Security, Privacy, Accessibility and Availability issues not a priority when developing web sites in the GCC

XANTHIDIS DIMITRIOS
Information Management
IMSIU University
Riyadh, SAUDI ARABIA

VIOLETTAS GEORGE1
ICT Department
Technical Trainers College (TTC)
Riyadh, SAUDI ARABIA

Abstract: - This is the 2nd part of a study on the evaluation of the Web sites of companies in the GCC (Gulf Council Countries) and attempts to answer the question of whether security and privacy but, also, accessibility and availability issues are addressed by the developers locally. A total number of 129 web sites from companies in Bahrain, Kuwait, Saudi Arabia, Qatar and United Arab Emirates were evaluated. The tables 3 and 4 (appendix), i.e. on accessibility/availability and security/privacy, from the WSEI (Web Site Evaluation Index) were applied during the evaluation. The results of the evaluation are not encouraging at all showing that security and privacy issues are not a priority when developing the web sites and accessibility and availability are not among their serious concern either.

Key-Words: Web sites, evaluation, security and privacy, accessibility and availability, GCC

1 Introduction

The modern business world is operating, currently and in the future, in a digital environment and mainly online regardless of the particularities of each different economic sector each business entity belongs to. This brings many opportunities for the market players to approach and attract potential clients and meet with their need online but, also, demands careful and thorough strategic planning of how certain challenges are to be addressed.

During the past decade, or so, the company executives in the Gulf Council Countries (GCC) have been active in responding to the growing number of people using the Internet everyday for a variety of purposes and currently about 15% of the businesses in the Middle East have an online presence with the GCC companies in the lead [1]. Especially the younger individuals aging below 40 years old and being very active in the social networks [2] are being targeted by the marketing officials of these GCC companies. Furthermore, the higher education institutions put increase interest in training local individuals in the new web technologies in an effort to prepare the manpower of the next decades that will address the growing needs for web designers and developers in the region.

There are a number of issues to be considered when designing a web solution and the whole task becomes increasingly critical in importance and large in size for the companies when they want to not just have an online presence but also deploy additional parts of their everyday operations on the Web as the Web Site Evaluation Index (WSEI) suggests [3].

Arguably four of the most important issues to be considered are those related with the security of the web sites and the privacy of the online clients in addition to ensuring 24/7 availability of their online presence and full compatibility with different electronic devices and operating system platforms. The question this paper is attempting to answer is to what extend these regional companies with online presence are successful in deploying web solutions that address these four issues.

2 Aims and Objectives

The aim of this 2nd part of the study is the evaluation of the web sites of 129 companies of the GCC, like in the 1st and the 3rd parts. More specifically its objectives are to:

- Examine whether necessary development strategy are followed to ensure security and privacy issues are addressed,
- Verify, if possible, the availability and accessibility of the web sites under different operating platform and on a variety of current electronic devices,
- Record possible useful clues and suggestions for the current update of the Web Site Evaluation Index (WSEI) (4th and final part of the study) which was used as the basis for the evaluation.

3 Literature review

Even though it is already 7 years old and needs to be updated with the current developments and

---

1 George Violettas wishes to thank TTC for financially and morally supporting this work
guidelines for designing web solution the WSEI provides a good number of suggestion of what are the functional and non-functional requirements a Web site of any online company in any region of the globe should address [3]. It is divided into 4 distinct categories i.e. HCI related issues called “stickiness”, guidelines associated with customization and/or globalization needs, the accessibility and availability requirements and, finally, checkpoints ensuring proper security and privacy measures implemented for the web solutions. The last one addresses a limited number of questions related to possible vulnerabilities of web sites.

The security list provided by OWASP [4], however, is considered today the most respected security guide in the wild and covers the list included in the old WSEI. (For more details on OWASP security list look at works [5], [6]). From this OWASP top-10 list not all thread categories can be tested in a black-box test like the evaluation at hand. The following is a brief of those threads that can be tested:

- **A2 - Broken Authentication and Session management**: the main 2 vulnerabilities in this category that could be tested are “session IDs are exposed in the URL,” and “passwords … and other credentials are sent over unencrypted connections” [7], [8],
- **A3 – Cross-Site Scripting (XSS)**: only a few standard tests can be conducted in the search & username input fields of the web sites in a black-box testing process,
- **A6 – Sensitive Data Exposure** [9]: the questions No 2, 3, 4 and 5, i.e. “is any data transmitted in clear text?”,” are any old weak cryptographic algorithms used?”,” are weak keys generated?” and “are any browser security directives or headers missing when sensitive data is sent to the browsers?” respectively can be answered in the context of a black-box testing.

