****

**الوظيفة**

|  |  |
| --- | --- |
| MWS ماجستير علوب الوب | الاختصاص |
| أمن الوب Web Security \_ AWS | المادة |
| 1 | رقم الوظيفة |
| اختيار أحد المواضيع الأمنية ( مذكورة في النص) | عنوان الوظيفة |
| د. معتصم شفاعمري | إعداد |
| د. معتصم شفاعمري | تدقيق |
| 3-11-2018 | تاريخ التوزيع |
| تاريخ التسليم النهائي 25-11-2018 | تاريخ الإعادة |
|  | الموارد |

**نص الوظيفة**

**أختر أحد المواضيع التالية:**

**الموضوع (1)**

**مقارنات بين تقانات التعريف البيومترية**

**Biometric Access control comparison**

هناك العديد من طرق التحكم بالنفاذ في نظم الحواسيب والشبكات، وفي الآونة الأخيرة كثر استخدام العديد من الخصائص البيولوجية للإنسان في التحقق من هوية الشخص، أو استخدامها في أمن المعلومات، نظراً لخصائصها الفريدة كبصمة الأصبع، أو بصمة الكف، التعرف على الوجوه، قزحية العين، بصمة الصوت وغيرها من الصفات البيولوجية الفريدة. الجوانب المختلفة لعلم وظائف الأعضاء البشرية، والكيمياء أو سلوك يمكن استخدامها للمصادقة البيومترية. اختيار بيومترية معينة لاستخدامها في تطبيق معين ينطوي على ترجيح لعدة عوامل. واختيار الأنسب منها أو الدمج في أكثر من خاصية بيومترية لتحقيق الأهداف المطلوبة:

**والمطلوب:**

1. دراسة الأنواع المختلفة لطرق التحقق باستخدام الخصائص البيومترية للأشخاص
2. بيان مبدأ عمل وخصائص الخوارزميات المختلفة في تحليل كل من العناصر البيومترية وكيفية عملها ومقارنة الإيجابيات والسلبيات لكل خوارزمية.
3. مقارنة الطرق البيومترية المختلفة وتحديد الاستخدامات المثلى لكل منها
4. البحث عن أدوات وبرمجيات مفتوحة المصدر يمكن استخدامها في بناء تطبيقات تعتمد على التعرف على المستثمرين/ أو السماحيات بالدخول للمستثمرين تعتمد على الخصائص البيولوجية وتقييم هذه الأدوات.
5. اقتراح تصميم للنفاذ إلى نظام الجامعة الافتراضية السورية باستخدام الهواتف الذكية واعتماد طرق النفاذ البيومتري.

**ملاحظات**

* تقدم الدراسة ضمن تقرير نظامي و ضمن الفترة المحددة لإنجازة، وترفع على نظام الوظائف في الجامعة الافتراضية- في حال تعذر ذلك يمكن إرسالها بالبريد الإلكتروني مع بيان الأسباب.
* لا تقبل أي وظيفة بعد التاريخ النهائي المحدد للاستلام
* عند وجود أي عملين( وظيفتين) متماثلين لا يتم تصحيحهما ويأخذ مقدميها علامة الصفر

**الموضوع 21)**

**أمن الشبكات المعرّفة برمجياً (SDN)**

**Software Defined Networks Security**

كان الانتشار الكبير والتغيرات الجذرية في تطوير واستخدامات الأجهزة النقالة و نظم إدارة المحتوى، والمحاكاة الافتراضية للخوادم، وظهور الخدمات السحابية من بين الاسباب التي جعلت أصحاب القرار في صناعة الشبكات لإعادة النظر في بنى الشبكة التقليدية. العديد من الشبكات التقليدية هي هرمية البنية، حيث بنيت مع طبقات من محولات إيثرنت مرتبة في هيكل شجري. هذا التصميم يبدو منطقياً عندما كانت الحوسبة تعتمد على مفهوم لخدمة العملاء المهيمنة Client-server، ولكن مثل هذه العمارة الثابتة لا تناسب حالياً احتياجات الحوسبة والتخزين الديناميكية لمراكز بيانات الشركات، الجامعات، وبيئات الناقل. بعض الاتجاهات الحوسبة الأساسية دفعت لضرورة وجود نموذج شبكي جديد،  
الشبكات المعرفة بالبرمجيات (SDN) هو نهج لشبكات الحاسوب الذي يسمح لمسؤولي الشبكة لإدارة خدمات الشبكة من خلال التجريد من وظائف المستوى الأدنى. والمقصود SDN لمعالجة الواقع بأن الهندسة المعمارية الثابتة في الشبكات التقليدية لم يعد يدعم احتياجات الحوسبة والتخزين للديناميكة.

