The Use of SSL and TLS Protocols in Providing a Secure Environment for e-commerce Sites

M.A. Sayal*
Computer Science Department, Faculty of Computer Science & Mathematics, University of Kufa.
E-mail: maha.asyal@utq.edu.iq

M.H. Alameady
Computer Science Department, Faculty of Computer Science & Mathematics, University of Kufa.
E-mail: maali.alameedi@uokufa.edu.iq

S.A. Albermany
Computer Science Department, Faculty of Computer Science & Mathematics, University of Kufa.
E-mail: salah.albermany@uokufa.edu.iq

Received July 12, 2020; Accepted September 14, 2020
ISSN: 1735-188X
DOI: 10.14704/WEB/V17I2/WEB17048

Abstract

The problem is that e-commerce is not reliable and people are afraid to buy things and make transactions with commercial websites. Only some well-known companies have a known digital document from where it was issued. To solve this problem and to document any individual commercial website, We suggested to design a personal commercial website, it is a website to buy books and enable access to a domain by purchasing it from the digital ocean cloud, then a server is installed in this domain and then we connect it to the digital certification from the website (lets encrypt), where certain software are added to client (certbot, root) server assistant program, and we have linked the server and the certification together via Linux instructions and codes. The commercial website. (PHP3.PHP) has been tested in SSL laboratories and the results are the division of service sites into three categories: current, best current, and worst currently with details of categories, and what are the weaknesses.

Keywords

Commercial Sites, Secure Socket Layer (SSL), Digital Certificate, Internet Transactions.

Introduction

E-commerce has become an important part of building the economy in the future, as trade here has become related to technology and its impact on the expansion and development of traditional trade prospects. Therefore, it is necessary to clarify this technology understanding, and challenges.

1) Electronic Commerce Concept

E-commerce is known as the process of buying and selling or exchanging the products, information and services through local, international and global networks, including the Internet[1]. It is a technical process that makes business transactions take place automatically and quickly from the economic and business point of view[2].

Shopping in online shopping centers, internet banks, buying shares and collaborating with the individuals in doing some research work are all examples of what is known as e-commerce applications [3]. To implement all of these applications, it requires the information support, infrastructure and advanced systems. E-commerce applications are supported by some infrastructures[4]. Performing these applications requires relying on four corner stones: people, customs, technical protocols, public policy, and other factors [5].

2) Challenges Facing E-Commerce

One of the most important challenges in the subject of e-commerce is the protection of information and this is the problem of research[6], as it is possible to violate privacy, security, information or interception and control of mail sent between the company or seller and the consumer[7]. And penetrating third parties to access customer data and identify the company's privacy. If the existence of a security curtain is denied because the mere access to the customer's personal computer can obtain information that leads to the methods of communication with customers and can communicate with them [8]. And flood the company with losses by knowing their inclinations and customers' wishes and thus the company's heavy losses and this is why the accounts and credit cards of customers and buyers are exposed to theft if there are no safe encryption methods [9].

Hence it was found that it is necessary to seek to solve this problem to maintain privacy and security and protect both the company and customers and customers[10], as the protection of the server of the commercial company for the company and the customer and the protection of the commercial site for the company and the customer, as the information passed between the two parties is encrypted through SSL technology and

used in the digital certificate that can be obtained from the Digital Certification Authority [11].

3) SSL/TLS and theirs Operating Mechanism

SSL or TLS is a program that contains some specialized encryption protocols in order to transfer information and some data that is encrypted between only two devices by Internet in a protected way therefore no one can be able to read it without the sender of the data and its future and the encryption method is also very complex and difficult to decipher, and it is different from the other encryption methods in one specific thing, which is the sender of the data has nothing to do with taking a step to encrypt the information in order to be protected [12].

This technology-based software encrypts any information from that browser to the server of the commercial location on which it is hosted, using the Transmission control protocol and the Internet, known as TCP/IP. The reason for calling it the security layer is because this program acts as a middle layer that links the Transport Control Protocol with the Multiple Text Transfer Protocol (HTTP).

The steps to use this technique are summarized as follows:

1. The Documentation Authority issues the digital certificate for the site after submitting a request from the owner of the commercial site to contain all the information that belongs to the authority such as the name of the authority and the date of issuance of the certificate and the date of completion, as well as the issuance of private keys and public keys to be stored SSL for the site and the site also secures a server device equipped with software to encrypt the public key of the site.
2. The browser provided by this program is connected to the secure server of the commercial site and asks it the following: digital certificate, its source, expiry date as well as the comparison between the name of the commercial site on the certification with the specific name of site in the servers device and comparison between the general number sent from the server to the browser with the electronic signature of the company, and all these steps are done to confirm if the site is credible and to protect the customer from the phantom company.
3. The information is encrypted to the customer by basis on public keys of the site to be transmitted in a very secure manners without interferences from it so no one can be able to steal or view the information except the site approved at the other party, which has the special key of the site to open and return the information to its normal state[13].

Proposed Work

The SSL is the way to encrypt location information and create a more secure link, in addition to that, the SSL certificate is offering identifying information about the protected server of site visitors.

In this research, it was proposed to install a specific server and then submitting a request in the form of digital certificate documentation to obtain SSL technology and certificate and then add it to the server and the sites hosted on it to secure its data and renew the certificate when it expires. Figure 1 (shown below) outlines the stages of providing a safe environment.

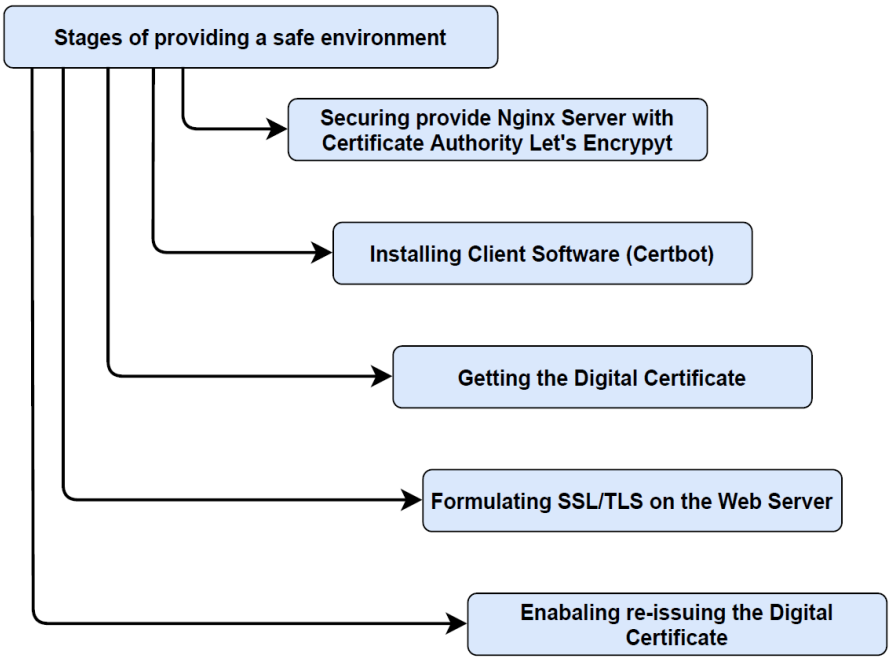

Figure 1 Summary of the stages of providing a safe environment.