On the contrary the following threads must be omitted from such an evaluation as either they do not provide complete and safe results but only in the negative cases or they are very much detailed and time-consuming or they can only be completed in the context of white-box testing which cannot be the case of such an evaluation:

- **A1: Injection,**
- **A4: Insecure Direct Object References,**
- **A5: Security Misconfiguration,**
- **A7: Missing Function Level Access Control,**
- **A8: Cross-Site Request Forgery (CSRF),**
- **A9: Using Component with Known Vulnerabilities,**
- **A10: Unvalidated Redirects and Forwards.**

The above two lists do not include the case of Denial of Service (DoS) as this is a possible attack thread and not a vulnerability [11], [12]. The main idea behind DoS is to attempt to make a computer resource unavailable to its intended users usually by overloading the resource. One major flavor of this attack can be examined in a black box testing if a SQL query is sent to the server of the resource using large strings as an input to search fields, e.g. %[^!_%/%}%{()}{{%])({()£$&N% _$£(5*$R"_][%]%[x]%a][$"£$-%-9]%$. DoS is checked obviously as a particular website vulnerability and not as a hosting server flaw or weakness.

The WSEI [4] together with the aforementioned tests provides a clear list of security and privacy issues that should be addressed by the web solution developers although more could be, also, included in it:

- Secure channel to login,
- Secure channel for electronic transactions,
- Use of TLS instead of the old SSL or no secure channel,
- Security certificate authentication is provided,
- Security key 256 (or 512) instead of 128 or even no key,
- Online anti-virus scanner protection,
- Control of a web site’s time out,
- Provision against XSS vulnerability,
- Protection against DoS attacks,
- Use of tracking mechanism with the user’s consent,
- Clear privacy statement,
- Masked email addresses.

As to the examination of the accessibility and/or availability the WSEI suggested the developers should address the following issues:

- Ensure platform compatibility especially with current electronic devices, e.g. tablets, smartphones,
- Optimization for the handicapped or the people with special needs,
- Appropriate loading time,
- Optimization for displaying properly in different resolutions,
- Support for “third party” components.

Keeping the above points in mind, and possibly others not included in these lists, when forming a web solution design strategy largely ensures that the most critical concerns associated with any type of online presence of a company are properly addressed and the deployment of such a solution is
for the benefit of the visitors but also of the companies.

4 Methodology

This is the 2nd part of the evaluation of the web sites of the companies of the GCC countries, namely Bahrain, Kuwait, Saudi Arabia, Qatar and United Arab Emirates. Like in the 1st and 3rd parts it examines the level of quality of the web sites of 129 companies randomly selected from each country and in particular 7 from Bahrain, 12 from Kuwait, 78 from Saudi Arabia, 4 from Qatar and 28 from United Arab Emirates. These countries from the GCC were selected as been more technologically and financially advanced with high Internet penetration and an increased level of computer and Internet literacy as opposed to others in the region under study. The difference in this part lies within the context of the questions answered which now address security and privacy issues but also with the provisions of the web developers associated with the accessibility and availability of the web sites under different platforms and on a variety of electronic devices.

In the case of the “accessibility and availability” issues the following points were addressed concerning each of the web sites:
1. Is it compatible across different platforms?
2. Is it optimized for the handicapped or people with disabilities?
3. Is it loading fast or slow?
4. Is it displayed properly in different resolutions?
5. Does it support “third party” components, i.e. offers downloadable components from other companies?

In the case of “security and privacy” provisions the following important issues were addressed in each of the web sites:
1. Does it provide secure login and/or transactions through secure channels? If so, does it use SSL or TLS?
2. If secure channel is provided is there a certificate verifying the channel and what is the key size?
3. Is there an anti-virus scanner provided?
4. Does it time-out?
5. Is it vulnerable mainly to cross-site scripting and/or DoS attacks?
6. If it uses tracking mechanisms does it ask for user’s consent?
7. Does it include a privacy statement?
8. Are the email addresses masked?

In all the above questions/issues a negative answer would result in a 0 whereas a positive one would be valued with 1. All these data once recorded were processed through SPSS 20 for cross-tabulation and ANOVA statistical analysis and the results were transferred to MS Excel 2011 (for Mac in both cases) for the production of high quality graphs.

5 Findings

In general, it could be said that the general findings are not satisfactory. A lot of the web sites analyzed look old and “abandoned”. They look as if someone decided to create a website once, put it on the wild and forgot about it since. The next 3 sections provide a more detailed analysis of the findings based on the data gathered through the evaluation of the web sites but more data is available upon request.

5.1 No interest in addressing security and privacy issues

Figure 1 above illustrates the results of the evaluation of the 129 web sites of the randomly selected companies from the GCC countries of Bahrain, Kuwait, Saudi Arabia, Qatar and United Arab Emirates from a security and privacy angle. The evaluation of the web sites unearthed a lot of problems concerning their secure connection (https) but also some others when addressing, or rather not, privacy and related issues.

