

Providing A Secure Environment For E-Commerce Sites Using SSL Technology

Maha A. Sayal

Department of Computer Sciences, College of Computer Sciences and Math, Thi-Qar University, Iraq

Email: maha.asyal@utq.edu.iq

(Received May 03, 2018; Accepted October 03, 2018; Available online March 01, 2020)

DOI: [10.33899/edusj.2020.164371](https://doi.org/10.33899/edusj.2020.164371), © 2020, College of Education for Pure Science, University of Mosul.

This is an open access article under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

Abstract:

The issue of security on the Internet is at the top of the interest for most users, especially those who want to buy online and therefore find a large majority of users, especially new ones refrain from buying online and are afraid to go into such an experiment to complete the image and know more safety in the use of credit cards for some websites.

In order to increase confidence in online business transactions, we have proposed a safe environment for commercial sites by installing a private server and then submitting on certificate authority for digital certificates and obtaining Secure Socket Layer SSL technology, certificate it, and adding it to the server as well as hosting sites to secure its data and renew the certificate at expiration. This allows the business website owner to host that website on the secure server so the customer information and data will be protected.

Keywords: commercial sites, Secure Socket Layer SSL, certificate authority, digital certificates, online business transactions

توفير بيئة امنية لمواقع التجارة الالكترونية بأستعمال تقنية طبقة الفتحات الامنة (SSL)

مها عبد اللطيف سايال

قسم علوم الحاسبات, كلية علوم الحاسوب والرياضيات, جامعة ذي قار, العراق

الخلاصة

ان ما يتصدر قائمة الاهتمامات لدى معظم مستخدمي الانترنت هو موضوع الأمنية على شبكة الإنترنت وخصوصاً عندما تكون لهم رغبة في الشراء عبر الإنترنت ولذلك تجد اغلب الاشخاص من المستخدمين وخصوصاً الجدد منهم يمتنعون عن الشراء عبر الإنترنت ويخشون من اعطاء معلومات عنهم حتى تكتمل الصورة لديهم و يتعرفون على مدى درجة الأمان في استعمال بطاقات الائتمان في بعض المواقع.

ولزيادة الثقة بالصفقات والتعاملات التجارية عبر الانترنت اقترحنا توفير بيئة امنية للمواقع التجارية عن طريق تنصيب خادم خاص ومن ثم التقديم على هيئة توثيق الشهادات الرقمية و الحصول على تقنية طبقة الفتحات الامنة Secure Socket Layer (SSL) وشهادتها وإضافتها للخادم والمواقع المستضافة عليه لتأمين بياناتها وإعادة تجديد الشهادة عند انتهاء صلاحيتها. وبذلك يمكن لصاحب الموقع التجاري ان يستضيف موقعه على ذلك الخادم الامن لحماية معطيات الزبون.

الكلمات المفتاحية: المواقع التجارية، طبقة الفتحات الامنة، هيئة التوثيق، الشهادات الرقمية، الصفقات التجارية عبر الانترنت .

1- المقدمة

ان التجارة الالكترونية اصبحت جزءاً مهماً في بناء الاقتصاد مستقبلاً، كون التجارة هنا اصبحت متعلقة بالتكنولوجيا وما لها من اثر في توسيع وتطوير افاق التجارة التقليدية . لذلك يجب توضيح مفهومها ومزاياها وتحدياتها.

1-1 مفهوم التجارة الالكترونية: Electronic Commerce

التجارة الالكترونية هي عملية شراء أو بيع أو تبادل المنتجات والمعلومات والخدمات من خلال الشبكات المحلية والدولية والعالمية ومن ضمنها الانترنت. فهي عملية تطبيق تقنية من أجل جعل المعاملات التجارية تجري بصورة تلقائية وسريعة هذا من وجه نظر الأعمال الاقتصادية و التجارية [1].

ان التسوق في المجمعات التجارية الموجودة على الانترنت و بنوك الانترنت وشراء الاسهم والتعاون مع بقية الأفراد في عمل بحث ما هي من تطبيقات التجارة الالكترونية [2]. و لتنفيذ هذه التطبيقات، يتطلب الحصول على دعم المعلومات وبنية تحتية وأنظمة. تكون تطبيقات التجارة الالكترونية مدعمة بأساس وبنية تحتية . وتؤدي عمل هذه التطبيقات يتطلب الاعتماد على أربعة اساسيات وهي الناس، المعايير و البروتوكولات التقنية، السياسة العامة، وشركات أخرى [3] .

1-2 مزايا التجارة الالكترونية

- تتمتع التجارة الالكترونية بمجموعة من المزايا يمكن ايجازها :
 - زيادة المنافسة: اذ تعد التجارة الالكترونية، الاداة لتحقيق ذلك اذ توفر وسائل وادوات تضاف الى المنافسة لزيادة الصادرات وسهولة وصول المستهلكين الى البضائع من خلال مواقع الانترنت، ويمكن اجمال ميزاتها بما يلي:
 - 1- امكانية التسويق على المستوى العالمي بكلفة محددة .
 - 2- السرعة في عقد الصفقات وانهاؤها اذ يكون الاجتماع مع الشركات المتعاقدة على الانترنت بأستعمال برامج فيديو و اجراء المحادثات عبر سكايب وغيرها دون الحاجة الى تحمل عناء السفر .
 - 3- مساهمة التجارة الالكترونية في التخلص من مشاكل العوائق الجغرافية واختصار الوقت في اداء المعاملات التجارية [1]
 - امكانية القيام بمشروعات صغيرة او متوسطة تعاني من غياب الموارد الاقتصادية اذ ان التجارة الالكترونية اعدت لكي تتمكن تلك المشاريع من القيام بعملها على اكمل وجه اذ ساعدها ذلك على الوصول الى السوق العالمية [3] .
 - ان التجارة التقليدية كانت مكلفة من ناحية الاعلان والدعاية والتسويق لكن بفضل دخول التجارة ضمن عالم الانترنت اصبحت تلك الكلف جداً منخفضة [4] .

1-3 بعض التحديات التي تواجه التجارة الالكترونية

من اهم التحديات في موضوع التجارة الالكترونية هي حماية المعلومات وهذا موضوع البحث اذ انه من الممكن انتهاك الخصوصية، الامن، المعلومات او اعتراض ومراقبة البريد المرسل بين الشركة او البائع والمستهلك [5] . واختراق اطراف خارجية للوصول الى بيانات العملاء والتعرف على خصوصيات الشركة اذا انتفى وجود سائر امني لان مجرد الوصول الى الحاسب الشخصي للعميل يمكن الحصول على معلومات توصل الى طرائق التواصل مع العملاء و بالامكان التواصل معهم واغراق الشركة بالخسائر عن طريق

معرفة ميولهم ورغبات العملاء وبالتالي تحميل الشركة خسائر جمة وهذا سبب تعرض حسابات وبطاقات ائتمان العملاء والمشتريين للسرقة اذا لم يكن هناك طرق تشفير امنة [6] .

ومن هنا وجد انه لا بد من السعي لحل تلك المشكلة للأحتفاظ بالخصوصية والامان وحماية كلا من الشركة والعملاء والزبائن , اذ تكون حماية الخادم الخاص بالشركة التجارية من اجل الشركة والعميل وحماية الموقع التجاري من اجل الشركة والزبون , اذ يتم تشفير المعلومات المارة بين الطرفين من خلال تقنية SSL واستعمالها في الشهادة الرقمية التي يمكن الحصول عليها من هيئة توثيق الشهادات الرقمية [7] .

