أعلن عن بعض الأمور الجديدة التي سيتم إضافتها للموقع ، لذلك ، فإن هذا الموقع أفضل موقع يمكنك متابعته الى حد الآن لكونه شامل و متجدد ايضا .

1 https://ctf365.com/
2 https://www.hacking-lab.com/index.html
3 https://www.hacking-lab.com/index.html
4 https://www.hackthissite.org/

ثالثاً : خطوات تطبيق الدراسة

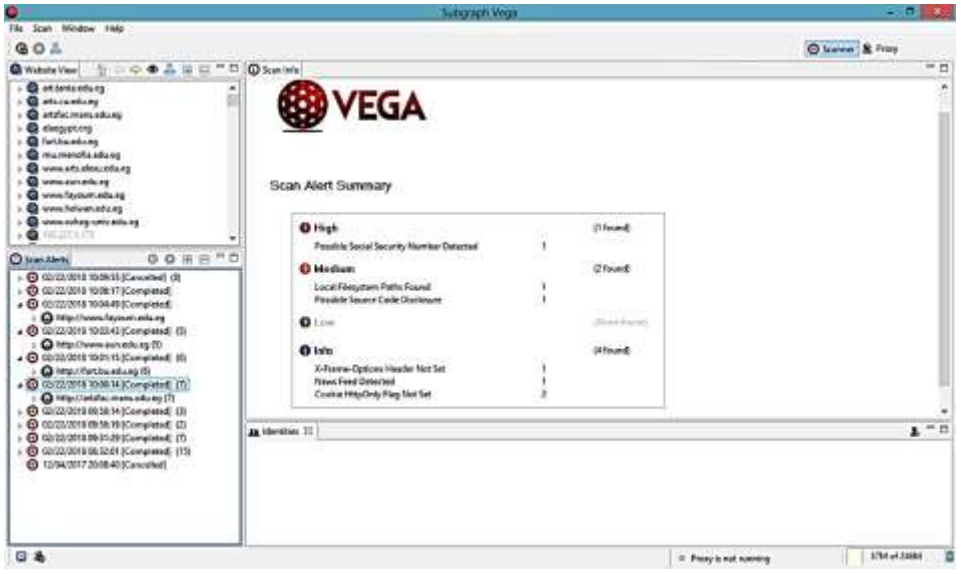
١- اختيار برنامج اختبار الاختراق الأمني لمواقع اقسام المكتبات والمعلومات على الانترنت
٢- تحديد مواقع اقسام المكتبات والمعلومات وفقا للشروط السابق ذكرها في مجتمع الدراسة
٣- تشغيل برنامج Vega لأجراء اختبار الاختراق

٣/١ اختيار برنامج اختبار الاختراق الأمني لمواقع اقسام المكتبات والمعلومات على الانترنت

بعد العرض السابق لمواقع وبرامج اختبار الاختراق لتطبيقات الويب وفحصها تم اختيار برنامج Vega لأجراء اختبار الاختراق لمواقع أقسام المكتبات والمعلومات على الانترنت كنموذج لبرامج تطبيق اختبار الاختراق ولما يتميز البرنامج من أنه يوجد منه نسخة تعمل على بيئة الويندوز الأكثر انتشارا واستخداما ، وسهل التحمل على الحاسب الآلي، ولا يحتاج إلى أى متطلبات أو إجراءات أضافة، وأنه مجانى، وسريع فى فحص المواقع، وسهل الاستخدام، وهو قوى بما فيه الكفاية لغرض هذه الدراسة ويحتوى على الاختبارات (*)الآتية :

١- اختبارات حقن البيانات injection modules ويضم ١٨ اختبار
٢- اختبارات معالجة الاستجابة response processing modules ويضم ٢٨ اختبار

بعد نجاح تنزيل هذا المنتج وتثبيته على جهاز كمبيوتر، بدأت عملية مراجعة استخدام البرنامج حيث كان من السهل أجراء الاختبار وتحديد اختياراته وإنتاج تقرير شامل بالثغرات الأمنية سهل القراءة و يحدد التقرير مكان الثغرة وأثارها السلبية وطرق إصلاحها حيث لا يحتاج البرنامج سوى URL الخاص بالموقع يعرض الشكل التالى شاشة البرنامج بعد إجراء اختبار الفحص لأحد المواقع



شكل رقم (١) شاشة تقرير اختبار برنامج Vega

* ملحق اختبارات برنامج Vega

٣/٢ تحديد مواقع اقسام المكتبات والمعلومات المصرية لإجراء الاختبار تم تحديد ثمانية عشر قسماً لها مواقع على الأنترنت

٣/٣ تشغيل برنامج Vega لأجراء اختبار الاختراق

لتحقيق أغراض هذه الدراسة تم تحميل برنامج Vega نسخة مجانية تعمل تحت بيئة ويندوز وتم تثبيته على جهاز الحاسب الآلي ، يتم إدخال URL(Uniform Resource Locator) الخاص بكل قسم من أقسام المكتبات والمعلومات مربع الفحص فى البرنامج، ومن ثم يبدأ البرنامج عملية فحص الموقع، ويستغرق الفحص ما بين ١٥ دقيقة و ساعتان يتوقف ذلك على حجم الموقع وعدد الصفحات وعدد الثغرات الأمنية الموجودة فى الموقع وسرعة الأنترنت .

بعد انتهاء عملية فحص الموقع يظهر تقرير بالثغرات الموجودة بالموقع مقسمة وفقا لدرجة خطورتها إلى الفئات التالية :

- **خطورة عالية** : مشاكل حادة لها تداعيات خطيرة على أمن تطبيقات الويب ويمكن أن تؤدى إلى وقوع أضرار أو احتمال وقوع هجمات، و يجب أن تأخذ هذه القضايا الأسبقية عند وضع جدول زمني للتصحيح.
- **خطورة متوسطة** : مشاكل متوسطة الخطورة ، و يجب تصحيحها ، ولكن بعد إصلاح المشكلات عالية المستوى.
- **منخفضة الخطورة**: مشاكل أمنية خطورتها منخفضة، ورغم ذلك يجب إصلاحها.
- **المعلوماتية**: عبارة عن رسائل لا تشكل مشكلة أو خطر يذكر ولكن يجب مراجعتها ومعالجاتها من قبل مطوري تطبيقات الويب

رابعاً : تحليل النتائج

بعد الانتهاء من فحص مواقع أقسام المكتبات والمعلومات عينة الدراسة باستخدام برنامج Vega تم تحليل التقارير التى يصدرها البرنامج لكل موقع حيث يعرض التقرير عدد الثغرات وأنواعها ودرجة خطورتها لك قسم من عينة الدراسة وذلك للخروج بنتائج الدراسة ومناقشتها كما يأتي :

جدول رقم (١) عدد الثغرات الأمنية فى أقسام المكتبات والمعلومات المصرية

			درجة الخطورة					
م	الجامعة	القسم	عالية	متوسطة	منخفضة	معلومات	المجموع	النسبة
١	المنوفية	المكتبات والمعلومات	8	-	1	6	15	%18
٢	سوهاج	المكتبات والمعلومات	2	-	-	6	8	%10
٣	اسكندرية	المكتبات والمعلومات	2	-	1	4	7	% 8