المطلوب:

1. دراسة أهمية الشبكات المعرفة برمجياً SDN والخدمات التي يوفرها
2. البنية الهيكلية للشبكات المعرفة برمجيا
3. الثغرات والمهددات الأمنية للشبكات المعرفة برمجياً SDN
4. الإجراءات الأمنية التي تم اتخاذها والأبحاث الجارية في حماية هذه الشبكات
5. بيان الرأي في مستقبل هذه الشبكات

**الموضوع -3**

**الأمن في إنترنت الأشياء**

**Security of Internet of Thinks (IoT)**

إنترنت الأشياء (IoT) هي شبكة من الأشياء المادية أو "الأشياء" والتي تعتبر جزءا لا يتجزأ من مع الالكترونيات والبرمجيات، وأجهزة الاستشعار والربط لتمكينها من تحقيق المزيد من القيمة والخدمة من خلال تبادل البيانات مع الشركة المصنعة ومشغل / أو غيرها من الأجهزة المتصلة. كل شيء Think هو معرف بشكل فريد من خلال نظام الحوسبة كجزءا لا يتجزأ، بل هو قادر على التعامل داخل البنية التحتية للإنترنت القائمة.

مصطلح "إنترنت الأشياء" تم توثيقها أول مرة من قبل صاحب الرؤية البريطانية، كيفن أشتون، في عام 1999. ومن المتوقع لـ IoT تقديم تقنيات توصيل البيانات المتطورة من الأجهزة والأنظمة والخدمات التي تتجاوز الاتصال كـ آلة إلى آلة ( M2M)، وتغطي مجموعة متنوعة من البروتوكولات والمجالات، والتطبيقات. وربط هذه الأجهزة المدمجة (بما في ذلك الكائنات الذكية)، حيث يتوقع أن تساهم في الأتمتة في جميع المجالات تقريبا.

الأشياء، في تقنيات IoT، يمكن أن تشير إلى مجموعة واسعة من الأجهزة مثل رصد دقات القلب المزروع، متابعة حيوانات المزرعة، والتحكم بالسيارات الذكية التي تحتوي على أجهزة الاستشعار، والتحكم بالأأجهزة المنزلية والمكتبية وغيرها، هذه الأجهزة تقوم بجمع بيانات مفيدة مع مساعدة من مختلف التكنولوجيات القائمة وتدفق البيانات بين الأجهزة الأخرى ،وتقديمم خدمات عديدة

قد أثيرت مخاوف من أن إنترنت الأشياء التي يجري تطويرها بسرعة دون الاعتبار المناسب للتحديات الأمنية العميقة المعنية والتغييرات التنظيمية التي قد تكون ضرورية. وقد بين المسح الذي أجري في الربع الأخير من عام 2014أن 39٪ من المستطلعين أن الأمن هو أكثر ما يثير القلق في اعتماد إنترنت الأشياء

**المطلوب:**

1. تقديم دراسة شاملة عن **إنترنت الأشياء** من حيث المتطلبات، البنية، الخدمات التي توفرها،
2. المزايا والمساوئ ( مع أمثلة عملية)
3. دراسة المهددات الأمنية والاختراقات التي تعرضت لها **إنترنت الأشياء** في السنوات الأخيرة مع تحليل كل طريقة اختراق (تهديد) وبيان نتائج وأثار كل من هذه المهددات.
4. دراسة الإجراءات اللازمة لحماية **إنترنت الأشياء** من المهددات التي تعرضت لها وبيات مستوى الأمن لكل من هذه الإجراءات
5. اقتراح تصميم إستراتيجية أمنية متكاملة وإطار عمل لحماية **إنترنت الأشياء**