1-4 هيئة توثيق الشهادات الرقمية (A certification authority (AC)

هي جهة مستقلة تقوم باصدار والغاء الشهادة الرقمية , و اضافة المفاتيح العام وغيرها من المهام الاساسية وتقوم بالتأكد من سيرة الموقع والخادم. ان الشهادة الرقمية وجدت لحل مشكلة انتحال الشخصية وهي عبارة عن وثيقة رقمية تحتوي على مفتاح عام Public Key ومعلومات عن مالك الشهادة أو المنظمة أو الشركة ومعلومات عن السلطة المصدرة للشهادة Certificate Authority و تاريخ اصدار الشهادة وانتهائها و الرقم التسلسلي للشهادة وهو الجزء الأهم, و تربط الخادم بمفتاح عام ويتم نشرها لاثبات هوية الخادم [7]. ان نشر الشهادة لا يحمل أي ضرر حيث لا تحتوي على معلومات سرية لان المفتاح العام سوف يربط مع المفتاح الخاص المعروف من قبل الكيان المالك للشهادة . واهمية الشهادة تكمن في اجراء المعاملات الرقمية ,عند الشراء عبر الانترنت وعند ارسال الرسائل لاثبات هوية الشخص. وكيفية معرفة الشخص بوجود شهادة رقمية للموقع , مثلا عند تحقق الشخص من حسابه البنكي عبر الانترنت مستخدماً إحدى المتصفحات عند دخوله الى موقع البنك تظهر اشارة قفل في شريط العنوان ملحقة ببروتوكول (HTTPS Hypertext Transfer Protocol Secure) وهو بروتوكول النصوص التشعبية الأمن وهذا يدل على ان الصفحة محمية ويستخدم شهادة رقمية لتأمين الصفحة , الشكل (1) [8] .



الشكل (1) يوضح وجود الشهادة الرقمية

1-5 تقنية طبقة الفتحات الامنة SSL وآلية عملها

تقنية طبقة الفتحات الامنة SSL هي برنامج يحتوي على بروتوكول تشفير متخصص لنقل المعلومات والبيانات التي تم تشفيرها بين جهازين عبر شبكة الانترنت بطريقة محمية بحيث لا يمكن لاحد من الاشخاص قراءتها غير مرسل البيانات والمستقبل لها وفي نفس الوقت تكون طريقة التشفير فيها معقدة ويصعب فكها, وهي تختلف عن بقية طرق التشفير في شئ واحد الا وهو ان مرسل البيانات ليس له علاقة في اتخاذ اي خطوات لتشفير المعلومات المراد حمايتها [9].

يقوم هذا البرنامج الذي يعمل بتلك التقنية بتشفير أي معلومة صادرة من ذلك المستعرض وصولاً إلى جهاز الخادم الخاص بالموقع التجاري المستضاف عليه، باستعمال بروتوكول التحكم بالإرسال والانترنت وهو ما يعرف ب (TCP/IP). وسبب تسميتها

بالطبقة الامنة لأن هذا البرنامج يعمل كطبقة وسطية تربط بين بروتوكول التحكم بالنقل و بروتوكول نقل النصوص المتشعبة (HTTP) [10].

وتتلخص خطوات استخدام هذه التقنية كالتالي [11]

1- تقوم هيئة التوثيق بإصدار الشهادة الرقمية الخاصة بالموقع بعد تقديم طلب من صاحب الموقع التجاري بحيث تحتوي على كل المعلومات التي تخص الهيئة مثل اسم الهيئة وتاريخ إصدار الشهادة وتاريخ الانتهاء، وكذلك يتم إصدار المفتاح الخاص private key و المفتاح العام public key ليتم تخزين SSL للموقع و يقوم الموقع أيضا بتأمين جهاز خادم مزود ببرنامج لتشفير المفتاح العام للموقع.

2- تقوم المستعرض المزود بهذا البرنامج بالارتباط بالجهاز الخادم الآمن للموقع التجاري و يطلب منه التالي :الشهادة الرقمية ، مصدرها ، تاريخ انتهاءها وكذلك تتم المقارنة بين اسم الموقع التجاري على الشهادة مع اسم الموقع في جهاز الخادم والمقارنة بين الرقم العام المرسل من الجهاز الخادم إلى المستعرض مع التوقيع الإلكتروني للشركة ، وكل هذه الخطوات تتم للتأكد من مصداقية الموقع وحماية الزبون من الشركات الوهمية.

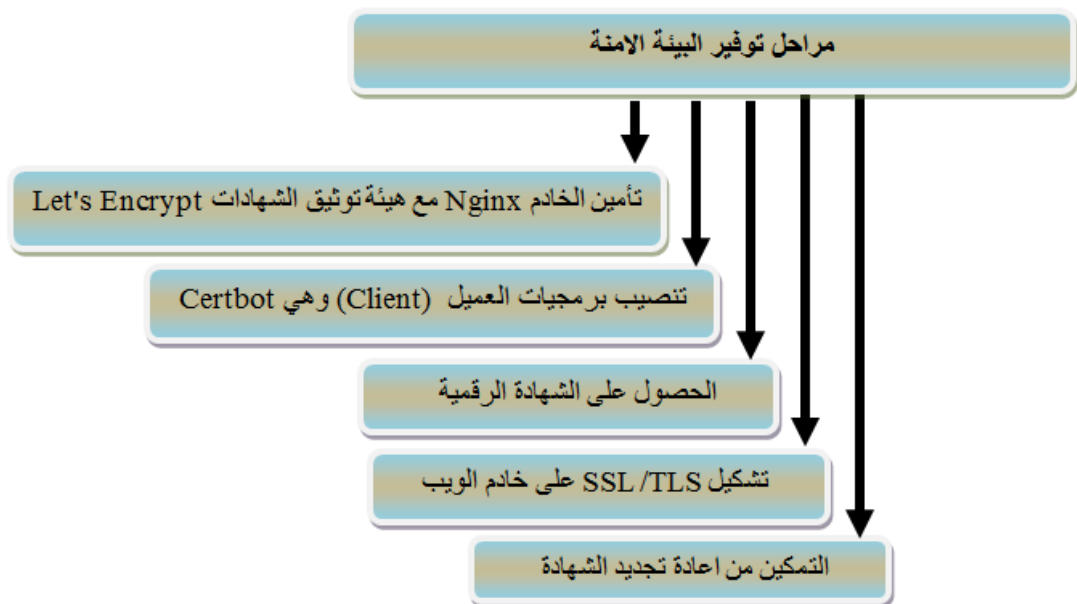
3- يتم تشفير المعلومات للزبون على أساس المفتاح العام لذلك الموقع ليتم نقل المعلومات بطريقة آمنة دون أي تدخل منه ولا يستطيع أحد سرقة المعلومات أو الإطلاع عليها سوى الموقع المعتمد في الطرف الآخر والذي يملك المفتاح الخاص للموقع لفتح وإعادة المعلومات إلى وضعها الطبيعي .

2- الجانب العملي

ان ال SSL هو الطريق لتشفير معلومات الموقع وخلق ارتباط أكثر امان ، بالإضافة الى ان شهادة ال SSL تعرض معلومات تعريفية عن الخادم المحمي لزوار الموقع .

تم في هذا العمل اقتراح تنصيب خادم معين ومن ثم التقديم على هيئة توثيق الشهادات الرقمية و للحصول على تقنية SSL وشهادتها و اضافتها للخادم والمواقع المستضافة عليه لتأمين بياناتها وإعادة تجديد الشهادة عند انتهاء صلاحيتها .

يوجز الشكل (2) مراحل توفير البيئة الامنة .



الشكل(2) ملخص مراحل توفير البيئة الامنة

1-2 البرمجيات ونظام التشغيل المستخدم في الجانب العملي

ان النظام المستخدم في العمل هو نظام Linux اصدار Ubuntu14.04 اذ ان مميزات هذا النظام انه مفتوح المصدر واكثر اماناً من نظام Windows لانه قابل للتحديث ملايين المرات في الدقيقة الواحدة , أي من الممكن اضافة خطوات لبرمجة جذر النظام وهذا سبب استخدامه في العمل , كذلك يتميز هذا النظام بكتابة الايعازات اكثر من استعمال الواجهات الرسومية للأوامر اذ تكتب الايعازات في نافذة ال terminal ويتم اضافتها الى جذر النظام Root .في حين نظام windows يحتاج الى استخدام محاكي طرفي لأضافة بعض الاوامر المستعملة في البحث على النظام .

يتم في البداية تهيئة البرمجيات المطلوبة للعمل وهي مجموعة برامج LEMP حيث انها مختصر ل (Linux, Nginx, PHP, MySQL) التي تمثل مجموعة من البرمجيات يمكن استعمالها لخدمة صفحات الويب الديناميكية وتطبيقات الويب , اذ L يقصد به نظام التشغيل Linux و E وهو الخادم المستعمل Nginx و M هي قاعدة البيانات MySQL و P هي اللغة الديناميكية لكتابة المواقع على الويب PHP.

من الجدير بالذكر ان جميع الايعازات والبرمجة تكتب بنافذة (Terminal) الخاصة بنظام Linux.