م	الجامعة	القسم	درجة الخطورة				المجموع	النسبة
			عالية	متوسطة	منخفضة	معلومات		
٤	الأزهر بأسيوط	كلية اللغة العربية-الوثائق والمكتبات	1	1	-	5	7	%8
٥	المنصورة	الوثائق والمكتبات والمعلومات	1	2	-	4	7	%8
٦	قناة السويس	المكتبات والمعلومات	5	-	-	2	7	%8
٧	بنها	المكتبات والمعلومات	1	1	1	3	6	%7
٨	أسيوط	المكتبات والوثائق والمعلومات	-	-	1	4	5	%6
٩	الأزهر بالقاهرة	الوثائق والمكتبات كلية الدراسات الإنسانية	1	-	1	2	4	% 5
١٠	عين شمس	المكتبات والمعلومات	2	-	1	1	4	%5
١١	القاهرة	المكتبات والوثائق والمعلومات	1	1	-	1	3	% 4
١٢	بنى سويف	قسم علوم المعلومات	1	-	-	1	2	%2
١٣	طنطا	الوثائق والمكتبات	-	-	-	2	2	%2
١٤	قنا	المكتبات والمعلومات	-	-	1	1	2	%2
١٥	كفر الشيخ	المكتبات والمعلومات	-	-	1	1	2	%2
١٦	الفيوم	الوثائق والمكتبات	-	-	-	1	1	%1

م	الجامعة	القسم	درجة الخطورة				المجموع	النسبة
			عالية	متوسطة	منخفضة	معلومات		
١٧	حلوان	المكتبات والمعلومات	-	-	-	1	1	%1
١٨	دمياط	المكتبات والمعلومات	٠	٠	٠	٠	٠	٠%
			٢٥	٥	٨	٤٥	٨٣	١٠٠

نلاحظ من الجدول السابق ما يأتي:

- أن موقع قسم المكتبات والمعلومات جامعة المنوفية يوجد به أكبر عدد من الثغرات الأمنية حيث يوجد به ١٥ ثغرة أمنية بنسبة ١٨ % من إجمالي الثغرات الأمنية بمواقع المكتبات والمعلومات عينة الدراسة من بينها ٨ ثغرات عالية الخطورة وثغرة واحدة منخفضة الخطورة و٦ معلومات لا تشكل خطورة ولكن يجب إصلاحها.
- موقع قسم الوثائق والمكتبات جامعة دمياط الموقع الوحيد الذى لا يوجد به ثغرات أمنية

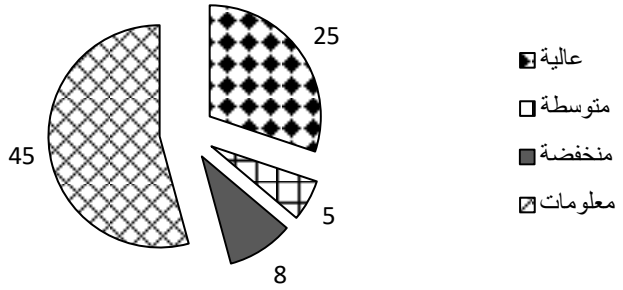
ويرجع الباحث ذلك إلى :

١- أن مطورين موقع قسم المكتبات والمعلومات جامعة دمياط ذو كفاء عالية في تصميم المواقع.
٢- يستخدم موقع قسم المكتبات والمعلومات جامعة دمياط أجهزة حماية الموقع من الاختراق
٣- قسم المكتبات والمعلومات جامعة المنوفية يوجد العديد من العيوب والخطاء في تصميم وبناء وبرمجة الموقع مما أدى إلى العديد من الثغرات الأمنية

جدول (٢) درجة خطورة الثغرات الأمنية وتكرارها

درجة الخطورة	عدد المكررات	النسبة
عالية	٢٥	%٣٠
متوسطة	٥	%٦
منخفضة	٨	%١٠
معلومات	٤٥	%٥٤
المجموع	**٨٣**	**%١٠٠**

عدد المكررات



شكل (٢) درجة الخطورة وتكرارها

من الجدول والشكل السابق يتضح أن مواقع أقسام المكتبات والمعلومات المصرية تعانى من ٨٣ ثغرة أمنية من بينها ٢٥ ثغرة عالية الخطورة بنسبة ٣٠ % وتحتل ثغرات" المعلومات" النسبة الأكبر من المخاطر الأمنية الموجودة بالمواقع حيث يبلغ عددها ٤٥ ثغرة بنسبة ٥٤ % ونستنتج من ذلك أن نسبة الثغرات الأمنية على اختلاف درجة خطورتها تبلغ ٤٦ % وهذه نسبة مرتفعة جدا من المخاطر الأمنية التى تهدد مواقع اقسام المكتبات والمعلومات لأن وجود نسبة ١ % فقط من المخاطر والثغرات الأمنية يمكن أن يتسبب بضرر شديد بالمواقع فما بالك بوجود ٤٦ % من المخاطر والثغرات التى تهدد مواقع أقسام المكتبات ويرجع الباحث ذلك لوجود العديد من الأخطاء فى برمجة مواقع أقسام المكتبات والمعلومات

جدول (٣) نتيجة اختبار الثغرات الأمنية لمواقع أقسام المكتبات والمعلومات المصرية

قضايا الثغرات	درجة الخطورة				المجموع
	عالية	متوسطة	منخفضة	معلومات	
مجموع الثغرات لجميع المواقع	25	5	8	45	83
متوسط عدد الثغرات لكل موقع	1	0.3	0.4	3	5
عدد أنواع الثغرات لكل المواقع	9	3	3	9	24
متوسط أنواع الثغرات لكل موقع	0.5	0.2	0.2	0.5	1.3
عدد المواقع التى لا يوجد بها ثغرات	7	13	9	0	29

يتضح من الجدول السابق ما يلى :