Methodology

Here we will show how to programmatically apply the above.

1) Software and Operating System Used in Practical Part

The system used in this research is Linux version Ubuntu16.04 as the features of this system are that it is open source and safer than Windows system because it can be updated millions of times per minute, i.e. it is possible to add steps to the system root program and this is the reason for its use in this research, as well as this system is characterized by writing instructions in the form of commands more than using graphical interfaces for

these commands as we write the commands in the terminal window and add them to the root of the system. Windows system, on other hand needs to use the simulator of both ends of some commands to add commands used in the search on the system.

The software required work are initially configured as these software are a set for briefed by LEMP for (Linux, Nginx, MySQL, PHP) which represents a set of software that can be used to serve dynamic web pages and web applications, as L means Linux operating system, E is for the server used which is Nginx, and M is the database MySQL and P is for PHP, the dynamic language of writing websites.

It is worth mentioning that all instructions and programming codes are written in the Linux Terminal window. The steps of installing the Nginx server are as following:

- Sudo apt-get update
- Sudo apt-get install nginx

Figure (2) shows the steps of installing the server correctly and booking a place on the internet.

Figure 2 Installing Nginx server

2) Securing Nginx Server with Let's Encrypt

"Let's Encrypt" is a very new digital certification authority (CA) which provides a very easy way of obtaining and installing SSL and TLS certification and its ability to authorize encrypted HTTPs to work on web servers. Figure (3) shows the logo of the certification authority.

Figure 3 Let's Encrypt Logo

This section deals with how to provide a digital certificate SSL, how to add and use it with Nginx. Here, Nginx, which is a web server, is linked to digital certificate. We also will know how to renew the digital certificate. The configuration file contains rules in favor of files and requests since this prevents access to files with names that are found in the file /.well-known/acme-challenge/xxx. Figure (4) illustrates the mechanism for granting digital certificates.

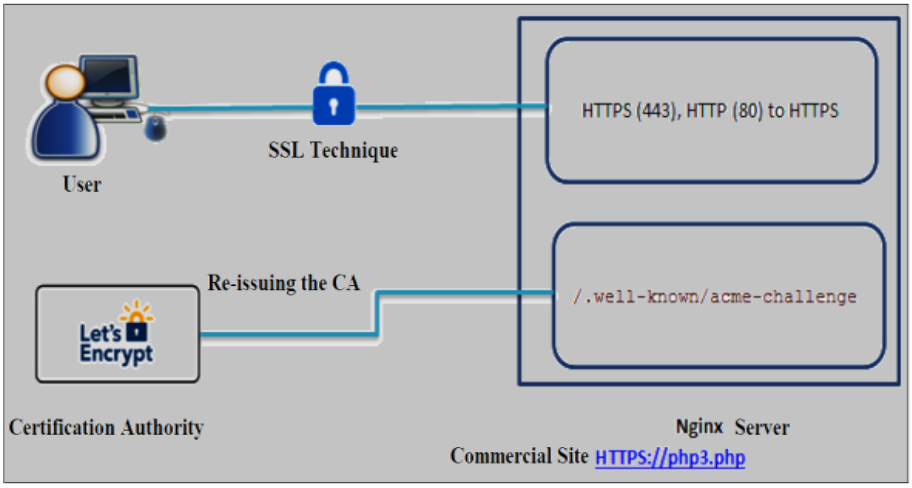

Figure 4 Mechanism of granting digital certificates

3) Installation of Client Software, Certbot

Certbot is a software that automatically tries to resolve most of the steps required for certification, let's Encrypt gives us the ease of obtaining a software SSL certificate regardless of the web server used.

In the first step, a storage warehouse is added through the following code:

sudo add-apt-repository ppa:certbot/certbot
sudo apt-get update (this is an update step)
sudo apt-get install Certbot (finally, installation is done)

4) Getting the Digital Certificate

"Let's Encrypt" is providing some methods for obtaining a certificate, and these methods or additions are called authentication. The additions are used in the event that a certificate must be issued to the server Nginx. The first basic step in obtaining the certificate is to use the plugin (web root) before using the plugin and we must be sure of the client software. To ensure that the client's software (certbot) can be accessed and validated, a change must be made on Nginx, as the nano command is used to open it and modify it:

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

After certbot is amended, it has to be verified if there are any errors that still there by implementing the following instructions:

sudo nginx –t

sudo service nginx restart

Now we are able to use web root plugin in order to request an SSL certification through the following instruction: certbot certonly – webroot – webroot-path=/usr/share/nginx/html-d as follows:

example.com -d "www.PHP3.com"

Where PHP3.com is the name of a commercial site hosted on the server, and then a digital certificate is given as in figure (5) below.