Sudo apt-get update Sudo

خطوات تنصيب الخادم Nginx تكون كالتالي :

apt-get install nginx

يوضح الشكل(3) خطوات تنصيب الخادم بصورة صحيحة و حجز مكان له على الشبكة العنكبوتية



الشكل (3) تنصيب الخادم Nginx

ملاحظة : في هذا البحث تعذر امكانية تعريب بعض الاشكال والجدول لاحتوائها على مصطلحات ومختصرات (معروفة علمياً). وفي حال تعريبها تصبح غير مفهومة بالنسبة لصاحب الاختصاص.

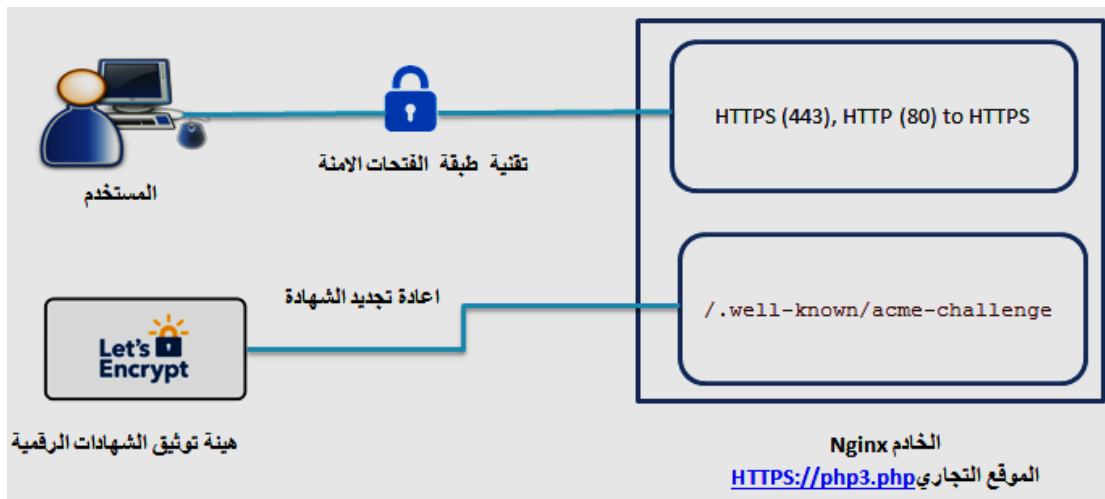
2-2 تأمين الخادم Nginx مع Let's Encrypt

Let's Encrypt هي هيئة توثيق (CA) شهادات رقمية جديدة توفر اساليب سهلة للحصول على وتنصيب شهادات SSL و TLS ومقدرتها على تحويل HTTPS مشفر للعمل على خادمتها الويب. الشكل(4) يوضح شعار هيئة التوثيق.



الشكل (4) شعار هيئة التوثيق [12]

يتناول هذا الجزء كيفية توفير شهادته رقمية SSL واضافتها واستعمالها مع Nginx هنا سوف يتم ربط Nginx وهو خادم ويب مع الشهادة الرقمية وكيفية اعادة تجديدها, ان ملف التهيئة يحتوي على قواعد لصالح الملفات والطلبات اذ يمنع الوصول الى الملفات بالاسماء الموجودة في الملف `/.well-known/acme-challenge/xxx`. يبين الشكل (5) الية منح الشهادات الرقمية.



الشكل (5) الية منح الشهادات الرقمية

3-2-2 تنصيب برمجيات العميل (Client) وهي Certbot

Certbot هي برمجيات تحاول الياً حل اغلب الخطوات المطلوبة للشهادة, هيئة التوثيق Let's Encrypt تمنحنا السهولة في الحصول على شهادة SSL برمجياً بغض النظر عن خادم الويب المستعمل. في الخطوة الاولى يتم اضافة مستودع للتخزين من خلال الشفرة التالية.

```
sudo add-apt-repository ppa:certbot/certbot
```

```
sudo apt-get update
```

```
sudo apt-get install certbot
```

في هذه الخطوة يتم بالتحديث

واخيراً يتم بتنصيب برمجيات العميل

2-4 الحصول على الشهادة الرقمية

يوفر ال Let's Encrypt طرائق متنوعة للحصول على الشهادة , وهذه الطرائق او الاضافات تسمى مصادقة. اذ ان الاضافات تستعمل في حالة وجوب اصدار شهادة للخادم Nginx . ان الخطوة الاساسية الاولى في الحصول على الشهادة هي كيفية استعمال البرنامج المساعد (root) web , قبل استعمال البرنامج المساعد يجب التأكد من برمجيات العميل . للتأكد من امكانية الوصول الى برمجيات العميل (certbot) والتأكد من صحتها, يجب القيام باجراء تغيير على Nginx , اذ يتم استعمال ايعاز ال nano لفتحه وتعديله .

`sudo nano /etc/nginx/sites-available/default`

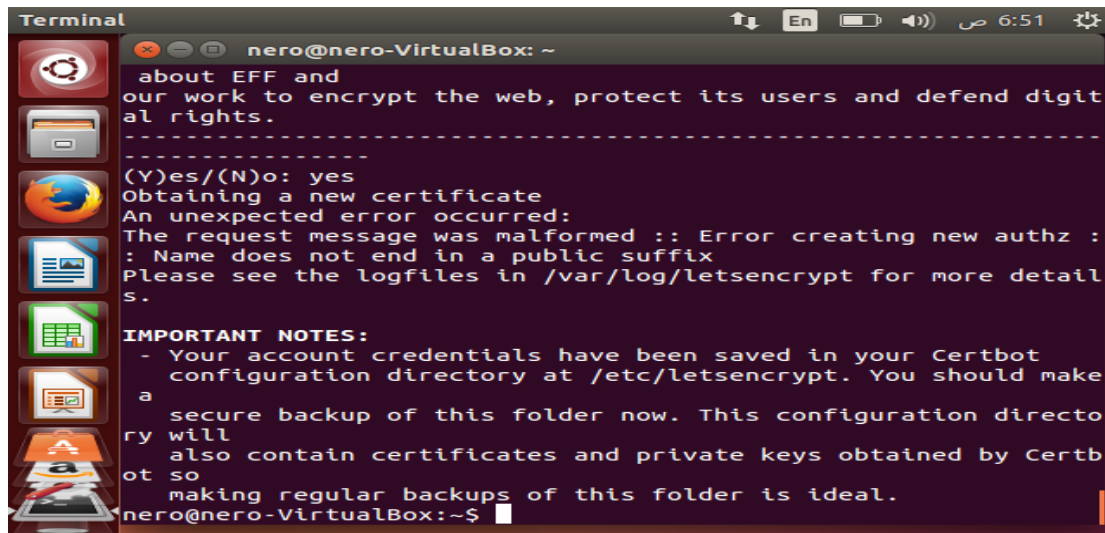
وبعد تعديله يتم التحقق اذا كان فيه اخطاء من خلال تنفيذ الايعازات التالية :

```
sudo nginx -t
sudo service nginx restart
certbot
```

والان يمكننا استعمال البرنامج المساعد التالي: web root لطلب شهادة SSL من خلال الايعاز

`certonly --webroot --webroot-path=/usr/share/nginx/html -d example.com -d www.PHP3.com`

PHP3.com هو اسم موقع تجاري مستضاف على الخادم, ومن ثم يتم اعطاء شهادة رقمية كما في الشكل (6) :



الشكل (6) منح الشهادة الرقمية للخادم

اذا كان المخرج يحتوي على تلك الملاحظات IMPORTANT NOTES , هذا يعني بانه تم الحصول على الشهادة الرقمية ولكي نكون على دراية بموقع ملفات الشهادة الرقمية من خلال الايعاز التالي :

`sudo ls -l /etc/letsencrypt/live/your_domain_name`

2-5 تشكيل SSL /TLS على خادم الويب Nginx

الان بعد ان تم امتلاك شهادة SSL , نحتاج الى تهيئة الخادم لأستعمالها لذلك نحرر بياناته الاولى لفتح ملف التهيئة للخادم يتم من خلال كتابة الايعاز التالي في نافذة terminal الخاصة بنظام Linux .

```
sudo nano /etc/nginx/sites-available/default
```

```
listen 80 default_server;
```

عند فتح الملف أولاً يتم حذف الخطوتين

```
listen [::]:80 default_server ipv6only=on;
```