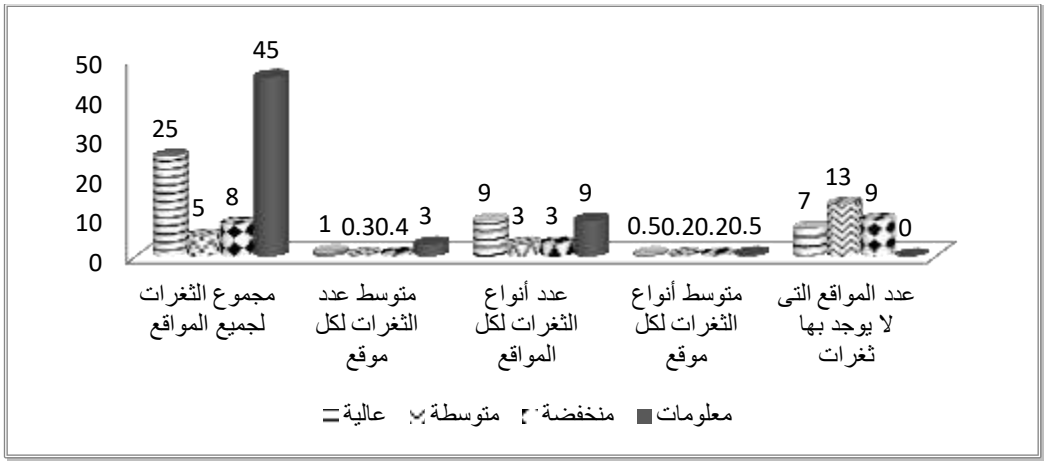
- عدد الثغرات الأمنية عالية الخطورة ٢٥ ثغرة بمتوسط عدد ١ ثغرة لكل موقع، وعدد الثغرات متوسطة الخطورة ٥ ثغرات بمتوسط ٠,٣ من الثغرة واحدة لكل موقع، وعدد الثغرات منخفضة الخطورة ٨ ثغرات بمتوسط٠,٤ من الثغرة لكل موقع، وعدد ٤٥ ثغرة معلومات بمتوسط ٣ ثغرات لكل موقع ، والعدد الإجمالي للثغرات لكل المواقع ٨٣ ثغرة بمتوسط ٥ ثغرات لكل موقع.
- عدد أنواع الثغرات الأمنية عالية الخطورة ٩ نوع بمتوسط ٠,٥ نوع لكل موقع، وعدد أنواع الثغرات متوسطة الخطورة ثلاثة أنواع بمتوسط ٠,٢ نوع لكل موقع، وعدد أنواع الثغرات منخفضة الخطورة

٣ أنواع بمتوسط ٠,٢ نوع لكل موقع، وعدد أنواع الثغرات المعلوماتية ٩ بمتوسط ٠,٥ نوع لكل موقع، وعدد أنواع الثغرات لكل المواقع ٢٤ نوع بمتوسط ١,٣ نوع لكل موقع.

- ٧ مواقع لا يوجد بها ثغرات عالية الخطورة، و ١٣ موقع لا يوجد به ثغرات متوسطة الخطورة ، و٩ مواقع لا يوجد بها ثغرات منخفضة الخطورة، ولا يوجد موقع يخلوا من الثغرات الأمنية المعلوماتية.

نستنتج مما سبق ما يلى :

- كل مواقع أقسام المكتبات والمعلومات المصرية يوجد بها ثغرات أمنية معلوماتية وهذه الثغرات لا تشكل تهديدا أمنيا ولكن يجب إصلاحها حتى لا تستخدم فيما بعد .
- يوجد ٢٤ نوع من الثغرات فى مواقع أقسام المكتبات والمعلومات المصرية منها ٩ أنواع عالية الخطورة وثلاثة أنواع متوسطة الخطورة وثلاثة أنواع منخفضة الخطورة و٩ انواع معلوماتية
- أكبر عدد من الثغرات التى توجد بمواقع أقسام المكتبات والمعلومات المصرية ٤٥ ثغرة معلومات وأقل عدد خمسة ثغرات متوسطة الخطورة .
- أكبر عدد من أنواع الثغرات التى توجد بمواقع أقسام المكتبات والمعلومات المصرية ٩ ثغرة عالية الخطورة و٩ أنواع ثغرات معلوماتية وأقلها ثلاثة أنواع ثغرات متوسطة ومنخفضة الخطورة



شكل(٣) **نتيجة اختبار الثغرات الأمنية لمواقع أقسام المكتبات والمعلومات المصرية**

جدول (٤)أنواع الثغرات مرتفعة الخطورة

م	نوع الثغرة	التكرار	نسبة عدد الثغرات	عدد الأقسام لكل ثغرة
1	Shell Injection	8	32 %	2
2	Session Cookie Without Secure Flag	5	20 %	5
3	Possible Social Security Number Detected	3	12 %	3
4	Session Cookie Without HttpOnly Flag	2	8 %	2

م	نوع الثغرة	التكرار	نسبة عدد الثغرات	عدد الأقسام لكل ثغرة
5	Page Fingerprint Differential Detect-possible Xpath Injection	2	8 %	2
6	Integer Overflow	2	8 %	1
7	Possible Social Insurance Number Detected	1	4 %	1
8	Page Fingerprint Differential Detect-possible Local File Include	1	4 %	1
9	Clear text Password over HTTP	1	4 %	1
		25	مجموع	18

يتضح من الجدول السابق ما يلى :

- نجد أن ثغرة **"حقن الأوامر"** تتكرر ٨ مرات فى موقعين فقط وتمثل ٣٢ % من إجمالي الثغرات عالية الخطورة وتتمثل خطورة هذه الثغرة فى أن المخترق من خلال استغلال هذه الثغرة يستطيع تنفيذ أوامر يتحكم من خلالها بخادم الويب عن بعد بالإضافة إلى استغلال هذه الثغرة بشكل أخطر وأكبر عن طريق جلب وتحميل ملفات من مواقع اخرى ، وجلب ملفات من داخل السيرفر واستكشاف محتويات الملف الذي يتصل مع قاعدة البيانات والحصول على بيانات القاعدة من اسمها وبيانات الدخول عليها و السيطرة على جميع المعلومات الموجودة على الخادم .

طريقة إصلاحها

لكى يتمكن مطور تطبيقات الويب من التغلب على هذه الثغرة يجب اتباع ما يلى :

- الفحص الدقيق للتعليمات البرمجية لصفحات الويب لتأكد إذا كانت الثغرة موجودة أم لا.
- يجب تجنب تنفيذ أوامر النظام من خلال مترجم الأوامر، و إذا كان ذلك ضروريًا ،يجب أن يأخذ المطور مزيدًا من الحذر مع التحقق من صحة المدخلات قبل تمريرها إلى المترجم.

- ثغرة **"ملف تعريف ارتباط جلسة العمل بدون علامة آمنة"** تتكرر ٥ مرات بنسبة ٢٠ % من إجمالي الثغرات عالية الخطورة فى ٥ مواقع وتتمثل خطورة هذه الثغرة فى أن ملفات تعريف الارتباط الخاصة بالجلسات هي بيانات اعتماد المصادقة حيث يمكن للمهاجمين الذين يحصلون عليها تحقيق وصول غير مصرح به إلى تطبيقات الويب.

طريقة إصلاحها

يجب على مطور الويب عند إنشاء ملف تعريف الارتباط في التعليمة البرمجية ، تعيين العلامة الآمنة على true

- ثغرة "وجود رقم الضمان الاجتماعي" تتكرر ثلاثة مرات فى ثلاثة مواقع بنسبة ١٢ % من إجمالى الثغرات عالية الخطورة وتتمثل خطورة هذه الثغرة فى أن الكشف غير المصرح به لهذه المعلومات يمكن أن يؤدي إلى الاحتيال ، أو سرقة الهوية

طريقة إصلاحها

- يجب التحقق من ذلك لتحديد طبيعة البيانات التي تتطابق مع نمط الاكتشاف.