**ملاحظات**

* تقدم الدراسة ضمن تقرير نظامي و ضمن الفترة المحددة لإنجازة، وترفع على نظام الوظائف في الجامعة الافتراضية- في حال تعذر ذلك يمكن إرسالها بالبريد الإلكتروني مع بيان الأسباب.
* لا تقبل أي وظيفة بعد التاريخ النهائي المحدد للاستلام
* عند وجود أي عملين( وظيفتين) متماثلين لا يتم تصحيحهما ويأخذ مقدميها علامة الصفر

**الموضوع )4)**

**أمن الشبكات الاجتماعية**

**Security of Social Networks**

شهدت السنوات الأخيرة تطورا ملحوظا في بعض التطبيقات الشبكية التي تعتمد على الإنترنت والوب وهي الشبكات الاجتماعية، كـ Face book, MyScpace LinkedIn, ResearchGate, Tweeter، وقد استقطبت الملايين من المستثمرين لما تقدمه من خدمات تواصل، وخدمات اجتماعية وعلمية وتجارية مختلفة. هذا الانتشار الواسع مع الكم الهائل من المعلومات التي تتضمنها الشبكات الاجتماعية جعلها هدفاً دسماً لمخترقي الشبكات و عرضة للاختراقات الأمنية المختلفة

**المطلوب:**

1. تقديم دراسة شاملة عن الخدمات الاجتماعية من حيث المتطلبات، البنية، الخدمات التي توفرها،
2. المزايا والمساوئ ( مع أمثلة عملية)
3. دراسة المهددات الأمنية والاختراقات التي تعرضت لها الشبكات الاجتماعية في السنوات الأخيرة مع تحليل كل طريقة اختراق (تهديد) وبيان نتائج وأثار كل من هذه المهددات.
4. دراسة الإجراءات اللازمة لحماية الشبكات الاجتماعية من المهددات التي تعرضت لها وبيات مستوى الأمن لكل من هذه الإجراءات
5. اقتراح تصميم إستراتيجية أمنية متكاملة وإطار عمل لحماية الشبكات الاجتماعية

ملاحظات

* تقدم الدراسة ضمن تقرير نظامي و ضمن الفترة المحددة لإنجازة، وترفع على نظام الوظائف في الجامعة الافتراضية- في حال تعذر ذلك يمكن إرسالها بالبريد الإلكتروني مع بيان الأسباب.
* لا تقبل أي وظيفة بعد التاريخ النهائي المحدد للاستلام
* عند وجود أي عملين( وظيفتين) متماثلين لا يتم تصحيحهما ويأخذ مقدميها علامة الصفر

**ملاحظات**

* تقدم الدراسة ضمن تقرير نظامي و ضمن الفترة المحددة لإنجازة، وترفع على نظام الوظائف في الجامعة الافتراضية- في حال تعذر ذلك يمكن إرسالها بالبريد الإلكتروني مع بيان الأسباب.
* لا تقبل أي وظيفة بعد التاريخ النهائي المحدد للاستلام
* عند وجود أي عملين( وظيفتين) متماثلين لا يتم تصحيحهما ويأخذ مقدميها علامة الصفر

**الموضوع (5)**

**تصميم موقع وب يهدف إلى تحليل الثغرات في مواقع الوب**

تتعرض الكثير من مواقع الوب إلى الهجوم والاختراق وذلك من خلال الثغرات الأمنية في التطبيق منها:

* + - JavaSript Injection
    - Java Applet , Active X attacks
    - SQL Injection
    - Second Order SQLi
    - Iframe Injection
    - Cross-Site Request Forgery (CSRF)

و غيرها.

**المطلوب:**

1. تصنيف نقاط الضعف في تطبيقات الوب بشكل عام
2. تحديد جميع الاختراقات الممكنة وشرح كيفية حدوثها
3. تحديد الآليات والطرق الواجب تجنب هذه الثغرات الأمنية
4. تصميم موقع وب يتضمن أدوات اختبار برمجية تقوم بما يلي:
   1. تحديد موقع الوب المراد اختباره وذلك من خلال إدخال عنوانه URL
   2. تحليل صفحات الوب للموقع المحدد بحيث يتم التحليل للصفحات ذات المستوى الأول والثاني فقط (أي الصفحة الرئيسية وصفحات الروابط التي تحويها فقط)
5. اختبار الثغرات الأمنية في هذه الصفحات وتقديم تقرير عبر الموقع المصمم و قابل للطباعة، يبين عدد الثغرات الأمنية في كل منها، ومحدداُ نوع كل ثغرة من هذه الثغرات – اسم الصفحة المتواجدة فيها ومكان الثغرة – السطر والتعليمة– وكيفية حمايتها.