تم حذف المنفذ 80 الذي يستعمله الخادم افتراضياً، ثم تم إضافة المنفذ 443 مع إضافة إمكانيات SSL .

```
listen 443 ssl;
```

```
server_name example.com www.example.com;
```

```
ssl_certificate/etc/letsencrypt/live/example.com/fullchain.pem;
```

```
ssl_certificate_key/etc/letsencrypt/live/example.com/privkey.pem;
```

وهنا يتمكن الخادم من استعمال SSL واستعمال الشهادة التي حصلنا عليها من هيئة التوثيق بعدما نقوم بإعادة تشغيل الخادم .

```
sudo service Nginx restart
```

6-2 التمكين من إعادة تجديد الشهادة الآلي

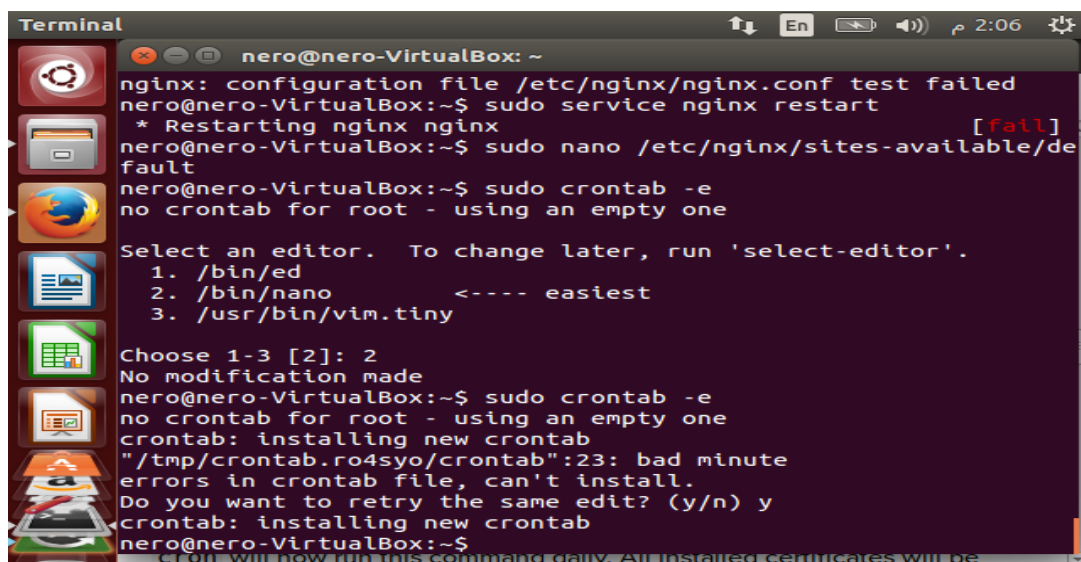
في هذه المرحلة يتم إعطاء فترة زمنية للشهادة الرقمية وسوف تكون الشهادة الرقمية صالحة لمدة تسعين يوماً هذا لتشجيع المستعملين على تجديد الشهادة الخاصه بهم سوف نحتاج الى اوامر تشغيل قانونية للتحقق من انتهاء صلاحية الشهادة وتجديدها تلقائياً (cron). هي خدمة نظام قياسية لتشغيل الوظائف الدورية . استدعاء ال cron ليقيم بعمله يتطلب فتح وتحرير ملف يدعى

```
sudo crontab -e
```

نضيف النص التالي في نهاية الملف

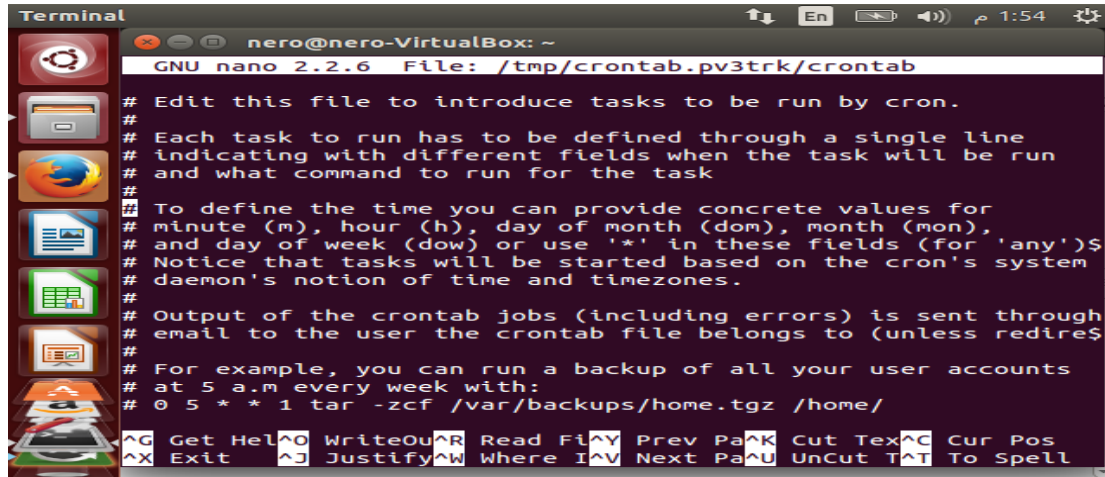
```
15 3 * * * /usr/bin/certbot renew --quiet --renew-hook "/usr/sbin/service nginx reload"
```

الرقم يعني تشغيل اوامر فحص التجديد في الساعة 3:15 am كل يوم ويمكن ان نختار أي وقت , لذلك يمكن تجديد الشهادة متى ما انتهت مدتها . هناك عدة اشكال توضح كيفية فتح الملف crontab والتعديل عليه.



الشكل (7) استدعاء crontab

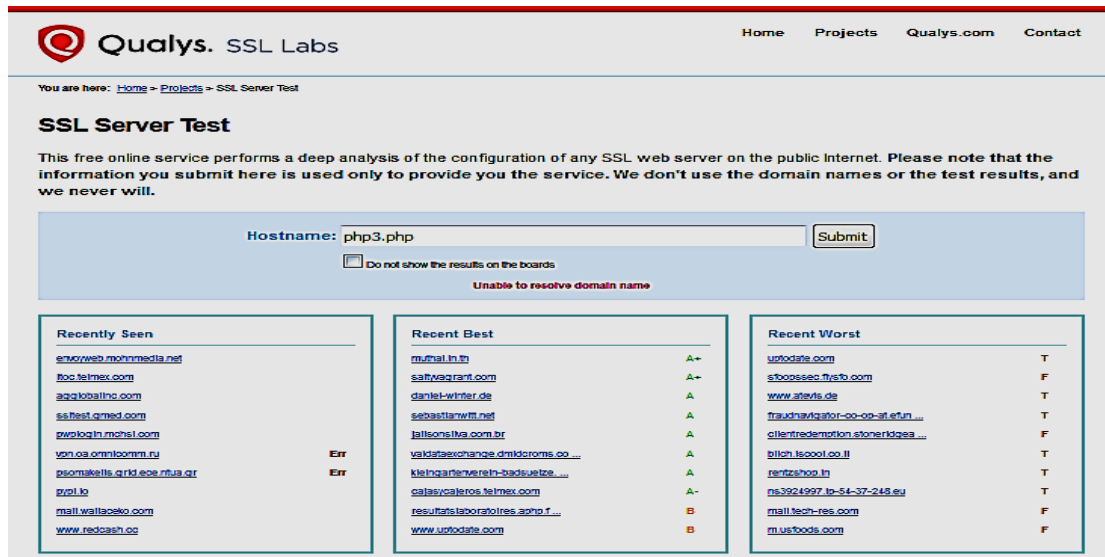
في الشكل (7) عند اختيار الرقم 2 التي تؤثر بسهم وهي /bin/nano سوف يظهر crontab ويتم كتابة النص المذكور سابقاً أسفل الملف وكما مبين بالشكل (8). وبذلك تم انجاز مهمة تجديد الشهادة.



الشكل (8) ملف crontab

4- النتائج والمناقشة

تقنية و شهادة SSL الان طبقت من هيئة التوثيق عن طريق عمل موقع تجاري (php3.php) يضم مكتبة لبيع الكتب , واستضافة ذلك الموقع على الخادم المستخدم بالبحث , ومن هذه اللحظة نستطيع اختبار ان التقنية والشهادة تعمل على النحو الصحيح , وذلك عن طريق زيارة المجال الخاص بنا في موقع هيئة التوثيق عن طريق متصفح الويب من خلال مختبرات SSL Qualys' . <https://www.Sslabs.com/ssltest/analyze.html?d=PHP3.PHP> . اذ يظهر مجموعة تقديرات اداء مواقع الخدمة على الخادم المستعمل والموقع المستضاف. وكما مبين بالشكل (9) .