- قد يكون السبب الأساسي للكشف عن البيانات قاعدة بيانات ملف مسطح أو تشغيل بعض الثغرات الأمنية غير المتوقعة.

- ثغرة " ملف تعريف ارتباط جلسة العمل بدون علامة آمنة على HttpOnly " تتكر مرتان فى موقعين بسنة ٨% من إجمالى الثغرات عالية الخطورة وتتمثل خطورة هذه الثغرة فى أنه عند عدم وجود هذه العلامة، من الممكن الوصول إلى ملف تعريف الارتباط عبر رمز البرنامج النصي من جانب العميل حيث أن تنشيط HttpOnly هو إجراء أمان يمكن أن يساعد في تخفيف مخاطر الهجمات النصية عبر المواقع التي تستهدف ملفات تعريف الارتباط للجلسة الضحية. إذا تم تعيين علامة HttpOnly وكان المستعرض يدعم هذه الميزة ، فلن يتمكن رمز البرنامج النصي الموفر من قِبل المهاجم من الوصول إلى ملف تعريف الارتباط.

طريقة إصلاحها

يجب على مطور الويب عند إنشاء ملف تعريف الارتباط في التعليمة البرمجية ، تعيين علامة HttpOnlyإلىtrue

- ثغرة " بصمة صفحة استجابة مختلفة فيما يتعلق بطلب حقن المسار XPath " تتكرر مرتان فى موقعين بنسبة ٨% من إجمالى الثغرات عالية الخطورة وتعنى هذه الثغرة أن محتوى صفحة الرد الذي يتم إرجاعه بواسطة تطبيق الويب له توقيع مختلف عن ذلك الذي تم إرجاعه بواسطة الطلب العادي ، وهو ما قد يشير إلى وجود ثغرة أمنية في المسار XPath ، و قد تتضمن بصمة الصفحة المختلفة رسائل خطأ أو تشير إلى تغيير حالة في التطبيق استجابة لمحاولة حقن المسار.

وتكمن خطورة هذه الثغرة فى أنها تمكن المهاجمين من تجاوز المصادقة أو الوصول غير المصرح به إلى بيانات XML الحساسة.

طريقة إصلاحها

يجب على المطور التفكير في استخدام عبارات XPath التي تم ترجمتها مسبقًا ، والتفكير فى خيارات الاستعلام

- ثغرة **"تجاوز عدد صحيح "** تتكرر مرتان فى موقع واحد بنسبة ٨% من إجمالى عدد الثغرات عالية الخطورة وتعنى أنه عندما تتجاوز أنواع البيانات الصحيحة قيمتها القصوى ، يمكن أن يكون للسلوك الناتج انعكاسات أمنية. وفي هذه الحالات ، سيتم تقليل الأعداد الصحيحة إلى قيمة رقمية أقل. وتكمن خطورة ذلك فى كيفية استخدام القيمة الصحيحة حيث إذا تم استخدمها كحجم مؤقت لتخزين البيانات ، فقد يؤدي إجباره على الالتفاف إلى قيمة أقل إلى تجاوز عمليات فحص الحجم ، مع إدخال شروط تجاوز سعة المخزن المؤقت المحتملة و أيضا مكن أن تحتوي أخطاء تجاوز السعة الصحيحة على مجموعة متنوعة من التأثيرات ، وفقًا للسياق والغرض من القيمة الصحيحة.

طريقة إصلاحها

يجب على المطور التحقيق من الخطأ وتحديد وجود ثغرة أمنية.

- ثغرة " **وجود رقم التأمين الاجتماعي** " توجد مرة واحدة فى موقع واحد نسبة ٤ % من إجمالى الثغرات عالية الخطورة وتتمثل خطورة هذه الثغرة فى أن الكشف غير المصرح به لهذه المعلومات يمكن أن يؤدي إلى الاحتيال ، أو سرقة الهوية

طريقة إصلاحها

- يجب التحقق من ذلك لتحديد طبيعة البيانات التي تتطابق مع نمط الاكتشاف.
- قد يكون السبب الأساسي للكشف عن البيانات قاعدة بيانات ملف مسطح أو تشغيل بعض الثغرات الأمنية غير المتوقعة.

- ثغرة **"بصمة صفحة استجابة مختلفة فيما يتعلق بتضمين بملف محلي "** تتكرر مرة واحدة فى موقع واحد بنسبة ٤ % من إجمالى الثغرات عالية الخطورة وتعني أن محتوى صفحة الرد الذي يتم إرجاعه بواسطة تطبيق الويب له توقيع مختلف عن ذلك الذي تم إرجاعه بواسطة طلب عادي ، مما قد يشير إلى أن وجود ملف محلي يشتمل على ثغرة أمنية ، قد تكون الاستجابات المتفاوتة دالة على وجود ثغرة في تعداد الملفات ، مما يسمح للمهاجم بتحديد ما إذا كانت هناك ملفات محددة على النظام أم لا.

تكمن خطورة هذه الثغرة فى السماح للمهاجمين بالوصول غير المصرح بـه إلـى المعلومـات الحساسـة الموجودة في الملفات المحلية ، والتي يمكن أيضًا الاستفادة منها في مزيد من الهجمات على تطبيق الويب.

طريقة إصلاحها

- يجب على المطور تحديد مسار أي مورد نظام ملفات يحتوي على مسار يتكون من مدخلات تم توفيرها خارجيًا ثم إجراء فحص تفويض قبل الوصول.
- يجب استخدام آليات للحد من الوصول غير المصرح به إلى نظام ملفات تطبيقات الويب

- ثغرة **" وجود حقل إدخال كلمة مرور عبر** HTTP **"** تتكرر مرة واحدة فى موقع واحد بنسبة ٤% من إجمالى الثغرات عالية الخطورة حيث أن وجود حقل إدخال كلمة مرور يتم إرساله إلى هدف غير آمن عبر HTTP قد ينتج عن ذلك الكشف عن كلمات المرور إلى مهاجمين الشبكة.

طريقة إصلاحها

يجب ألا يتم إرسال كلمات المرور مطلقًا عبر النص الواضح.
يجب عدم إرسال قيم كلمة المرور مطلقًا عبر القنوات غير الآمنة.

جدول (٥)أنواع الثغرات متوسطة الخطورة

م	نوع الثغرة	عدد الثغرات	نسبة عدد الثغرات	عدد الأقسام لكل ثغرة	النسبة عدد الأقسام
1	Local Filesystem Paths Found	3	60 %	3	17%
2	HTTP Trace Support Detected	1	20 %	1	6 %
3	Possible Source Code Disclosure	1	20 %	1	6 %
		5	100 %	5	المجموع

- ثغرة **" العثور على مسارات ملفات النظام"** تتكرر ثلاثة مرات فى ثلاثة مواقع بنسبة ٦٠ % من إجمالى الثغرات متوسطة الخطورة وهذه المعلومات حساسة، لأنها قد تكشف أشياء عن بيئة خادم الويب للمهاجمين، وايضا معرفة مسار ملفات النظام يزيد من فرص نجاح الهجمات العمياء

طريقة إصلاحها :

- ممكن أن تكون المشكلة بسبب خطأ في التطبيق أو خطأ في تهيئة خاد الويب .