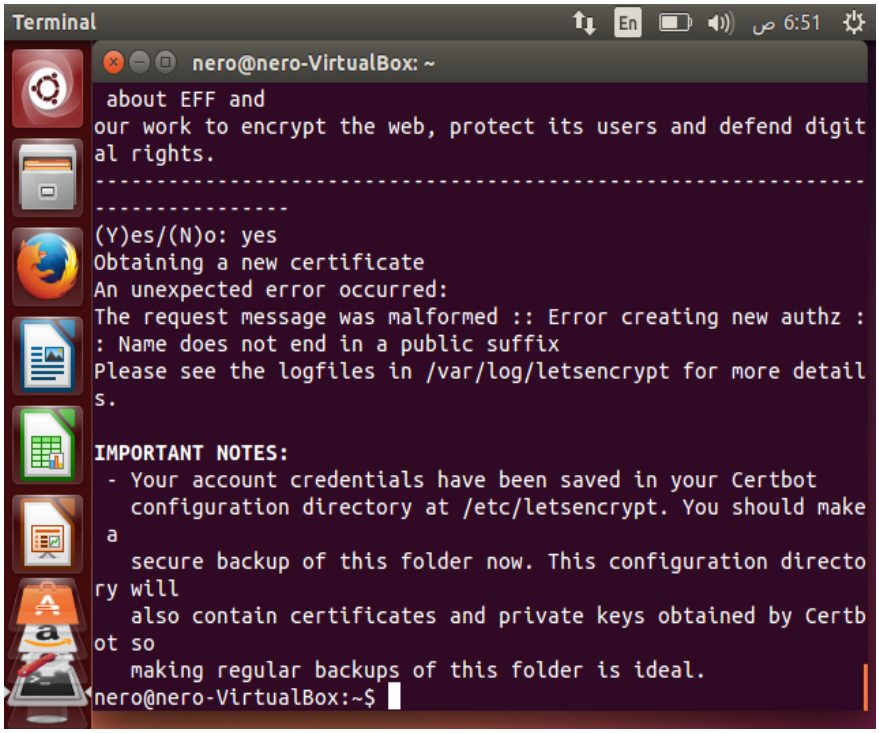

Figure 5 Granting the digital certificate to the server

If the output contains the phrase IMPORTANT NOTES, this means that the digital certificate has been obtained and to know the location of the digital certification files through the following instructions:

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

5) SSL/TLS Formation on Nginx Web Server

Now that the SSL certificate has been acquired, we need to configure the server to use it, so we edit its initial data to open the server's configuration file by writing the following instruction in the Linux terminal window:

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

When we open the file for the first time, the two steps

listen 80 default_server;

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

are deleted. Port 80 used by the server was deleted by default, and port 443 was added with the addition of SSL capabilities:

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;

This is where the servers can use both SSL and use the certificate that we obtained from the certification authority after we restart the servers:

sudo service Nginx restart

6) Enabling the Renewal of the Automated Certificate

At this stage, a period is given for the digital certificate and the digital certificate will be valid for 90 days. This is to encourage users to renew their certificate. We will need legal operating orders to verify the expiry of the certificate and renew it automatically. Cron is a standard system service for the operation of periodic functions. Calling the cron to do its job requires opening and editing a file called crontab. This is achieved by means of instruction:

sudo crontab -e

We must add all the following text to end of the file:

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

The number means that renewal check orders are turned on at 3:15 a.m. every day and we can choose any time, so the certificate can be renewed once it expires. There are several forms that illustrate how to open the crontab file and how to modify it.

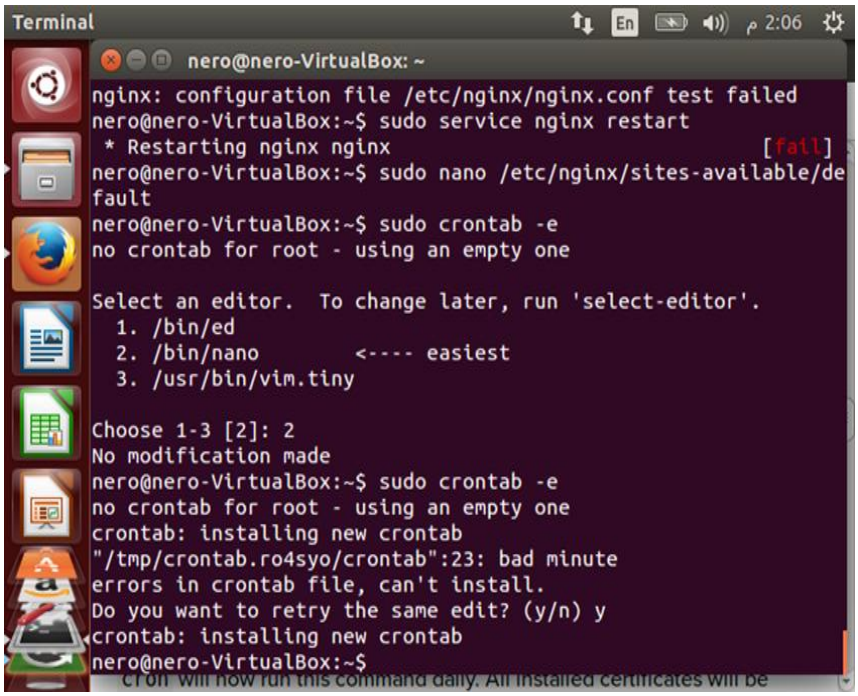

Figure 6 Calling cron

In figure (6), when we choose the number 2 that indicated by an arrow which is /bin/nano, crontab will appear. The text mentioned above is written at the bottom of the file and as shown in figure (7). Thus, the task of renewing the certificate was completed.

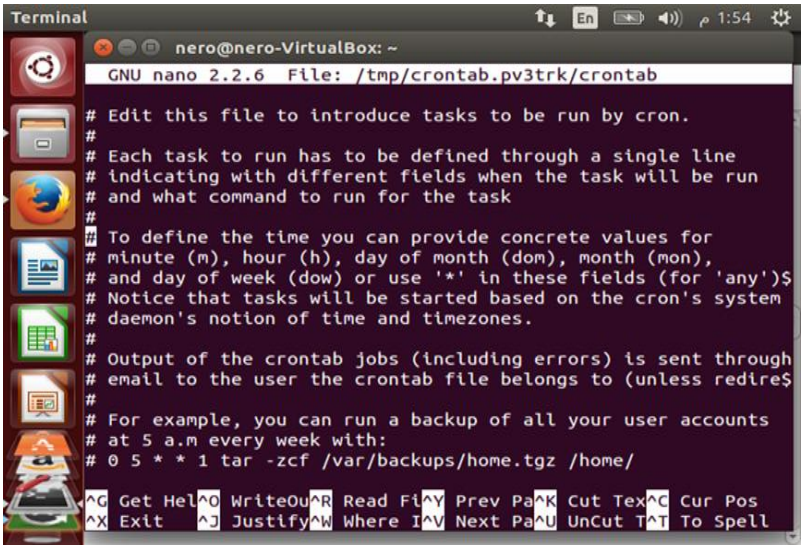

Figure 7 File crontab

Results and Discussion

SSL technology and certification are now applied by the Documentation Authority through the work of a commercial site (php3.php) that includes commercial website for the sale of books, and the hosting of that site on Nginx server. We can test this site and the services of SSL work properly or not. This is done by visiting our domain in the site of the documentation authority through the web browser through Qualys' SSL laboratories:

"https://www.Ssllabs.com/ssltest/analyze.html?d=PHP3.PHP"

This shows the set of service site performance estimates on the user server and hosted site as it is shown in figure (8).