الشكل (9) اختبار SSL

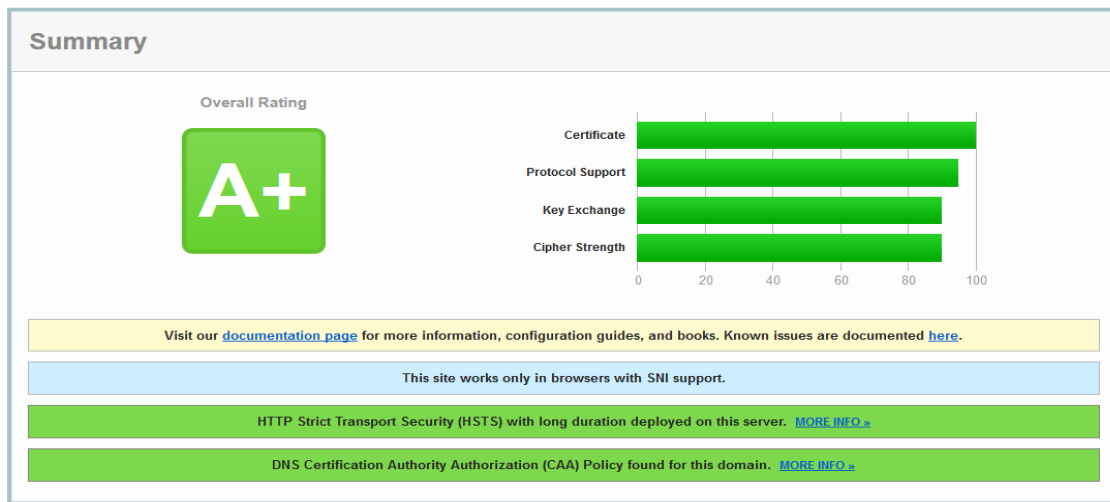
من ملاحظة الشكل (9) يتبين بأن هناك ثلاث مجموعات من مواقع الخدمات المرتبطة ب SSL والتي تقدم خدمات معينة (قوة التشفير , تبديل المفتاح , بروتوكول الدعم , الشهادة , درجة تقييم اداء الخدمة) فالمجموعة الاولى على اليسار تضم كل مواقع الخدمة المرئية حديثاً (Recently Seen) والمجموعة الثانية تضم مواقع الخدمة الافضل حالياً (Recent Best) والمجموعة الثالثة تضم المواقع الاسوء خدمة حالياً (Recent Worst). ان كل موقع خدمة من مواقع الخدمة المذكورة في الشكل (9) تقدم تقييم لأداء الموقع التجاري

المستخدم وما تقدمه مواقع الخدمة من خدمات حسب تقارير مختبرات SSL. ان الجداول (1) و(6) و(9) توضح تقييم الاداء لكل خدمة مع التقدير . الجداول مقسمة حسب مجموعات مواقع الخدمة الافضل والحالية والاسوء المذكورة في الشكل السابق .

جدول رقم (١) تقييم مواقع الخدمة الافضل حالياً حسب تقرير مختبرات SSL

Grade	Cipher Strength	Key Exchange	Protocol Support	Certificate	Name of Service
A+	90	90	93	100	muthai.in.th
A+	90	90	93	100	saltyvagrant.com
A	90	90	93	100	daniel-winter.de
A-	90	90	93	100	cajasycajeros.telmex.com
B	90	90	97	100	resultatslaboratoires.aphp.fr

يحصل موقع الخدمة على التقدير A+ وهي اعلى نسبة تقدير للأداء اذا كان الموقع يقدم الخدمات بالنسب التالية (قوة الشهادة 100% , بروتوكول الدعم 93% , تبديل المفتاح 90% , قوة التشفير 90%) وكما موضح بالشكل(10).



الشكل (10) يوضح نسب الخدمات حسب التقدير A+

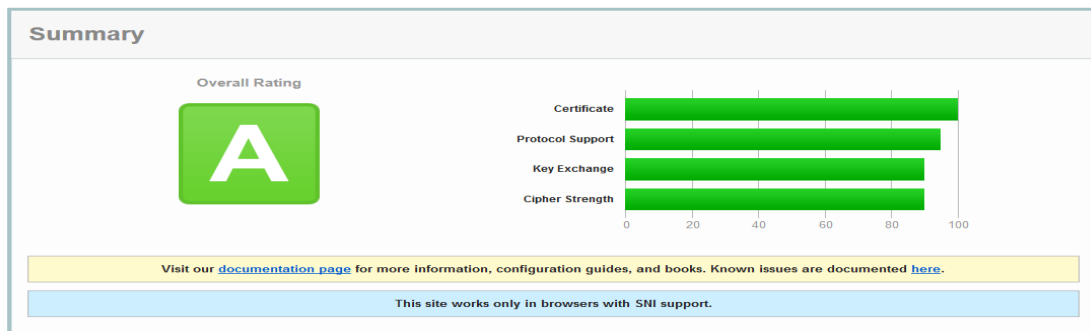
ان خصائص التقدير A+ تكون حسب نسب الخدمات التي يقدمها الموقع اضافة الى تقييم كل خدمة حسب نوعية وقوة الالية المستعملة في الخدمة, بالنسبة للموقع الحاصل على التقدير A+ تكون خصائصه موجزة بالجدول (2).

جدول رقم (٢) الخدمة ومميزاتها للتقدير A+

Properties	Service
RSA 4096 bits (SHA256withRSA)	Certificate
RSA 4096 bits	Key
SHA256withRSA	Signature algorithm
Let's Encrypt Authority X3 http://cert.int-x3.letsencrypt.org/	Issuer
Handshake, TLS 1.2, TLS 1.1, TLS 1.0	Protocols
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Cipher Suites
Firefox TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Handshake Simulation

يتم ملاحظة المعلومات في الجدول(2) ان الشهادة مشفرة باستعمال طريقة RSA لكل 4096 bits مع التوقيع الرقمي, ومفتاح الشفرة يستعمل ايضاً RSA لكل 4096 bits, كذلك خوارزمية التوقيع الرقمي تستعمل طريقة SHA256 مع RSA, و ان مصدر الشهادة الرقمية هو الهيئة (Let's Encrypt Authority X3) وموقع الهيئة (<http://cert.int-x3.letsencrypt.org/>), اما البروتوكولات

المستعملة (Handshake, TLS 1.2, TLS 1.1, TLS 1.0) هنا يتم ملاحظة ان البرتوكول باللون الاخضر هو من الاصدارات الاحدث وملائم جداً مع موقع الخدمة المعني , اما بالنسبة لطرائق التشفير مع البرتوكولات التي يستعملها (TLS_ECDHE_RSA مع AES_256_GCM_SHA384) تكون ملائمة . من الجدير بالذكر ان ECDHE هي مختصر Elliptic Curve Diffie-Hellman Exchange) هو الاساس لبرتوكول ارتباط الويب الامن SSL التقليدي وهو مدعم بواسطة كل المستعرضات الحديثة [7]. كذلك تجري مصافحة الموقع مع المتصفح Firefox (وهو المتصفح المستعمل بالعمل) عن طريق احدى طرائق التشفير و البرتوكولات المذكورة (TLS_ECDHE_RSA مع AES_256_GCM _ SH A256). اما اذا كان التقدير A يحصل موقع الخدمة على نسبة عالية للأداء اذا ان الموقع يقدم الخدمات بالنسب التالية (قوة الشهادة 100%, برتوكول الدعم 93%, تبديل المفتاح 90%, قوة التشفير 90%) وكما مبين بالشكل (11).