- لا يجب إرسال مخرجات الأخطاء التي تحتوي على معلومات حساسة مثل مسارات ملفات النظام إلى العملاء البعيدين عن خوادم الويب .

- ثغرة "اكتشاف دعم تتبع HTTP " تتكرر مرة واحدة فى موقع واحد بنسبة ٢٠ % من إجمالى الثغرات متوسط الخطورة وهى أسلوب يطلب من خادم الويب إرسال تتبع HTTP مرة أخرى إلى العميل حيث قد يتمكن المهاجمون من استخدام التتبع عبر الموقع مع وجود ثغرة البرمجة النصية عبر المواقع من استرداد قيمة ملفات تعريف الارتباط

طريقة الإصلاح

يجب تعطيل خاصية TraceEnabl بالنسبة لخوادم الويب وذلك لتعطيل دعم تتبع HTTP

- ثغرة " إفشاء مصدر الكود" تتكرر مرة واحدة فى موقع واحد بنسبة ٢٠ % من إجمالى ثغرات المواقع متوسطة الخطورة حيث يمكن أن تكون هذه التعليمات البرمجية لمصدر الكود مرئية بشكل غير مقصود للعملاء البعدين ويحدث هذا في التطبيقات التي تستخدم تقنيات مثل PHP و JSP ، والتي تسمح بأن يتم خلط الشفرة مع محتوى العرض التقديمي الثابت. على سبيل المثال ، يتم التعليق أحيانًا على التعليمات البرمجية المضمنة باستخدام تعليقات HTML ، مما يؤدي إلى إرسالها إلى العملاء البعيدين. بالنسبة للمهاجم ، يمكن أن تكشف شفرة المصدر معلومات عن طبيعة التطبيق ، مثل تصميمه ، و سلسلة اتصال قاعدة البيانات ، و مثل كلمات المرور

طريقة إصلاحها

يجب على المطور التحقق من أن المخرجات التي تم اكتشافها هي في الحقيقة شفرة مصدر تطبيق ومن ثم تحديد السبب فى ذلك، وإزالة المادة أو منعها من الظهور .

جدول (٦)أنواع الثغرات منخفضة الخطورة

م	نوع الثغرة	عدد الثغرات	نسبة عدد الثغرات	عدد الأقسام لكل ثغرة	النسبة عدد الأقسام
1	Email Addresses Found	6	75 %	6	33 %
2	ASP/ASPX Error Detected	1	12.5 %	1	6 %
3	Form Password Field with Autocomplete Enable	1	12.5 %	1	6 %
		8	100%	8	المجموع

- ثغرة " إيجاد عناوين البريد الإلكتروني " تتكرر ٦ مرات فى ٦ أقسام بنسبة ٧٥ % من إجمالى الثغرات منخفضة الخطورة حيث الكشف عن أنماط تشبه عناوين البريد الإلكتروني قد تكون هذه عناوين المستخدمين للنظام ، أو العناوين المدرجة في المحتوى المقدم من قِبل المستخدم ، أو عناوين الجهات الخارجية المضمنة في مكونات التطبيق وتكمن الخطورة فى ذلك حيث يتم إضافة عناوين البريد الإلكترونية هذه إلى قوائم البريد العشوائي وأيضا استخدمها في هجمات الاستهداف و التصيد الاحتيالي وأيضا لتخمين أسماء المستخدمين بشكل أكثر دقة.

طريقة إصلاحها

- إذا كانت عناوين البريد الإلكتروني هي تلك الخاصة بالمستخدمين ، فيجب على المطورين التحقق من سبب إخراجهم ومحاولة إزالتها أو تشويشها.
- يوصى بعدم عرض عناوين البريد الإلكتروني على الأجزاء المكشوفة من تطبيق الويب ، بشكل مباشر أو غير مباشر.
- هناك احتمال آخر وهو أن الخادم قد تم تهيئته تلقائيًا ليشمل عناوين البريد الإلكتروني. فيجب إزالة ذلك .

- ثغرة " رسالة خطأ مرتبطة بإطار Microsoft ASP / ASP.NET " تتكرر مرة واحدة فى موقع واحد بنسبة ١٢,٥ من إجمالى الثغرات منخفضة الخطورة حثيث اكتشاف رسائل خطأ حول لغة البرمجة المستخدمة فى موقع الويب وتكمن خطورة ذلك فى الكشف عن معلومات حساسة حول التطبيق الذي يمكن أن يساعد في هجمات أكثر تعقيدًا وقد يكون رسالة الخطأ مؤشرا على وجود ثغرة أمنية.

طريقة إصلاحها

- يجب على المطور التحقق من رسائل الخطأ والتأكد من أنها لا تمثل نقطة ضعف.
- تعطيل رسائل الخطأ للمستخدمين عن بعد.
- تهيئة خادم الويب لعرض رسائل خطأ آمنة لا تتضمن معلومات حساسة.

- ثغرة " نموذج حقل إدخال كلمة المرور بشكل تلقائيا" تتكرر مرة واحدة فى قسم واحد بنسبة ١٢,٥ % من إجمالى الثغرات منخفضة الخطورة حيث اكتشاف نموذجًا يتضمن حقل إدخال كلمة المرور ولم يتم إيقاف خاصية autocomplete فقد يؤدي ذلك إلى قيام بعض المتصفحات بتخزين قيم المدخلات من قِبل المستخدمين محليًا وتكمن الخطورة فى إمكانية استرداد كلمات المرور المخزنة محليًا من قِبل مستخدمين آخرين

طريقة إصلاحها

يجب ضبط خاصية autocomplete على قيمة OFF

جدول (٧) أنواع ثغرات المعلومات

م	نوع الثغرة	عدد الثغرات	نسبة عدد الثغرات	عدد الأقسام لكل ثغرة	نسبة عدد الأقسام
1	X-Frame-Option Header Not Set	28	62 %	17	94 %
2	Interesting Meta tags Detected	5	11 %	4	22 %
3	News Feed Detected	5	11 %	4	22 %
4	Cookie HttpOnly Flag Not Set	2	4.4%	1	6 %
5	Character Set Not Specified	1	2.2 %	1	6 %
6	HTTP Error Detected	1	2.2 %	1	6 %

م	نوع الثغرة	عدد الثغرات	نسبة عدد الثغرات	عدد الأقسام لكل ثغرة	نسبة عدد الأقسام
7	Possible AJAX code detected	1	2.2 %	1	6 %
8	Unsafe Or Unrecognized Character Set In Response Body	1	2.2 %	1	6 %
9	Unsafe Or Unrecognized Character Set In Response Header	1	2.2 %	1	6 %
		45		31	المجموع