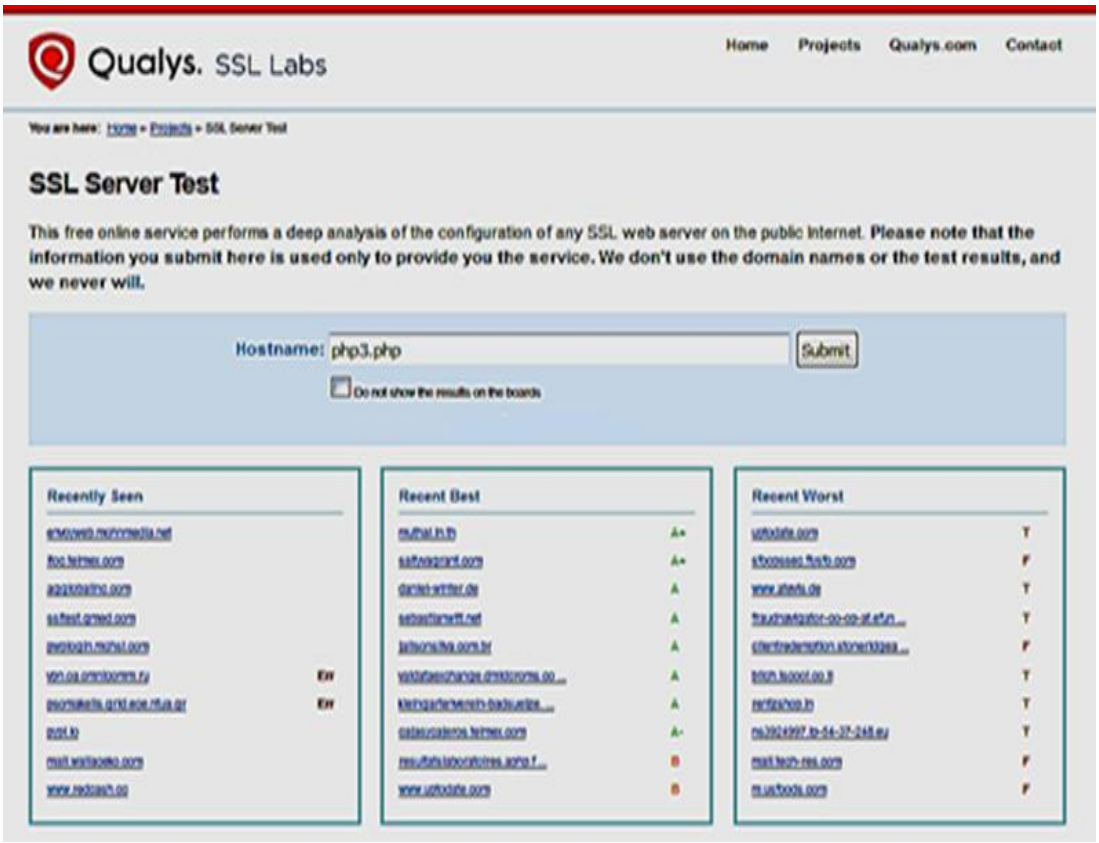

Figure 8 SSL test

From noticing figure (8), it is apparent that there are three sets of service sites associated with SSL that provide certain services (encryption strength, key switch, support protocol, certificate, service performance assessment) the first group on the left includes all newly visible service sites (recently seen), the second group includes the recent best service sites (recent best) and the third group includes the recent worst-service sites. Each service site

mentioned in figure (8) provides an assessment of the performance of the commercial site used and the services provided by the service sites according to SSL laboratories reports. The tables (1), (6) and (9) are divided by the best, recent and worst service site groups mentioned in the previous format.

Table 1 Evaluating the recent best service web sites according to SSL laboratory report

Name of service	Certificate	Protocol support	Key exchange	Cipher strength	Grade
muthai.in.th	100	93	90	90	A+
saltyvagrant.com	100	93	90	90	A+
daniel-winter.de	100	93	90	90	A
cajasycajeros.telmex.com	100	93	90	90	A-
resultatslaboratoires.aphp.fr	100	97	90	90	B

The service site receives an A+ rating (A+ grade), which is the highest performance rating if the site provides services in the following ratios (100% certificate strength, 93% support protocol, 90% key switch, 90% encryption strength) as described in figure (9).

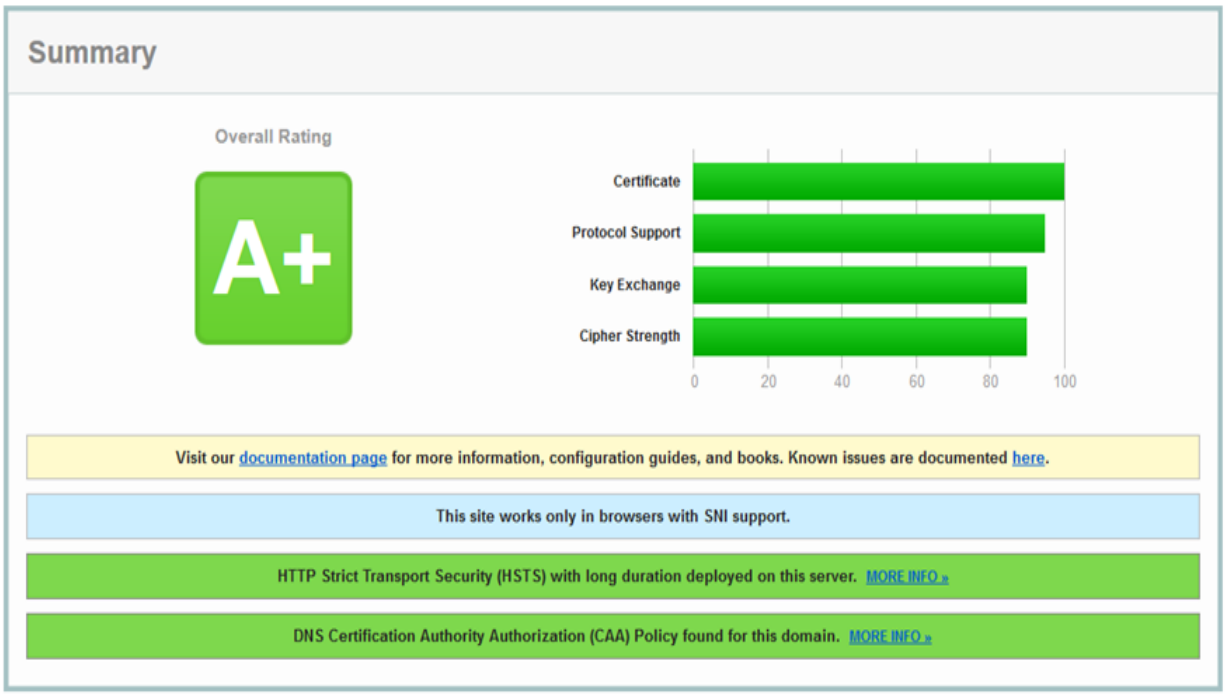

Figure 9 It illustrates the ratios of services according to A+ rating

The A+ rating characteristics are based on the ratios of services provided by the site as well as the evaluation of each service according to the quality and strength of the mechanism used in the service, for the site with the A+ rating, its characteristics are summarized in table (2).