الشكل (11) يوضح نسب الخدمات حسب التقدير A

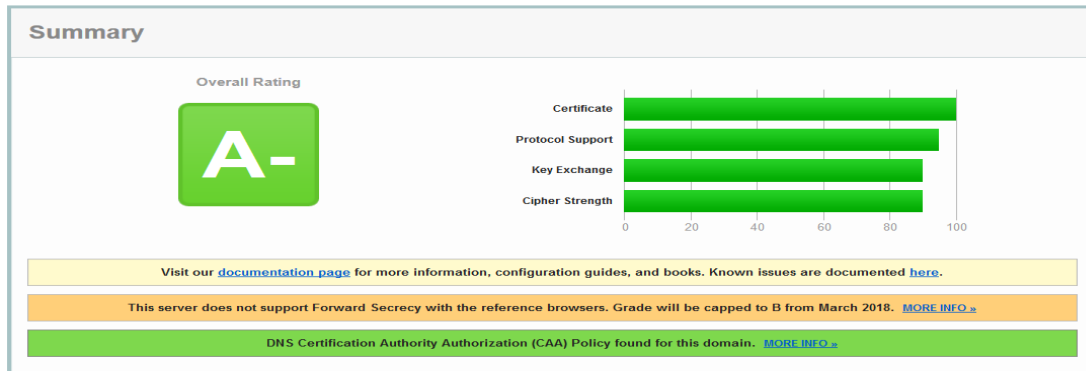
ان خصائص التقدير A تكون حسب نسب الخدمات التي يقدمها الموقع اضافة الى تقييم كل خدمة حسب نوعية وقوة الالية المستعملة في الخدمة , يجب ان نلاحظ ان مواقع الخدمة هنا تعمل فقط على المتصفحات التي تدعم SNI (هي مختصر Server Name Indication أي بمعنى اشارة اسم الخادم وهي تدير عدة شهادات SSL على نفس عنوان IP) [8]. ان الموقع الحاصل على التقدير A تم ايجاز خصائصه في الجدول (3).

جدول رقم (3) الخدمة وخصائصها للتقدير A

Properties	Service
RSA 2048 bits (SHA256withRSA)	Certificate
RSA 2048 bits	Key
SHA256withRSA	Signature algorithm
Let's Encrypt Authority X3 http://cert.int-x3.letsencrypt.org/	Issuer
Handshake , TLS 1.2 , TLS 1.1, TLS 1.0	Protocols
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Cipher Suites
Firefox	Handshake Simulation

من ملاحظة الجدول اعلاه ان الشهادة مشفرة بأستعمال طريقة RSA لكل 2048 bits مع طريقة التوقيع الرقمي, المفتاح يستعمل ايضاً RSA لكل 2048 bits , خوارزمية التوقيع الرقمي تستعمل طريقة SHA256 مع RSA, المصدر للشهادة الهيئة (Let's Encrypt Authority X3) مع ذكر موقع الهيئة (<http://cert.int-x3.letsencrypt.org/>), البرتوكولات المستعملة (Handshake, TLS 1.2, TLS 1.1, TLS 1.0) يمكن ملاحظة ان البرتوكول باللون الاخضر هو من الاصدارات الاحدث و ملائم جداً مع موقع الخدمة المعني, بالنسبة لطرائق التشفير مع البرتوكولات التي يستعملها الموقع وهي TLS_ECDHE_RSA مع AES_256_GCM_SHA384 تكون ملائمة , وتجري مصافحة الموقع مع المتصفح Firefox (وهو المتصفح المستعمل بالعمل) بأستعمال احدى طرائق التشفير و البرتوكولات المذكورة في الخدمة TLS_ECDHE_RSA مع AES_256_CBC_SHA .

يُحصل موقع الخدمة على التقدير - A وهي نسبة تقدير للأداء إذا كان الموقع يقدم الخدمات بالنسب التالية (قوة الشهادة 100% , بروتوكول الدعم 93% , تبديل المفتاح 90% , قوة التشفير 90%), كما موضح بالشكل (12).



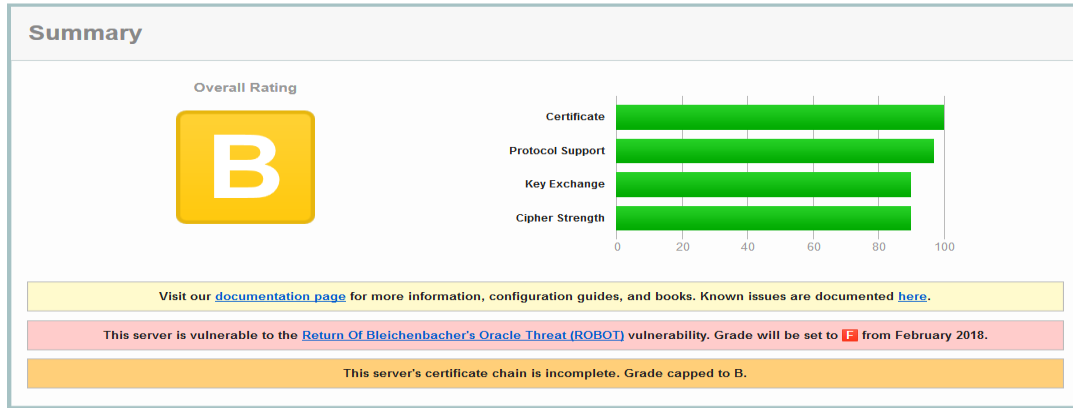
الشكل (12) يوضح نسب الخدمات حسب التقدير - A

ان خصائص التقدير - A تكون حسب نسب الخدمات التي يقدمها الموقع اضافة الى تقييم كل خدمة حسب نوعية وقوة الالية المستعملة في الخدمة , نلاحظ هنا ان الخادم في تلك المواقع لا يدعم السرية بالنسبة لمصدر المتصفحات , ان الموقع الحاصل على التقدير - A تكون خصائصه موزعه في الجدول (4).

جدول رقم (4) الخدمة ومميزاتها للتقدير - A

Properties	Service
RSA 2048 bits (SHA256withRSA)	Certificate
RSA 2048 bits	Key
SHA256withRSA	Signature algorithm
DigiCert SHA2 Secure Server CA http://cacerts.digicert.com/DigiCertSHA2SecureServerCA.crt	Issuer
Handshake, TLS 1.2	Protocols
TLS_RSA_WITH_AES_256_GCM_SHA384 WEAK	Cipher Suites
Firefox TLS_RSA_WITH_AES_128_CBC_SHA	Handshake Simulation

من ملاحظة الجدول اعلاه ان الشهادة مشفرة بأستعمال طريقة RSA لكل 2048 bits مع طريقة التوقيع الرقمي, المفتاح يستعمل ايضاً RSA لكل 2048 bits, خوارزمية التوقيع الرقمي تستعمل طريقة SHA256 مع RSA, المصدر للشهادة الهيئة (DigiCert SHA2 Secure Server CA) مع ذكر موقع الهيئة (<http://cacerts.digicert.com/DigiCertSHA2SecureServerCA.crt>), البروتوكولات المستعملة فقط (Handshake, TLS 1.2) يمكن ملاحظة ان البروتوكول باللون الاخضر هو من الاصدارات الاحدث وملائم جداً مع موقع الخدمة المعني , بالنسبة لطرائق التشفير و البروتوكولات التي يستعملها الموقع وهي TLS_RSA مع AES_256_GCM_SHA384 تكون ضعيفة وغير ملائمة , وتجرى مصافحة الموقع مع المتصفح Firefox (وهو المتصفح المستعمل بالعمل) عن طريق احدى طرائق التشفير والبروتوكولات المذكورة في الخدمة TLS_RSA مع AES_128_CBC_SHA . يحصل موقع الخدمة على التقدير B وهي نسبة تقدير للأداء إذا كان الموقع يقدم الخدمات بالنسب التالية (قوة الشهادة 100% , بروتوكول الدعم 97% , تبديل المفتاح 90% , قوة التشفير 90%) كما موضح بالشكل (13).



الشكل (13) يوضح نسب الخدمات حسب التقدير B

ان خصائص التقدير B تكون حسب نسب الخدمات التي يقدمها الموقع اضافة الى تقييم كل خدمة حسب نوعية وقوة الالية المستعملة في الخدمة , نلاحظ هنا ان سلسلة الشهادات الرقمية للخوادم غير مكتملة , ان الموقع الحاصل على التقدير B تم ايجاز خصائصه في الجدول (5).