- ثغرة **" عدم وجود خيار رأس الإطار "** تتكرر ٢٨ مرة فى ١٧ مواقع بنسبة ٦٢ % من إجمالى ثغرات المعلومات حيث يتيح هذا الرأس تحديد إذا كان يمكن تضمينه في إطارات في نطاقات أخرى وكذلك النطاقات المسموح بها، وعند تعيين الرأس، قد يساعد هذا في التخفيف من هجمات النقر فوق المتصفحات التي تدعم هذه الميزة

طريقة الإصلاح

عيّن رأس X-Frame-Options

- ثغرة **" اكتشاف العلامات الوصفية المثيرة للاهتمام"** تتكرر ٥ مرات فى ٤ مواقع بنسبة ١١ % من إجمالى ثغرات المعلومات حيث اكتشاف علامات وصفية قد تكشف عن معلومات حساسة أو تتطلب فحصًا دقيقًا حيث يمكن أن تتضمن هذه العلامات معلومات مثل خصائص النظام الأساسي أو تكوين التطبيق حيث قد تساعد المعلومات حول التطبيق التي يتم الكشف عنها دون داع في محتوى الصفحة في الاستغلال الناجح لهجمات أكثر تطوراً.

طريقة إصلاحها

يجب مراجعة العلامات الوصفية المضمنة في المحتوى لضمان عدم وجود شيء يمكن أن يساعد أحد المهاجمين.

- ثغرة " التغذية بالأخبار" تتكرر ٥ مرات فى ٤ مواقع بنسبة ١١ % من إجمالى ثغرات المعلومات حيث خدمة متابعة الأخبار بشكل مباشر RSS والتنسيقات ذات الصلة هي طرق لنشر محتوى ويب يتم تحديثه بانتظام، و خلاصات RSS هي مستندات XML متاحة للتنزيل من قبل العميل ويتم تضمينها غالبًا في أنظمة إدارة المحتوى ، مثل المدونات.
- ثغرة " تعيين ملف تعريف الارتباط غير آمن" تتكرر مرتين فى موقع واحد بنسبة ٤,٤ % من إجمالى ثغرات المعلومات حيث وجود علامة HttpOnly هو إجراء أمان يمكن أن يساعد في تخفيف مخاطر الهجمات النصية عبر المواقع التي تستهدف ملفات تعريف الارتباط للجلسة الضحية.

طريقة إصلاحها

- عند إنشاء ملف تعريف الارتباط في التعليمة البرمجية ، قم بتعيين علامة HttpOnly إلى true.

- ثغرة" مجموعة حروف غير محددة" تتكرر مرة واحدة فى موقع واحد بنسبة ٢,٢ % من إجمالى ثغرات المعلومات حيث إذا لم يتم تحديد مجموعة الأحرف ، قد يقوم المتصفح بافتراضات حول مجموعة الأحرف استنادًا إلى المحتوى، وقد يمثل هذا مشكلة أمنية إذا كان المحتوى يتم إنشاؤه ديناميكيًا وينشأ من المستخدمين، وفي مثل هذه الحالة ، قد يستغل المستخدمون الخبيثون كيفية تفسير متصفحات معينة للأحرف للتسبب في عرض محتوى ضار.

طريقة إصلاحها
يحب تحديد مجموعة أحرف محددة جيدًا (مثل UTF-8) داخل نوع محتوى رأس الاستجابة أو نص الاستجابة.

- ثغرة " رسالة خطأ خاصة HTTP[١] " تتكرر مرة واحدة فى موقع واحد بنسبة ٢,٢ % من إجمالى ثغرات المعلومات حيث يجيب التحقيق من هذه الرسائل من خلال فحص الطلب والاستجابة تشير رسالة الخطأ إلى حدث غير معروف على الخادم قد يكون مقترنًا بمشكلة عدم الأمان أو التهيئة.

طريقة إصلاحها
يجب على المطور التحقيق في كيفية حدوث هذا الخطأ ولماذا وضمان عدم وجود ثغرة أمنية.

- ثغرة " اكتشاف كود AJAX " تتكرر مرة واحدة فى موقع واحد بنسبة ٢,٢ % من إجمالى ثغرات المعلومات حيث تشير AJAX إلى مجموعة من التقنيات المستخدمة لجعل تجربة المستخدم لتطبيقات الويب أكثر تفاعلية، و تتضمن وظيفة AJAX إرسال طلبات غير متزامنة ومعالجة ردودها باستخدام جافا سكريبت ، دون الحاجة إلى إعادة تحميل الصفحة.

وتكمن الخطورة فى اكتشف محتوى استخدام AJAX ، إلى وجود نقاط حقن محتملة قد توجد بها نقاط ضعف.

طريقة إصلاحها
يمكن أن تعرض واجهات AJAX الخلفية نقاط الضعف المحتملة ويجب تضمين الفحص اليدوي في أي تقييم شامل للأمان.

- ثغرة "مجموعة أحرف غير آمنة أو غير معروفة في جسم الاستجابة " تتكرر مرة واحدة فى موقع واحد بنسبة ٢,٢ % من إجمالى ثغرات المعلومات حيث وجود مجموعة أحرف غير آمنة أو غير معروفة في نص الاستجابة قد يتسبب هذا في حدوث سلوك غير متوقع اعتمادًا على كيفية تفسير المستعرض لمجموعة الأحرف وقد يمثل هذا مشكلة أمنية إذا كان المحتوى تم إنشاؤه ديناميكيًا وينشأ من المستخدمين، في مثل هذه الحالة ، قد يستغل المستخدمون الخبيثون كيفية تفسير متصفحات معينة للأحرف للتسبب في عرض محتوى ضار.

على سبيل المثال ، قد يتمكن أحد المهاجمين من تجاوز عامل تصفية برامج نصية عبر المواقع بتشفير حمولته الضارة في مجموعة أحرف بديلة ، والتي يمكن تنفيذها بناءً على كيفية تفسير المستعرض للمحتوى المشفر .

طريقة إصلاحها
حدد مجموعة أحرف محددة جيدًا (مثل UTF-8) داخل نوع محتوى رأس الاستجابة أو نص الاستجابة.

١ Hyper Text Transport Protocol ومعناه بالعربية بروتوكول نقل النص الفائق

- ثغرة " مجموعة أحرف غير آمن أو غير معروف في رأس الاستجابة " تتكرر مرة واحدة فى موقع واحد بنسبة ٢,٢ % من إجمالى ثغرات المعلومات حيث وجود مجموعة أحرف غير آمنة أو غير معروفة في عنوان الاستجابة قد يتسبب هذا في حدوث سلوك غير متوقع اعتمادًا على كيفية تفسير المستعرض لمجموعة الأحرف، وقد يمثل هذا مشكلة أمنية إذا احتوى المورد المتأثر على محتوى تم إنشاؤه ديناميكيًا وينشأ من المستخدمين، وفي مثل هذه الحالة ، قد يستغل المستخدمون الخبيثون كيفية تفسير متصفحات معينة للأحرف للتسبب في عرض محتوى ضار.

