جامعة دمشق

كلية الهندسة المعلوماتية

قسم الذكاء الصنعي - مشروع عملي أمن المعلومات

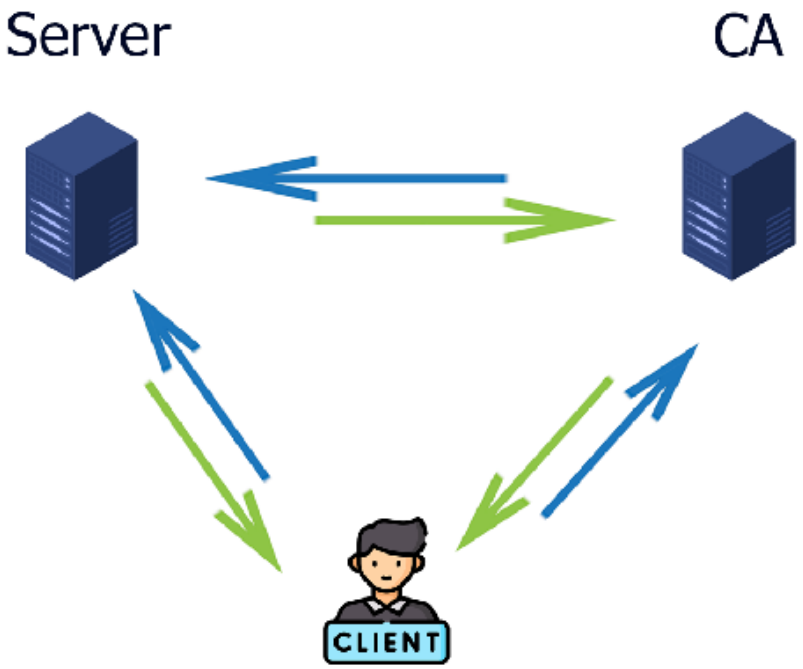
القسم الأول : إنشاء مخدم للملفات المهمة

الهدف :

إنشاء نظام حكومي لتخزين الوثائق الشخصية المهمة للأفراد بهدف الوصول إليها الكترونياً عند الطلب دون الحاجة لنسخة ورقية

وذلك عن طريق بناء تطبيق ويب موجود على سيرفر يمكن الوصول إليه عن طريق المتصفح بحيث يُمكّن المواطنين من تسجيل الدخول و رفع الوثائق الشخصية بالمقابل هناك حسابات للمؤسسات يمكن من خلاله الاطلاع على الوثائق الخاصة بالمواطنين

معمارية النظام :



Client

الاعتماد على thin-client بالتالي لا يوجد حاجة لبرمجية مخصصة

Server

يتم عليه انشاء حسابات للمستخدمين وتخزين الملفات المرتبطة بكل مستخدم

CA (Certificate Authority)

المخدم المسؤول عن منح وتصديق الشهادات

الوصف :

توليد الشهادة الرقمية للمخدم :

عند أول تشغيل للمخدم يقوم بإرسال طلب لـCA لتوليد شهادة رقمية فيقوم الـCA بحفظ هذه المعلومات وتوليد شهادة رقمية ثم يرسلها إلى المخدم

تسجيل الحساب :

يقوم المستخدم بطلب صفحة الويب ويدخل المعلومات الشخصية (الاسم – الرقم الوطني – تاريخ الميلاد - رقم الهاتف) إضافة إلى كلمة مرور للحساب بدوره المخدم يقوم بتخزين هذه المعلومات ضمن الداتابيز مع الانتباه أن كلمة المرور يجب أن تخزن بشكل غير صريح ويعيد للمستخدم رسالة بنجاح عملية التسجيل

هناك نوعان للحسابات :

حساب شخصي خاص بالأفراد التي تقوم بعمل upload للوثائق الشخصية الخاصة بهم

حساب مسؤول خاص بالمؤسسات التي تقوم بعمل download لهذه الوثائق دون القدرة على تعديلها حيث يظهر لمستخدم هذا الحساب عند الدخول واجهة تمكنه من البحث عن الوثائق المتعلقة بأي شخص باستخدام الرقم الوطني

تسجيل الدخول ورفع أو تنزيل الوثائق :

تتم عملية تسجيل الدخول باستخدام الرقم الوطني وكلمة المرور الخاصة بالمستخدم بعد إجراء عملية التحقق يمكن لمستخدم الحساب الشخصي رفع الوثائق الخاصة ومستخدم الحساب المسؤول يمكنه الاطلاع وتنزيل هذه الوثائق

ملاحظات :

- نعتبر CA كيان موثوق بالنسبة للمخدم والزبون بالتالي يمكن اعتماد الشهادة الرقمية التي يرسلها **الخاصة به فقط** دون التحقق منها
- يجب حفظ البيانات على المخدم الخاص بالتطبيق ومخدم الشهادات بشكل آمن لا يمكن تعديله
- يجب على المخدم التأكد من سلامة البيانات المخزنة لديه قبل إرسالها لأي أحد
- يجب أن تكون الاتصالات بين جميع الكيانات محمية ومشفرة وذلك باستخدام Hybrid encryption method
- عند رفع الوثائق على المخدم يجب على المخدم التوقيع الرقمي عليها ليكون هذا التوقيع بمثابة تصديق على صحة المحتوى ثم يتم تخزينها على المخدم
- عند تنزيل الوثائق من المخدم يمكن للمستخدم التأكد من صحة التوقيع على هذه الوثائق وذلك عن طريق الاتصال مع CA وطلب الشهادة الرقمية الخاصة بالمخدم ثم التحقق من التوقيع الرقمي
- الاعتماد في المخدم والCA على multi-threading أي ممكن أن يخدموا أكثر من زبون في نفس الوقت
- يجب التأكد أن موقع الويب محمي من ثغرة cross site scripting
- يجب التأكد أن موقع الويب محمي من ثغرة SQL injection
- يجب التأكد من الملفات قبل تخزينها على المخدم بحيث لا تكون هذه الملفات ضارة للمخدم أو العميل (virus-Trojan-worm)

القسم الثاني : تطبيقات عملية

في الروابط أدناه تطبيقات عملية لثغرات الويب التي ذكرناها ضمن المحاضرات ,المطلوب هو حل هذه التطبيقات مع **فهم كيفية الوصول إليها واكتشافها** حيث سيتم بالمقابلة السؤال عن خطوات التطبيق والحل المقترح

https://portswigger.net/web-security/sql-injection/lab-sql-injection-with-filter-bypass-via-xml-encoding

https://portswigger.net/web-security/cross-site-scripting/contexts/lab-href-attribute-double-quotes-html-encoded

أمور تنظيمية :

- يجب التركيز بالعمل على النواحي الأمنية وكيفية معالجتها دون التدقيق بالتفاصيل البرمجية من واجهات وخوارزميات
- يجب الاعتماد بالتشفير وفك التشفير على مكتبات جاهزة وخوارزميات قوية دون الحاجة إلى إعادة كتابة توابع خاصة لذلك
- الالتزام بالنقاط المذكورة عدا ذلك لكم حرية الاختيار
- عدد الطلاب في المجموعة الواحدة من 3 إلى 5
- مواعيد المقابلات المبدئي في الأسبوع الأول من شهر كانون الثاني

بالتوفيق...المهندس عبد الهادي اسامي