**تسليم الوظيفة: تسلم الوظيفة ضمن الفترة المحددة لها حصراً**

* يتم كتابة التقرير ونتائج الاختبارات وتسليمه عبرالظام الإلكتروني للجامعة ، لا مانع من إرسال نسخة – إضافية- من التقرير عبر البريد الإلكتروني.
* يجب أن يتضمن التقرير أيضاُ رابطاً إلى الموقع المنفذ عبر الإنترنت (أو عنوان موقع المشروع) ليتم اختباره.
* على الطلاب المشاركين في مشروع واحد كتابة أسمائهم على صفحة الغلاف، وكذلك إعلامي مسبقاً عبر البريد الإلكتروني مع تحديد رقم الطالب

يمكنكم الاطلاع على بعض المواقع التي تهتم Web Application Vulnerability منها:

<https://mosaicsecurity.com/categories/33-webbased-application-security-scanners>

<http://sectools.org/web-scanners.html>

**الموضوع (6)**

**تصميم نظام أمن للرعاية الصحية الإلكترونية**

**E\_ Health SystemٍSecure**

ترغب إحدى المشافي في أتمتة أعمالها الصحية وتقديم نظام الخدمات والرعاية الصحية الإلكترونية حسب المعايير الدولية، والمطلوب:

1. تحديد وتعريف نظام السجل الصحي الإلكتروني EHR (Electronic Health Record ) للمريض حسب المعايير الدولية ليكون متوافقاً في المستقبل لترابطه مع الأنظمة الصحية المؤتمتة الأخرى.
2. تحديد العلاقة بين مستخدمي السجل الصحي الإلكتروني والمعلومات التي يحويه ( المريض، الطبيب، الصيدلي، المخبر، الإدارة المالية، التصوير الشعاعي، العيادات، .....الخ
3. تحديد الخدمات الطبية الإلكترونية والبنية التحتية اللازمة
4. دراسة متطلبات البنى التحتية والمتطلبات الأمنية لتقديم هذه الخدمات، ووضع التصميم اللازم.
5. تصميم وإنشاء موقع إلكتروني يقدم بعض الخدمات الصحية الإلكترونية مع تأمين الحماية اللازمة للمعلومات المتبادلة عبره.

**ملاحظات**

* تقدم الدراسة ضمن تقرير نظامي و ضمن الفترة المحددة لإنجازة، وترفع على نظام الوظائف في الجامعة الافتراضية- في حال تعذر ذلك يمكن إرسالها بالبريد الإلكتروني مع بيان الأسباب.
* لا تقبل أي وظيفة بعد التاريخ النهائي المحدد للاستلام
* عند وجود أي عملين( وظيفتين) متماثلين لا يتم تصحيحهما ويأخذ مقدميها علامة الصفر

**الاسم النظامي لملف الوظيفة:**

**Program name\_Course code\_Semester\_HW\_Student name\_StudentCode.docx**

**سلم التصحيح لكل من الخيارات السابقة**

|  |  |  |
| --- | --- | --- |
| **التسلسل** | **رقم الطلب أو اسم المعيار** | **العلامة** |
| 1 | الطلب رقم 1 | 10 |
| 2 | الطلب رقم 2 | 15 |
| 3 | الطلب رقم 3 | 15 |
| 4 | الطلب رقم 4 | 15 |
| 5 | الطلب رقم 5 | 15 |
| 6 | الالتزام بالمعايير الشكلية | 5 |
| 7 | الخلو من الأخطاء العلمية | 10 |
| 8 | الجهد في جمع البيانات | 10 |
| 9 | جودة التحليل الوصفي | 5 |
| **العلامة الإجمالية** |  | **100** |