طريقة إصلاحها
حدد مجموعة أحرف محددة جيدًا (مثل UTF-8) داخل نوع محتوى رأس الاستجابة أو نص الاستجابة.

مما سبق نستنتج ما يلى :

- بالنسبة للثغرات عالية الخطورة تمثل ثغرة **"حقن الأوامر"** أعلى نسبة ٣٢ % و تتكرر ٨ مرات فى موقعين بينما أقل نسبة ٤ % لثغرات : **وجود حقل إدخال كلمة مرور عبر** HTTP ، **وجود رقم التأمين الاجتماعي ، بصمة صفحة استجابة مختلفة فيما يتعلق بتضمين بملف محلي "** ، وتتكرر مرة واحدة فى موقع واحد .
- بالنسبة للثغرات متوسطة الخطورة أعلى نسبة ٦٠ % لثغرة **" العثور على مسارات ملفات النظام"** و تتكرر ثلاثة مرات فى ثلاثة ، وأقل نسبة٢٠ % لثغرات **: إفشاء مصدر الكود ، اكتشاف دعم تتبع HTTP** وتتكرر مرة واحدة فى موقع واحد
- بالنسبة لثغرات منخفضة الخطورة أعلى نسبة ٧٥ % لثغرة **" إيجاد عناوين البريد الإلكتروني "** وتتكرر ٦ مرات فى ٦ أقسام ، وأقل نسبة ١٢,٥ % لثغرات **": نموذج حقل إدخال كلمة المرور بشكل تلقائيا ، رسالة خطأ مرتبطة بإطار** Microsoft ASP / ASP.NET حيث تتكرر مرة واحدة فى موقع .
- بالنسبة لثغرات المعلومات أعلى نسبة ٦٢ % لثغرة **عدم وجود خيار رأس الإطار** وتتكرر ٢٨ مرة فى ١٧ وأقل نسبة ٢,٢ % لثغرات : **مجموعة حروف غير محددة ، رسالة خطأ خاصة HTTP ، اكتشاف كود AJAX ، مجموعة أحرف غير آمنة أو غير معروفة في جسم الاستجابة، مجموعة أحرف غير آمن أو غير معروف في رأس الاستجابة** و تتكرر مرة واحدة فى موقع .

وفى نهاية تحليل الثغرات التى توجد بمواقع أقسام المكتبات والمعلومات المصرية يرجع الباحث وجود هذه الثغرات على اختلاف أنواعها و خطورتها إلى ما يأتي :

١. تدنى كفاءات ومهارات مطوري مواقع أقسام المكتبات والمعلومات المصرية حيث ان مطور الويب ذو الكفاء العالية يستطيع إصلاح ومعالجة ما يوجد بالموقع من ثغرات أمنية
٢. عدم استخدام أقسام المكتبات والمعلومات المصرية أجهزة أو برامج لحماية المواقع من الاختراق حيث وجود هذه الأجهزة والبرامج تخبر مسئول الموقع عن وجود أى تهدد أو ثغرات أمنية للموقع وبالتالي العمل على العلاج والإصلاح
٣. عدم تعاقد أقسام المكتبات والمعلومات المصرية مع الشركات المتخصصة فى حماية تطبيقات الويب من الاختراق لحماية مواقعها ومعالجة ما بها من ثغرات أمنية

نتائج الدراسة

- موقع قسم المكتبات والمعلومات جامعة المنوفية يوجد به أكبر عدد من الثغرة الأمنية بنسبة ١٨% من إجمالي الثغرات الأمنية بمواقع المكتبات والمعلومات
- تحتل ثغرات المعلومات ٥٤ % النسبة الأكبر من المخاطر الأمنية بينما تحتل الثغرات الأمنية عالية الخطورة ٣٠ % والمتوسطة الخطورة ٦% والمنخفضة الخطورة ١٠ % .
- ٩٤% من مواقع أقسام المكتبات والمعلومات المصرية يوجد بها ثغرات أمنية ، ٦ % فقط لا يوجد به أى ثغرة أمنية .
- يوجد ٢٤ نوع من الثغرات فى مواقع أقسام المكتبات والمعلومات المصرية منها ٩ أنواع عالية الخطورة وثلاثة أنواع متوسطة الخطورة وثلاثة أنواع منخفضة الخطورة و٩ انواع معلوماتية
- ثغرة **" إيجاد عناوين البريد الإلكتروني "** أعلى نسبة ٧٥ % النسبة لثغرات منخفضة الخطورة
- ثغرة **" عدم وجود خيار رأس الإطار"** أعلى نسبة ٦٢ % بالنسبة لثغرات المعلومات
- ثغرة **"العثور على مسارات ملفات النظام"** أعلى نسبة ٦٠ % بالنسبة للثغرات متوسطة الخطورة
- ثغرة **"حقن الأوامر"** أعلى نسبة ٣٢ % بالنسبة للثغرات عالية الخطورة

التوصيات

١- إنشاء برنامج مميز في المكتبات والمعلومات بعنوان " الأمن الرقمي للمكتبات والمعلومات" يدور هذا البرنامج حول المحاور الآتية :
- استخدام التكنولوجيا في تأمين مباني المكتبات ومراكز المعلومات
- تأمين وتشفير قواعد البيانات
- تأمين تطبيقات الويب
- بحوث الثغرات الأمنية وتطبيقات الاختراق
- تأمين شبكات المعلومات
- برامج الأمن المعلوماتي

٢- تقوم أقسام المكتبات والمعلومات والجمعية المصرية للمكتبات والمعلومات بتنظيم العديد من الدروات التدريبية عن تطبيقات أمن المعلومات في المكتبات والمعلومات مثل :
- دورة عن التشفير وخاصة تشفير قواعد البيانات والمعلومات .
- دورة عن التحقيق الجنائي الرقمي لاكتشاف انتهاك حقوق الملكية الفكرية.
- دورة عن اختراق تطبيقات الويب.
- دورة عن الهندسة الاجتماعية وتأثيرها على الأمن المعلوماتي الرقمي.
- دورة عن الهندسة العكسية وتأثيرها في معالجة مشاكل قواعد البيانات

٣- تقوم جمعية المكتبات والمعلومات المصرية بوضع سياسة واضحة لإجراءات الأمن والحماية لمواقع الويب في مجال المكتبات والمعلومات وذلك ليكون حماية المواقع نتيجة لسياسة واضحة وليست ردة فعلٍ لحدث معين وتتضمن السياسة العناصر الاتية :
- الشخص المسئول عن وضع السياسة وتنفيذها ومتابعتها بمؤسسات المعلومات.
- الإجراءات الوقائية لحماية المواقع من الاختراق.

- البرامج المستخدمة في الحماية من الاختراق.
- الدورات التدريبية اللازمة للقائمين بحماية المواقع من الاختراق.