Table 2 The service and its properties for rating A+

Services	Properties
Certificate	RSA 4096 bits (SHA256 with RSA)
Key	RSA 4096 bits
Signature algorithm	SHA256 with RSA
Issuer	Let's Encrypt Authority "http://cert.int-x3.letsencrypt.org/"
Protocols	Handshake, TLS 1.2, TLS 1.1, TLS 1.0
Cipher suites	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Handshake simulation	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 on Firefox

The information provided by table (2) indicates that the certificate is encrypted using RSA method per 4096 bits with the digital signature, and the code key also uses RSA per 4096 bits, The digital signature algorithm also uses SHA256 with RSA, and the source of the digital certificate is the authority (Let's Encrypt Authority X3) and the authority's website "http://cert.int-x3.letsencrypt.org/", while the used protocols are Handshake TLS 1.2, TLS 1.1,TLS 1.0. Here, it should be noted that the protocol in green color (**TLS 1.2)** is one of the most recent versions and is very convenient with the service site in question, for the encryption methods with the protocols that are used is TLS_ECDHE_RSA with AES_256_GCM_SHA384 which is very appropriate. It is worth noting that ECDHE is the acronym (Elliptic Curve Diffie-Hellman Exchange) is the basis for the traditional SSL security web link protocol and is supported by all modern browsers [7]. The site's handshaked with Firefox (which is the browser used in this work) and is also conducted through one of the encryption methods and protocols mentioned like TLS_ECDHE_RSA with AES_128_GCM _ SH A256. If the rating is A, it gets a high performance, if the site offers services in the following ratios (100% certificate strength, 93% support protocol, 90% key switch, encryption strength of 90%) As shown in the figure (10).

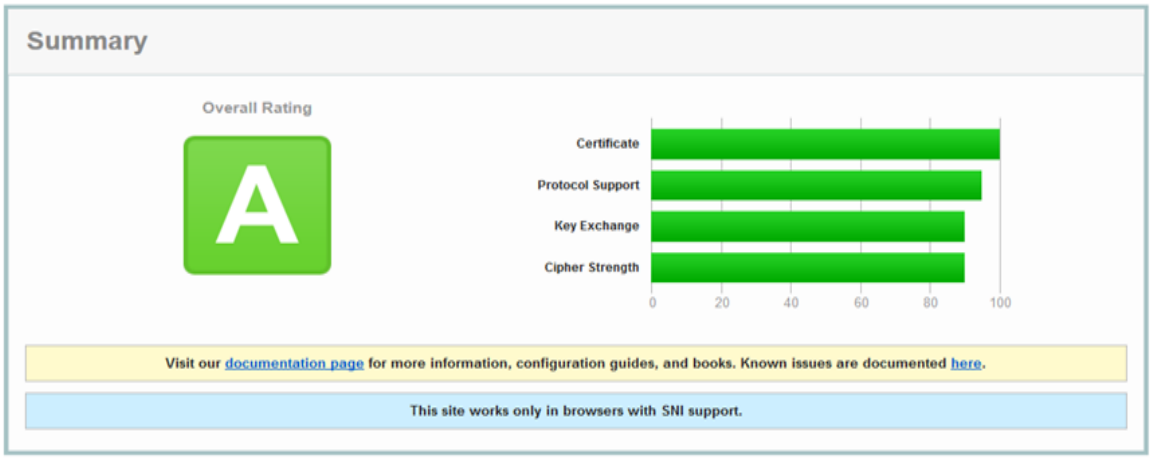

Figure 10 It illustrates the ratios of services according to A rating

A's rating characteristics are based on the ratios of the service that is provided by the site also the evaluating of each service according to the quality and strength of the mechanism used in the service. We should note that the service sites here only work on browsers that support SNI (is a short for Server Name Indication, which means the name signal of the server and it manages several SSL certificates on the same IP address) [8]. The site with a grade A (rating A) has been summarized in table (3).

Table 3 The service and its properties for rating A

Services	Properties
Certificate	RSA 4096 bits (SHA256 with RSA)
Key	RSA 4096 bits
Signature algorithm	SHA256 with RSA
Issuer	Let's Encrypt Authority "http://cert.int-x3.letsencrypt.org/"
Protocols	Handshake, TLS 1.2, TLS 1.1, TLS 1.0
Cipher suites	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Handshake simulation	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 on Firefox

By noticing table (3) shown above, we see that the certificate is encrypted using RSA method with 2048 bits with the digital signature method, the key also uses RSA with 2048 bits, the digital signature algorithm uses the method SHA256 with RSA, the source of the authority certificate (which is Let's Encrypt Authority X3) and the location of the authority:
"http://cert.int-x3.letsencrypt.org/"

The protocols used are Handshake TLS 1.2, TLS 1.1, TLS 1.0. It is noted that the protocol TLS 1.2 is one of the latest versions and is very convenient with the service site in question, for encryption methods with protocols used by the site which is TLS_ ECDHE_ RSA associated with AES_256_GCM_SHA384 is also very appropriate. The site is handshaked with the browser Firefox (which is the browser used in this research) using one of the encryption methods and protocols mentioned in the service with TLS_ECDHE_RSAAES_256_CBC_SHA. The service site receives an A rating, which is a performance rating if the site provides services at the following percentages (100% certificate strength, 93% support protocol, 90% key switch, 90% encryption strength) as described in figure (11).