جدول رقم (5) الخدمة وخصائصها للتقدير B

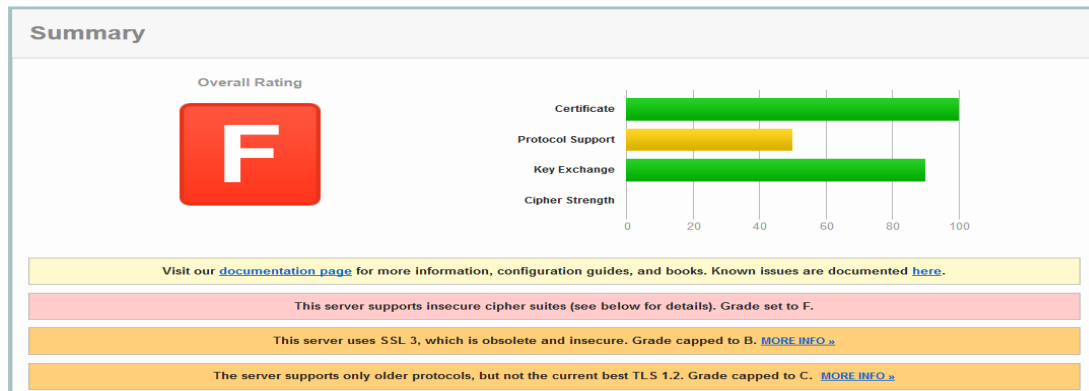
Properties	Service
RSA 2048 bits (SHA256withRSA)	Certificate
RSA 2048 bits	Key
SHA256withRSA	Signature algorithm
GlobalSign Domain Validation CA - SHA256 - G2 http://secure.globalsign.com/cacert/gsdomainvalsha2g2r1.crt	Issuer
Handshake, TLS 1.2, TLS 1.1	Protocols
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Cipher Suites
Firefox TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256_ECDH	Handshake Simulation

من ملاحظة الجدول اعلاه ان الشهادة مشفرة بأستعمال طريقة RSA لكل 2048 bits مع طريقة التوقيع الرقمي , المفتاح يستعمل RSA لكل 2048 bits, خوارزمية التوقيع الرقمي تستعمل طريقة SHA256 مع RSA, المصدر للشهادة الهيئة (GlobalSign Domain Validation CA - SHA256 - G2) مع ذكر موقع الهيئة (<http://secure.globalsign.com/cacert/gsdomainvalsha2g2r1.crt>) نلاحظ ان البرتوكول باللون الاخضر هو من الاصدارات الاحدث وملائم جداً مع موقع الخدمة المعني , بالنسبة لطرائق التشفير والبرتوكولات التي يستعملها الموقع وهي TLS_ECDHE_RSA مع AES_128_GCM_SHA256 تكون ملائمة , وتجري مصافحة الموقع مع المتصفح Firefox (وهو المتصفح المستعمل بالعمل) بواسطة طرائق التشفير والبرتوكولات المذكورة في الخدمة (TLS_ECDHE_RSA مع AES_128_GCM_SHA256_ECDH) . ان ECDH مختصر ل Elliptic Curve Diffie- Hellman هو بروتوكول اتفافية المفتاح المجهول تسمح للطرفين بامتلاك مفتاحين , عام وخاص لتأسيس امن مشترك على القناة غير الآمنة هذا الامن المشترك ربما يستعمل كمفتاح او يستعمل لأشتقاق مفتاحاً اخرأ يستعمل لتشفير الاتصالات اللاحقة بأستعمال تشفير مفتاح متماثل هو مغاير الى بروتوكول Diffie-Hellman اذ يستعمل كتابة منحني مشفرة اهليلجية[9].

جدول رقم (٦) يوضح مواقع الخدمة المرئية حالياً حسب تقرير SSL

Grade	Cipher Strength	Key Exchange	Protocol Support	Certificate	Name of Service
A	90	90	93	100	envoyweb.mohnmedia.net
A	90	90	93	100	itoc.telmex.com
A	90	90	93	100	mail.wallaceko.com
Assessment failed: Unable to connect to the server					vpn.oa.omnicomm.ru
Assessment failed: Unable to connect to the server					psomakelis.grid.ece.ntua.gr

يوضح الجدول رقم (6) مواقع الخدمة المرئية حالياً ان اغلب تقديرات الخدمة هي A وتوجد مواقع غير قادرة على الربط بالخادم حالياً اذ تعطي تقييمات خاطئة . يحصل موقع الخدمة على التقدير F وهي نسبة تقدير للأداء اذا كان الموقع يقدم الخدمات بالنسب التالية (قوة الشهادة 100% , بروتوكول الدعم 50% , تبديل المفتاح 90% , قوة التشفير 0%) ويبين الشكل (14) ذلك بوضوح.



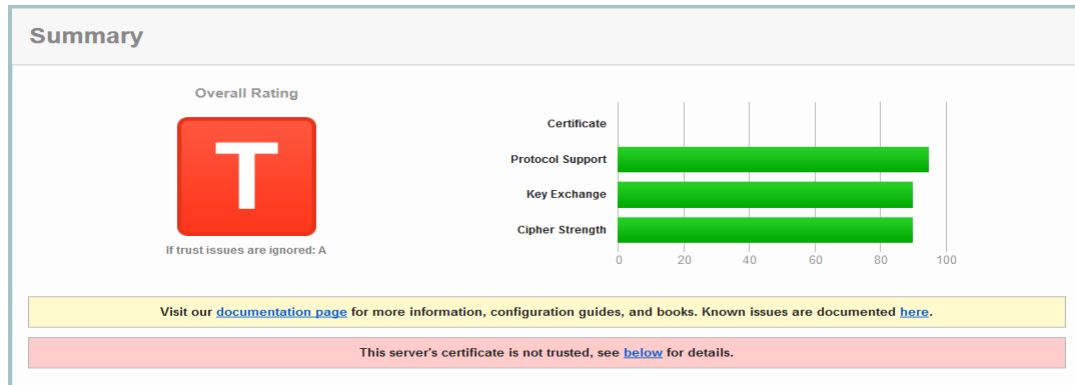
الشكل (14) يوضح نسب الخدمات حسب التقدير F

ان خصائص التقدير F تكون حسب نسب الخدمات التي يقدمها الموقع اضافة الى تقييم كل خدمة حسب نوعية وقوة الالية المستعملة في الخدمة , نلاحظ هنا ان الخوادم تدعم طرائق تشفير غير امنية وتستخدم بروتوكولات قديمة. بالنسبة للموقع الحاصل على التقدير F تكون خصائصه موجزة في الجدول (7).

جدول رقم (٧) الخدمة وخصائصها للتقدير F

Properties	Service
RSA 2048 bits (SHA256withRSA)	Certificate
RSA 2048 bits	Key
SHA256withRSA	Signature algorithm
COMODO RSA Organization Validation Secure Server CA http://crt.comodoca.com/COMODORSAArganizationValidationSecureServerCA.crt	Issuer
Handshake,TLS 1.0 , SSL 3 INSECURE	Protocols
TLS_RSA_WITH_RC4_128_MD5 INSECURE	Cipher Suites
Firefox TLS_RSA_WITH_3DES_EDE_CBC_SHA	Handshake Simulation

من ملاحظة الجدول اعلاه ان الشهادة مشفرة بأستعمال طريقة RSA لكل 2048 bits مع طريقة التوقيع الرقمي , المفتاح يستعمل RSA لكل 2048 bits, خوارزمية التوقيع الرقمي تستعمل طريقة SHA256 مع RSA, المصدر للشهادة الهيئة (COMODO RSA Organization Validation Secure Server CA) مع ذكر موقع الهيئة <http://crt.comodoca.com/COMODORSADomainValidationSecureServerCA.crt>, البرتوكولات المستعملة (Handshake, TLS 1.2, SSL 3) نلاحظ ان البرتوكول باللون الاخضر هو من الاصدارات الاحدث وملائم جداً مع موقع الخدمة المعني بينما SSL 3 المستعمل هنا غير امن , بالنسبة لطرائق التشفير والبرتوكولات التي يستعملها الموقع وهي TLS_RSA مع RC4_128_MD5 تكون غير آمنة, وتجري مصادقة الموقع مع المتصفح Firefox (وهو المتصفح المستعمل بالعمل) بواسطة طرائق التشفير والبرتوكولات المذكورة في الخدمة TLS_RSA مع 3DES_EDE_CBC_SHA . يحصل موقع الخدمة على التقدير T وهي اعلى نسبة تقدير للأداء اذا كان الموقع يقدم الخدمات بالنسب التالية (قوة الشهادة 90% , برتوكول الدعم 93% , تبديل المفتاح 90% , قوة التشفير 90%) وكما مبين بالشكل (15).



