كلية الهندسة المعلوماتية - جامعة دمشق

السنة الخامسة -قسم البرمجيات عملي أمن نظم المعلومات

نظام أمن لشبكة مواقف سيارات

الوصف

- **الهدف هو إنشاء نظام يعمل على الربط بين كيان مواقف السيارات مع المستخدمين (موظفين ، زوار)**
- **يبنى النظام على Server-Client Model: مخدم المواقف (server) وكيان المستخدمين (الموظفين والزوار) (client)**
- **الاعتماد في المخدم على Multi-Threading أو Event-Driven (أي من الممكن أن يخدم أكثر من Client في نفس الوقت)**

وبحيث تكون النتائج النهائية للمشروع تدعم أمن المعلومات و خاصة من النواحي التالية :

1. سرية المعلومات Confidentiality
2. سلامة المعلومات Integrity
3. عدم النكران Non-Repudiation
4. Authentication, Authorization
5. التأكد من أن الشخص أو السيرفر الذي يتم التواصل معه هو فعلًا الشخص المراد التواصل معه
6. تجنب استخدام خوارزميات وطرق التشفير الضعيفة
7. يستخدم السيرفر البورت 3000

مراحل المشروع :

المرحلة الأولى (تسجيل وإنشاء الحسابات)

الوصف :

يسمح النظام للعميل Client بإرسال Request إلى السيرفر لإنشاء حساب للمستخدم يتضمن الحقول التالية:

- الاسم الكامل.
- نوع المستخدم (موظف، زائر)
- رقم الهاتف.
- لوحة السيارة.
- كلمة المرور.

الوظيفة :

- يستقبل السيرفر الطلب (Request) ويتحقق من البيانات المُرسلة.
- بعد التحقق، يتم إنشاء حساب جديد للعميل وتخزين البيانات في قاعدة البيانات.
- يقوم العميل لاحقًا بتسجيل الدخول باستخدام الاسم وكلمة المرور.

المرحلة الثانية : إدارة المواقف (سرية المعلومات):

الوصف :

الهدف هو الحفاظ على سرية البيانات المُرسلة بين العميل والسيرفر.

الوظيفة :

- يتم الاتفاق بين العميل والمخدم على مفتاح تشفير متناظر.(Session Key)
- عند حجز موقف معين، يتم تشفير البيانات (رقم الموقف، الوقت) باستخدام مفتاح الجلسة المتفق عليه.
- يرسل العميل الطلب المُشفر إلى السيرفر.
- يقوم السيرفر بفك التشفير، تأكيد الحجز، وإرسال الرد إلى العميل مشفرًا.

المرحلة الثالثة: دفع الرسوم (التشفير الهجين)

الوصف:
يهدف النظام إلى حماية عملية الدفع باستخدام التشفير الهجين.

الوظيفة:
- يتم توليد مفتاحي تشفير Public/Private Keys لكل من العميل والسيرفر عند أول محاولة اتصال.
- يتم تنفيذ Handshaking بين الطرفين لتبادل المفتاح العام (Public Key).
- يقوم العميل بتوليد مفتاح جلسة (Session Key) لتشفير بيانات الدفع.
- يتم تشفير مفتاح الجلسة بالمفتاح العام الخاص بالسيرفر وإرساله إليه.
- يتم تشفير بيانات الدفع باستخدام مفتاح الجلسة وإرسالها للسيرفر.
- بعد فك التشفير، يرسل السيرفر تأكيد العملية للعميل.

الخطوة الرابعة: مراقبة النشاط (التوقيع الرقمي)

الوصف:

يتم استخدام التوقيع الرقمي لضمان عدم التلاعب بالبيانات وتوثيق العمليات.

الوظيفة:
- عند إجراء أي عملية (حجز موقف، دفع رسوم)، يتم توليد توقيع رقمي للبيانات .
- يتم التحقق من التوقيع لضمان سلامة البيانات وعدم تعديلها أثناء النقل.
- يقوم النظام بتسجيل العملية في سجل الأنشطة مع حفظ التوقيع الرقمي.

المرحلة الخامسة: التوثيق باستخدام الشهادات الرقمية

الوصف:
الهدف هو التحقق من هوية المستخدم والسيرفر باستخدام شهادات رقمية.

الوظيفة:
- يقوم المستخدم (العميل) بإرسال طلب توليد شهادة رقمية (CSR) إلى جهة موثوقة (CA).
- يتم ربط الشهادة بالمفتاح العام الخاص بكل مستخدم.
- يتم التحقق من صحة الشهادة عند كل عملية اتصال بين العميل والسيرفر.
- يتم استخدام الشهادات لتوثيق العمليات.

المرحلة السادسة (إيجاد حلول برمجية مناسبة)

الوصف:

الهدف هو إيجاد طرق مناسبة للتصدي من هجمات XSS,SQL Injection.

وظيفة الويب

يجب تنفيذ هجوم الوارد في المحاضرة Xss بهدف XSS Attacks to People'sProfiles Change Other وذلك على منصة Elgg .

ملاحظات إضافية :

- **عدد الطلاب في المجموعة: 4 طلاب على الأكثر .**
- **يجب تسليم تقرير يتضمن:**
  - **شرح المراحل العملية.**
  - **الكود البرمجي مع التعليقات.**
  - **شرح التوابع المستخدمة في النظام.**
- **مقابلة المشروع تحدد لاحقاً.**
- **يمكن للطالب استخدام اللغة البرمجية التي يفضلها شرط أن يتمكن من خلالها من تحقيق كامل مراحل المشروع المطلوبة.**

مع تمنياتي بالتوفيق للجميع .....

م. أريج رحال