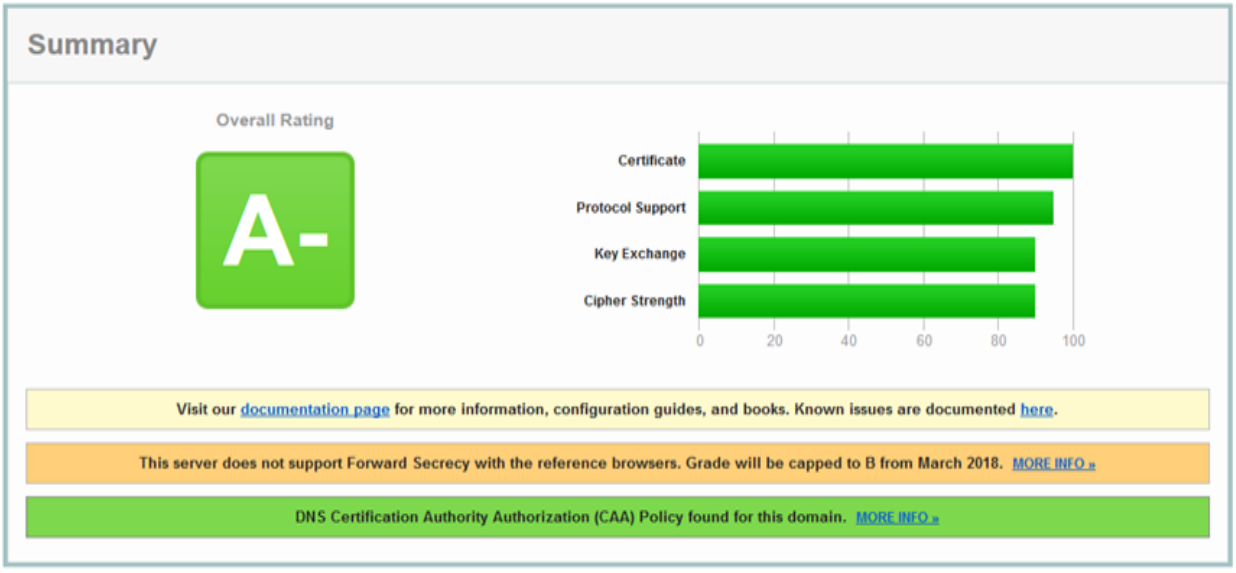

Figure 11 It illustrates the ratios of services according to A- rating

The characteristics of the A- grade are according to the ratios of services from the site also the evaluation of each service according to the quality and strength of the mechanism used in the service, we note here that the server in those sites does not support confidentiality for the source of browsers, that the site rated A- has its characteristics summarized in table (4).

Table 4 The service and its properties for rating A-

Services	Properties
Certificate	RSA 2048 bits (SHA256 with RSA)
Key	RSA 2048
Signature algorithm	SHA256 with RSA
Issuer	DigiCert SHA2 Secure Server CA “http://cacerts.digicert.com/DigiCert SHA2SecureServerCA.crt”
Protocols	Handshake, TLS 1.2
Cipher suites	TLS_RSA_WITH_AES_256_GCM_SHA384 WEAK
Handshake simulation	TLS_RSA_WITH_AES_128_CBC_SHA on Firefox

By noting table (4) above, we notice that the certificate is encrypted using RSA method with 2048 bits and the digital signature method, the key also uses RSA with 2048 bits, the digital signature algorithm uses SHA256 with RSA, source of body certification (DigiCert SHA Secure Server CA) with the CA website (http://cacerts.digicert.com/DigiCert Sha2SecureServerCA.crt). It can be noted that the protocol TLS 1.2 is one of the latest versions and is very convenient with the service site in question, for the encryption methods and protocols used by the site which is TLS_RSA with

AES_256_GCM_SHA384, they were weak and inappropriate. The handshake of the site with the browser Firefox (which is the browser used by the work) is conducted by one of the encryption methods and protocols mentioned in the service, which are TLS_RSA with AES_128_CBC_SHA. The service site receives a B rating, which is a performance rating if the site provides services at the following percentages (100% certificate strength, 97% support protocol, 90% key switch, 90% encryption strength) as described in the figure (12).

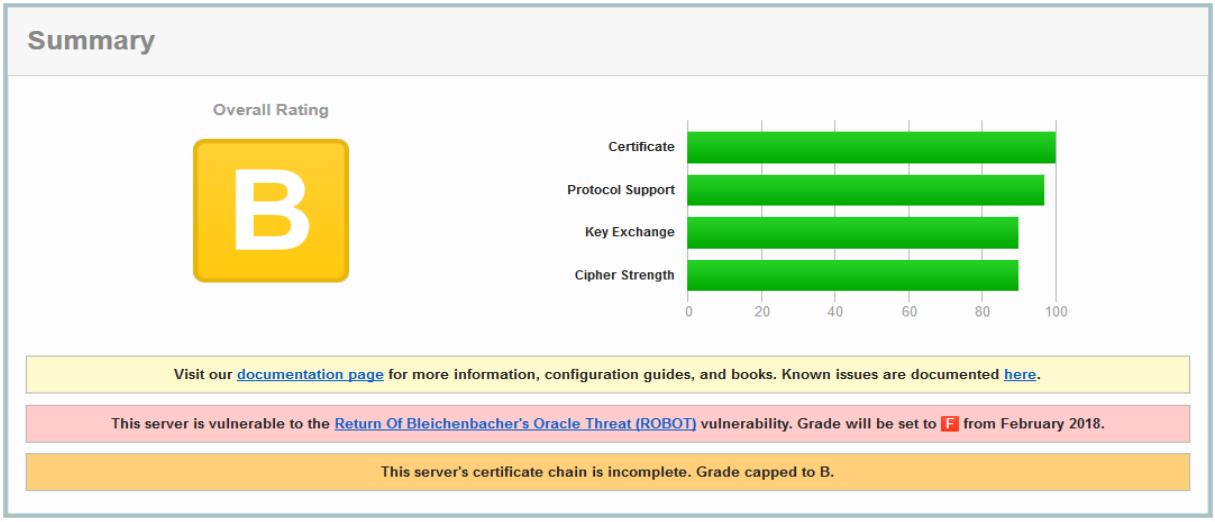

Figure 12 It illustrates the ratios of services according to B rating

The characteristics of the Grade B (B rating) are according to the ratios of services from the site also the evaluation of each service according to the quality and strength of the mechanism used in the service. We note here that the series of digital certificates of the servers is incomplete, that the site with the grade B and its characteristics have been summarized in table (5).