الشكل (15) يوضح نسب الخدمات حسب التقدير T

ان خصائص التقدير T تكون حسب نسب الخدمات التي يقدمها الموقع اضافة الى تقييم كل خدمة حسب نوعية وقوة الالية المستعملة في الخدمة , نلاحظ هنا ان الشهادات الرقمية للخوادم ليست موثوقة. ان الموقع الحاصل على التقدير T يوجز الجدول (8) خصائصه.

جدول رقم (٨) الخدمة وخصائصها للتقدير T

Properties	Service
RSA 2048 bits (SHA256withRSA) , NOT TRUSTED	Certificate
RSA 2048 bits	Key
SHA256withRSA	Signature algorithm
COMODO RSA Domain Validation Secure Server CA http://crt.comodoca.com/COMODORSADomainValidationSecureServerCA.crt	Issuer
Handshake, TLS 1.2, TLS 1.1, TLS 1.0	Protocols
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Cipher Suites
Firefox _ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH	Handshake Simulation

من ملاحظة الجدول اعلاه ان الشهادة مشفرة بأستعمال طريقة RSA لكل 2048 bits مع طريقة التوقيع الرقمي لكنها غير موثوقة , والمفتاح يستعمل RSA لكل 2048 bits, و ان خوارزمية التوقيع الرقمي تستعمل طريقة SHA256 مع RSA, كذلك المصدر للشهادة الهيئة COMODO RSA Domain Validation Secure Server CA مع ذكر موقع الهيئة (<http://crt.comodoca.com/COMODORSADomainValidationSecureServerCA.crt>), البرتوكولات المستعملة (TLS 1.0, TLS 1.1, TLS 1.2, Handshake) يمكن ملاحظة ان البرتوكول باللون الاخضر هو من الاصدارات الاحدث وملائم جداً مع موقع الخدمة المعني , بالنسبة لطرائق التشفير مع البرتوكولات التي يستعملها TLS_ECDHE_RSA مع AES_256_CBC_SHA384 تكون ملائمة , وتجري مصافحة الموقع مع المتصفح Firefox (وهو المتصفح المستعمل بالعمل) بواسطة طرائق التشفير والبرتوكولات ECDHE_RSA مع AES_256_CBC_SHA ECDH. هنالك عدة اسباب لكي تكون الشهادة الرقمية غير موثوقة وقد تمت الاشارة الى المشكلة في التقرير باللون الاحمر , وسببها احدى النقاط التالية :

- 1- شهادة رقمية لم يتم التحقق منها
 - 2- تهيئة للخادم لم يتم التحقق من صحتها
 - 3- الهيئة المانحة للشهادات الرقمية تكون مجهولة
- لذلك يجب تطوير البرتوكولات وطرائق التشفير من اجل معالجة الاسباب في النقاط 1 و 2, اما النقطة الثالثة فيجب التأكد من هيئة التوثيق المانحة للشهادات الرقمية قبل تقديم الطلب من صاحب الموقع التجاري للحصول على الشهادة .

جدول رقم (9) يوضح مواقع الخدمة الاسوء حالياً حسب تقرير SSL

Grade	Cipher Strength	Key Exchange	Protocol Support	Certificate	Name of Service
F	0	90	50	100	sfoopssec.flysfo.com
T	90	90	93	0	blich.iscool.co.il
T	90	90	93	0	rentzshop.in
F	0	90	50	100	mail.tech-res.com
T	90	70	93	0	www.atevis.de

من ملاحظة الجدول رقم (9) الذي يوضح مواقع الخدمة الاسوء حالياً ان اغلب تقديرات الخدمة هي F و T أي ان مواقع الخدمة فيها غير موثوقة وغير امانة .

4- الاستنتاج

ان من اهم المشاكل التي تواجه التجارة الالكترونية هي التحديات المتعلقة بالامن والخصوصية وحماية المعلومات. لذلك فإن امكانية خلق بيئة امانة للمواقع التجارية تؤدي الى امكانية الشراء بطريقة امانة في أي وقت واي دولة وباستطاعة أي شخص ان يشتري الشئ الذي يرغب فيه من ابعد دولة .فالتجارة الالكترونية بصورة او بأخرى ادت الى تقريب المسافات بين الدول.

من خلال هذا البحث تم استنتاج ما يلي :

- امكانية تأمين الموقع التجاري وكسب ثقة الزبائن والعميل عن طريق اضافة تقنية SSL وشهادته من هيئة موثوقة على الخادم الويب لخدمة محتوى HTTP بشكل امن , والتأكد من عملها عن طريق متابعة مجال الخادم في موقع هيئة التوثيق.

- العمل على نظام Linux يعطي تأمين وإمكانية أعلى مقارنة بنظام Windows , إذ إن الشركات التي تصدر الشهادات الرقمية تمنح الخادم ميزات إضافية ممكن برمجتها على نظام Linux لأنه مفتوح المصدر , ولا يمكن إضافتها في حال استعمال نظام Windows.
- من خلال درجات التقدير الموجودة في مواقع الخدمة والتي تحدد تقييم الأداء يمكن لصاحب الموقع معرفة درجة الأمان بالنسبة للموقع التجاري التابع له .
- من خلال مجال الخادم في موقع هيئة التوثيق ممكن معرفة إذا كانت مواقع الخدمة في حالة صيانة, وبهذا يتوجب إيقاف التعامل التجاري لفترة تجنباً للاختراق أو إمكانية نقل الموقع التجاري إلى موقع خدمة آخر .

5- العمل المستقبلي

إضافة تقنية ل Secure Electronic Transactions (SET) وهي تقنية تؤمن الصفقات بين الشركات التي تتم عن طريق الـ VISA CARD عن طريق الإنترنت. وهذا يتطلب طرف آخر في العمل وهو المصرف , إذ إن البحث يحتوي على طرف واحد فقط وهو الموقع التجاري . ويتم إضافة تقنية SET إلى خادمي كلا الطرفين و تأمين توقيع ثنائي رقمي لخادم التاجر وخادم المصرف .

Acknowledgements:

Maha Abdul Latif Sayal is a teacher working at Thi-Qar University / College of Computer Science and Mathematics. Bachelor in Computer Science from the College of Science / Thi- Qar University (2005). Master in Computer Science specialization Cloud Computing College of Science / University of Baghdad (2015), currently PhD student College of Computer Science and Mathematics / University of Kufa.

المصادر

- 1- Aba Zaid, d. Thanaa, Tishreen University Journal for Studies and Scientific Research, Economic and Legal Sciences Series Volume 27, No. 4, 2017.
- 2- Nabil Mahdi Al-Janabi, Muhammad Al-Zaidi, Muhammad Nima, "Economic Intelligence is the only entry point to Knowledge Intelligence", Al-Qadisiyah University, 2018.
- 3- Ibrahim Ahmed Abdel-Khaleq Al-Dawi, "E-Commerce An Applied Study on Libraries", King Fahd National Library for Printing and Publishing, 2016.
- 4- Boss, Richard W. "E-Commerce for Libraries". McGraw Hill. August 2007.
- 5- Thamer Abdul-Ali Kazem Al-Shammari, Fadel Abbas Kazem Al-Shabani, Al-Qadisiyah Journal of Administrative and Economic Sciences, Volume 16, Issue 1, Year 2014.

- 6- Kurdish Ahmed El-Sayed, "Arab E-Commerce... Prospects and Challenges," Encyclopedia of Islam and Development, 2017.
- 7- Hanaa Syed Jawad Al-Nasser, "The Impact of E-Commerce on Competition in Arab Local Markets", Research Study: Arab Democratic Center, 2017.
- 8- Hala Al-Hassan, Damascus University Journal for Economic and Legal Sciences - Volume 30 - First Issue. 2014
- 9- William Stallings, "Principles and Practices of Cryptography and Network Security, Fourth Edition," ISBN 10: 0-13-187316-4, Prentice-Hall, 2005.
- 10- Mohammed Al-Banat, "Electronic Contracts. Symposium on Electronic Commerce Contracts and their Areas", Cairo, Arab Administrative Development Organization, 2013.
- 11- Farouk Sayed Hussein, "Electronic Commerce and Insurance", Arab Printing House and Hala Publishing and Distribution, 2015.