٤- العمل على زيادة الوعى بأهمية أمن المعلومات وخطورة الثغرات الأمنية لدى كل من أعضاء هيئة التدريس والطلاب وأخصائي المكتبات والمعلومات ومتخذي القرار بالمؤسسات المعلوماتية وذلك بإقامة العديد من المحاضرات والندوات و ورش العمل حول أهمية أمن المعلومات وخطورة الثغرات الأمنية ، ويمكن وضع مقرر ضمن برامج أقسام المكتبات والمعلومات بعنوان" الوعى المعلوماتي الرقمي"

٥- تخصيص مقرر أو أكثر عن أمن المعلومات ضمن مقررات برامج أقسام المكتبات والمعلومات.

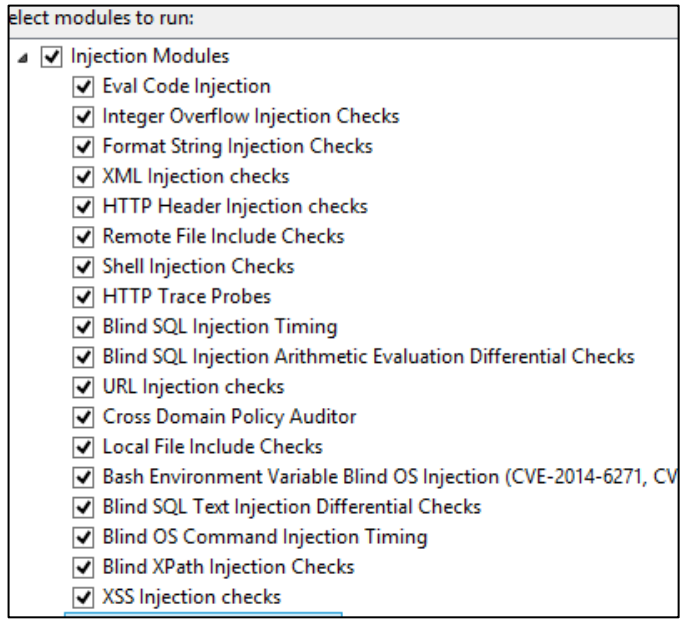
مواقع أقسام المكتبات المصرية

م	الفيس	الموقع
١	الوثائق والمكتبات- جامعة طنطا	http://art.tanta.edu.eg/laibrary/
٢	المكتبات والوثائق والمعلومات – جامعة القاهرة	http://arts.cu.edu.eg/index.aspx?id=80#
٣	الوثائق والمكتبات والمعلومات-جامعة المنصورة	http://artsfac.mans.edu.eg/sectors-ar/academic-departments/732-lib-dept
٤	المكتبات والمعلومات –جامعة بنها	http://fart.bu.edu.eg/fart/dept/liberaries-and-information-home
٥	المكتبات والمعلومات- جامعة المنوفية	http://mu.menofia.edu.eg/art/LIB/Home/ar
٦	المكتبات والمعلومات- جامعة الإسكندرية	http://www.arts.alexu.edu.eg/dept/libraries/
٧	المكتبات والوثائق والمعلومات-جامعة اسيوط	http://www.aun.edu.eg/faculty_arts/arabic/Department_Details.php?id=1505
٨	الوثائق والمكتبات- جامعة الفيوم	http://www.fayoum.edu.eg/Arts/DocumentsAndLibraries/AboutBoard.aspx
٩	المكتبات والمعلومات- جامعة حلوان	http://www.helwan.edu.eg/Arts-Ar/?page_id=1058
١٠	المكتبات والمعلومات –جامعة سوهاج	http://www.sohag-univ.edu.eg/facart/?page_id=8957
١١	قسم المكتبات والمعلومات بقنا – جامعة جنوب الوادي	http://www.svu.edu.eg/arabic/links/camps/qena/art/#
١٢	قسم علوم المعلومات – جامعة بنى سويف	http://www.arts.bsu.edu.eg/Content.aspx?section_id=1393&cat_id=3
١٣	المكتبات والمعلومات –جامعة قناة السويس	http://art.scuegypt.edu.eg/?page=pages&page_id=160
١٤	الوثائق والمكتبات- جامعة دمياط لا يوجد ثغرات	http://www.du.edu.eg/faculty/art/up/unitData.aspx?id=34&n=97

م	الفيس	الموقع
١٥	المكتبات والمعلومات-جامعة كفر الشيخ	http://www.kfs.edu.eg/arts/display_dep.aspx?topic=4574&dep=134
١٦	المكتبات والمعلومات- جامعة عين شمس	http://arts.asu.edu.eg/article.php?action=show&id=50#
١٧	الوثائق والمكتبات – كلية اللغة العربية– جامعة الأزهر بأسيوط	http://www.arabicazhar-asiut.com/page.php?pid=397 http://www.azhar.edu.eg/araic-asyout/%D8%A7%D9%84%D8%A7%D9%82%D8%B3%D8%A7%D9%85/%D9%82%D8%B3%D9%85-%D8%A7%D9%84%D9%88%D8%AB%D8%A7%D8%A6%D9%82-%D9%88-%D8%A7%D9%84%D9%85%D9%83%D8%AA%D8%A8%D8%A7%D8%AA
١٨	الوثائق والمكتبات- كلية الدراسات الانسانية - جامعة الأزهر بالقاهرة	http://www.azhar.edu.eg/anthropology-cairo/%D8%A7%D9%84%D8%A7%D9%82%D8%B3%D8%A7%D9%85/-%D8%A7%D9%84%D9%88%D8%AB%D8%A7%D8%A6%D9%82-%D9%88%D8%A7%D9%84%D9%85%D9%83%D8%AA%D8%A8%D8%A7%D8%AA

ملحوظة قسم الوثائق والمكتبات جامعة المنيا رابط القسم لا يعمل

ملحق اختبارات برنامج Vega


elect modules to run:
Injection Modules
Eval Code Injection
Integer Overflow Injection Checks
Format String Injection Checks
XML Injection checks
HTTP Header Injection checks
Remote File Include Checks
Shell Injection Checks
HTTP Trace Probes
Blind SQL Injection Timing
Blind SQL Injection Arithmetic Evaluation Differential Checks
URL Injection checks
Cross Domain Policy Auditor
Local File Include Checks
Bash Environment Variable Blind OS Injection (CVE-2014-6271, CV
Blind SQL Text Injection Differential Checks
Blind OS Command Injection Timing
Blind XPath Injection Checks
XSS Injection checks


Select modules to run:
Path Disclosure
X-Frame Options Header Not Set
HTTP Authentication Over Unencrypted HTTP
Social Security/Social Insurance Number Detector
Error Page Detection
Insecure Cross-Domain Policy
File Upload Detection
WSDL Detector
RSS/Atom/OPL Feed Detector
HTTP Header Checks
Insecure Script Include
Internal IP Addressess
Cookie Security Module
E-Mail Finder Module
Cleartext Password Over HTTP
Source Code Disclosure Module
Character Set Not Specified
Credit Card Identification
Empty Reponse Body Module
Unsafe Or Unrecognized Character Set
Interesting Meta Tag Detection
Oracle Application Server Fingerprint Module
Form autocomplete
AJAX Detector
Version Control String Detection
Directory Listing Detection
Cookie Scope Detection