Table 5 The service and its properties for rating B

Services	Properties
Certificate	RSA 2048 bits (SHA256 with RSA)
Key	RSA 2048 bits
Signature algorithm	SHA256 with RSA
Issuer	GlobalSign Domain Validation CA-SHA256-G2 “http:/secure.globalsign.com/cacert/gsdomainvalsha2g2r1.crt”
Protocols	Handshake, TLS 1.2, TLS 1.1
Cipher suites	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
Handshake simulation	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256_ECDH on Firefox

We note in table (5) above, that the certificate is encrypted using RSA method with 2048 bits and the digital signature method, the key uses RSA with 2048 bits, the digital signature algorithm uses the SHA256 method with RSA, the source of the Body Certification (GlobalSign Validation Domain CA256-G2) with the authority's website: "http:/secure.globalsign.com/cacert/gsdomainvalsha2g2r1.crt"

The Used Protocols are the Handshake TLS 1.2 and TLS 1.1. We note that the protocol TLS 1.2 is one of the latest versions and is very convenient with the service site in question. The encryption methods and protocols used by the site which are TLS_ECDHE_RSA with AES_128_ GCM_SHA256 are appropriate in this case. The site is handshaked with the browser Firefox (which is the browser used by this research) is conducted by the encryption methods and protocols mentioned in the service (TLS_ECDHE_RSA with AES_ 128 _GCM _SHA256 _ ECDH). ECDH is an acronym for Elliptic Curve Diffie-Hellman which is an anonymous key agreement protocol which allows the parties to have two keys, public and private to establish joint security on the unsafe channel, this common security can be used as keys or used in deriving different key used to encrypt subsequent connections by using identical key encryption, which is different from Diffie-Hellman's protocol that uses elliptic curve encryption [9].

Table 6 Web sites of recent reachable services according to SSL report

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

Table (6) clarifies the recent service sites and it shows that most of the service estimate are A (rating A) and there are sites that are not able to connect to the server at the moment as they give false ratings. The service site receives an F rating, which is a performance rating if the site provides services at the following percentages (100% certificate strength, 50% support protocol, 90% key switch, encryption strength of 0%). Figure (13) clearly shows this.

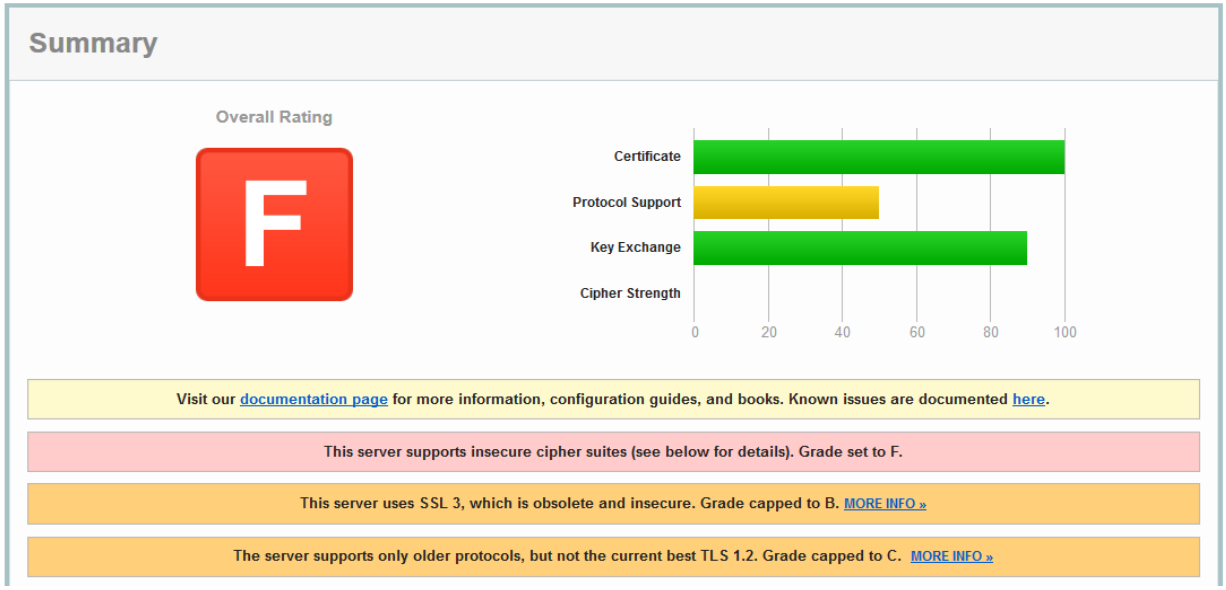

Figure 13 It illustrates the ratios of services according to F rating

The F rating characteristics are based on the ratios of services from the site also to the evaluating of each service according to the quality and strength of the mechanism used in the service. Here, we note that the servers support unsafe encryption methods and use old protocols. For the site with the Grade F, its properties are summarized in table (7).

Table 7 The service and its properties for rating F

Services	Properties
Certificate	RSA 2048 bits (SHA256 with RSA)
Key	RSA 2048 bits
Signature algorithm	SHA256 with RSA
Issuer	COMODO RSA Organization Validation Secure Server CA "http://crt.comodoca.com/COMODORSAOrganizationValidationSecureServer CA.crt"
Protocols	Handshake, TLS 1.1, SSL3 INSECURE
Cipher suites	TLS_RSA_WITH_RC4_128_MD5 INSECURE
Handshake simulation	TLS_RSA_ WITH_3DES_EDE_CBC_SHA on Firefox

From table (7) shown above, we note that the certificate is encrypted using RSA method with 2048 bits length and the digital signature method, the key uses RSA, also with 2048 bits length, the digital signature algorithm uses the method SHA256 with RSA, the source of the authority certification (COMODO RSA Organization Secure Server CA) with the location:
"http://crt.comodoca.com/COMODORSAOrganizationValidationSecureServerCA.crt"
The used protocols are handshake, TLS 1.2 and SSL 3. We note that the protocol TLS 1.2 is one of the latest versions and is very convenient with the service site in question while SSL 3 that is used here is unsafe. The encryption methods and protocols used by the site which are TLS_RSA with RC4_128_MD5 are unsafe, and the site is handshaked with the

browser Firefox (which is the browser used in this work) by the encryption methods and protocols mentioned in the service TLS_RSA3DES_EDE_CBC_SHA. The service site receives a T rating, which is the highest performance rating if the site provides services at the following percentages (certificate strength 0%, 93% support protocol, 90% key switch, encryption strength of 90%) as is shown in figure (14).

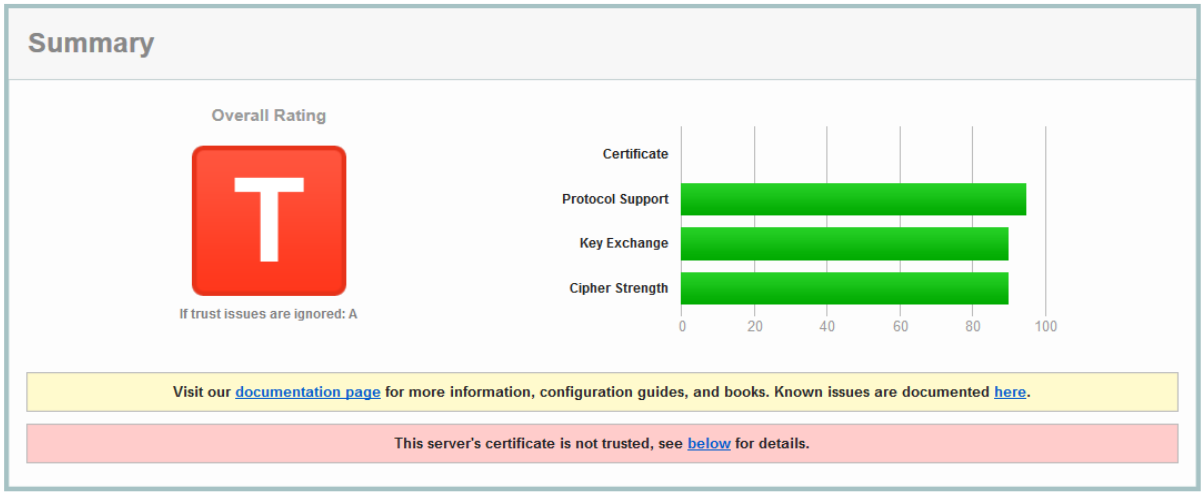

Figure 14 It illustrates the ratios of services according to T rating

The characteristics of the T rating are according to the ratios of services from the site also the evaluation of each service according to the quality and strength of the mechanism used in the service, we note here that the digital certificates of the servers are not reliable. The site with the grade T with its characteristics is shown in table (8).

Table 8 The service and its properties for rating T

Services	Properties
Certificate	RSA 2048 bits (SHA256 with RSA), NOT TRUSTED
Key	RSA 2048 bits
Signature algorithm	SHA256 with RSA
Issuer	COMODO RSA Organization Validation Secure Server CA “http://crt.comodoca.com/COMODORSAOrganizationValidationSecureServer CA.crt”
Protocols	Handshake, TLS 1.2, TLS 1.1, TLS 1.0
Cipher suites	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
Handshake simulation	_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH on Firefox

From table (8) shown above, we note that the certificate is encrypted using the RSA method with 2048 bits length and the digital signature, but it is unreliable. The key uses RSA with 2048 bits length, and that the digital signature algorithm uses the method SHA256 with RSA, as well as the source of the certificate COMODO RSA Domain Validation Secure Server CA with the location of the authority:

"http://crt.comodoca.com/COMODORSADomainValidationSecureServerCA.crt"

The used protocols are the Handshake TLS 1.2, TLS 1.1 and TLS 1.0. It can be noted that the protocol TLS 1.2 is again one of the latest versions and is very convenient with the service site in question. The encryption methods with protocols used by TLS_ECDHE_RSA_ with AES_256_CBC_ SHA384 are being appropriate. The site is handshaked with the browser Firefox (which is the browser used to work) by encryption methods and protocols ECDHE_RSA_ with AES_256_CBC_SHA_ECDH.

There are several reasons for the digital certificate to be unreliable and the problem has been mentioned in the report in red, and it is caused by one of the following points:

1. Unverified digital certificate
2. Server configuration has not been validated
3- The digital certificate donor is anonymous

Therefore, the protocols and encryption methods must be developed in order to address the causes in points 1 and 2, and the third point must be confirmed by the certification authority for digital certificates before submitting the request from the owner of the commercial website to obtain the certificate.

Table 9 The worst recent service web sites according to SSL report.

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

From table (9) which shows the recent worst service locations, we note that most of the service ratings are F and T, i.e. the service sites are not reliable and unsafe.

Conclusion

One of the most important problems facing e-commerce is the challenges related to security, privacy and information protection.
Through this research, the following have been concluded:

- The possibility of securing the commercial site and gaining the trust of customers and the customer by adding SSL technology and his certificate from a certified body on the web server to serve http content securely, and to ensure its work by following the field of the server in the site of the documentation authority.
- Working on Linux gives insurance and higher possibility compared to Windows, as companies that issue digital certificates give the server additional features that can be programmed on Linux because it is open source and cannot be added if using Windows.
- Through the grades found on the service sites that determine the performance evaluation, the owner of the site can know the degree of safety for her/his commercial site.
- Through the server domain in the documentation authority site it is possible to know if the service sites are in a state of maintenance, and thus the commercial transaction must be stopped for a period to avoid penetration or the possibility of transferring the commercial site to another service site

Future Work

Adding Secure Electronic Transactions (SET), which is a technology that secures transactions between companies made via VISA CARD across the Internet. This requires another party to work, the bank, as the search contains only one party, which is the commercial site. SET technology is added to the servers of both parties and secures a digital binary signature for the merchant server and the bank server.

References

Zaid, A., & Thanaa, D. (2017). The Reality of E-Commerce and the Challenges Facing it Arably and Globally. *Tishreen University Journal for Studies and Scientific Research, Economic and Legal Sciences Series*, *27*(4).

Al-Janabi, N.M., Al-Zaidi, M., & Nima, M. *Economic Intelligence is the only entry point to Knowledge Intelligence.* Al-Qadisiyah University, 2018.

Al-Dawi, I.A.A. (2016). *E-Commerce an Applied Study on Libraries*. King Fahd National Library for Printing and Publishing.

Boss, W.R. (2007). *E-Commerce for Libraries*. McGraw Hill.

Th. Kazem, A., & Kazem, F.A. (2014). The Role of E-Commerce in Economic Development and District Management in Iraq. *Al-Qadisiyah Journal of Administrative and Economic Sciences*, *16*(1).

El-Sayed, K.A. (2017). *Arab E-Commerce Prospects and Challenges*. Encyclopedia of Islam and Development.

Syed Jawad Al-Nasser, H. (2017). *The Impact of E-Commerce on Competition in Arab Local Markets*. Research Study: Arab Democratic Center.

Al-Hassan, H. (2014). Authenticating the Electronic Signature for Electronic Documentation. *Damascus University Journal for Economic and Legal Sciences*, *30*(1).

Stallings, W. (2005). *Principles and Practices of Cryptography and Network Security*. Fourth Edition, Prentice-Hall.

Al-Banat, M. (2015). Electronic Contracts. *Symposium on Electronic Commerce Contracts and their Areas. Cairo, Arab Administrative Development Organization*.

Hussein, F.S. (2015). *Electronic Commerce and Insurance.* Arab Printing House and Hala Publishing and Distribution.

Sarkar, P.G., & Fitzgerald, S. (2016). *Attack on SSL: A Comprehensive study of beast, crime, time, breach, lucky 13 and RC4 biases, San Francisco, CA, isec Partners.*

Stalling, W. (2011). Transport-Level Security. *In Cryptography and Network Security*. *5th ed. Upper Saddle River, NJ: Pearson*, 485-520.