In the case of secure channels used by the web sites the evaluation shows that such connections are not very much used and when they are the SSL protocol version 1.5 is used, which has some security issues, and not the latest TLS. To make things worse even the key used is only 128 bit (13%) although the trend in the developed countries is to easily have 256 or 512 bit encryption without a significant compromise of the communication speed. Add to the above that there are web sites with expired SSL certificates or certificates not issued by a trusted certificate agency (CA) (28%). Even if this for some people is not considered severe, it is a very bad sign for the reputation of the company represented by the website.

Most of those websites using SSL for the final transaction (76.7%) are not utilizing it for the user login page! This is a major security breach because someone can easily intercept the user credentials having access to the user account. On those websites where ALL information exchange pages are encrypted the answer to the question if secure channel (TLS or else) was used for economic
The number of web sites with obvious signs of cross-site scripting (XSS) flaws is rather high (7%). This is one of the easiest to deploy attacks. Also some websites show profound signs of vulnerability against SQL injection(s). For the economy of time and to avoid legal complications of the task, the vulnerabilities were not explored any further. It has to be stated here that many websites are obviously made with Joomla. This gives them some basic security features such as (at least basic) protection against XSS and DoS (Denial of Service attacks). On the other hand, because https is not enabled by default in Joomla in username & password exchange, almost all of those websites lack this feature, making them completely vulnerable to leak of personal information. This simply means that the website developer just used something out of the box, put the site on the wild and just forgot about it. Nowadays, however, maintaining strong security requires constant monitoring, continuous updates, personal effort and above all total awareness.

Concerning DoS, 20% of the websites show some signs of vulnerability. Although it was stated earlier that those vulnerabilities are very difficult to verify through such an examination as this evaluation was, however, this percentage implies the very low quality of some websites and the
indifferent attitude of the webmasters. A DoS attack can bring a website completely offline sometimes for days or weeks, eliminating the credibility of the particular product or company behind it.

Fig. 2 Reasons for hesitating to reveal the true identity online

Only 1.6% of the web sites have a default time out mechanism. This is not a mainly security issue but it is one of those characteristics that distinguish a well maintained web site from the others. A time-out mechanism serves a dual purpose. It will ensure that critical web pages containing sensitive data will not stay on the screen of the computer even if the user left the web page on and the computer unattended. If the intruder tries to do something on this particular webpage, s/he will see that the webpage is no longer available and the user has to logon again. The other purpose is to ensure that the data provided, at the moment, are up to date and accurate which is likely not to be the case after a certain period of time causing, thus, the page to be not valid any more and requiring the user to resend the original request.

Half of the websites are using tracking mechanisms without the consent of the user. This means that the websites are utilizing the user’s data (private or not) such as IP address, most likely by storing a cookie into the user’s computer for reference and personalizing their usage, without the user being aware of this. In many countries of the world today this could be even illegal.

In 40% there is no privacy statement, which is also a very serious matter. This leaves a lot of room
for suspicions that the company behind the website might use the data collected from the user (personal or not) for purposes the user is not informed of. This data could be sold or given to third parties for further processing, for advertising purposes, for statistical reasons or even direct market targeting and other activities. In any of the above circumstances, the user should be absolutely aware of how and where her data will be used. Once again it should be noted and cannot be stressed enough that this is a legal obligation in a lot of countries, especially developed ones, of the world today.

5.2 Limited concerns about threads

Figure 2 is indeed one picture worth a thousand words. Apparently the designers and/or developers of the web sites evaluated are not seriously interested in addressing any issues related to accessibility and/or availability.

The majority of the websites are not loading fast enough, especially on tablets/smartphones, as it takes in several cases even more than 20”” to load which is, of course, absolutely unacceptable given the modern technologies. This is mainly because of the non-optimized size of graphics and the lack of modern web design (dynamic web pages etc.). It looks that the designers are focusing more in developing “any” web site even barily functional than in producing an effective online solution. Furthermore, but not surprisingly given the low level of overall quality of the products, almost none of them is optimized for handicapped people.

In 44% of those websites there are unmasked e-mail addresses. Nowadays, all e-mail addresses should be protected by scripts or being depicted in a graphic element and not as text. Those unmasked addresses can be easily collected by crawlers to be used either for spam e-mail or even for phishing attacks.

Finally, 6% of the web sites have issues when comes to different platform compatibility, i.e. different browser and/or OS or device. This suggests those websites are not accessible from all the potential users.

6 Discussion-Conclusions

The results of the evaluation of the 129 randomly selected GCC companies’ web sites are not are not very encouraging, to say the least, as seen in the previous findings section. The matter of security does not look to be a very hot topic in the region. A lot of sites lack basic security attributes leaving security holes wide open and, quite likely, rapidly and dramatically reducing, or even eliminating, the level of trust of their web users.

There are a lot of websites that look “orphan” or “abandoned”, i.e. it is obvious that they are left over without any maintenance resulting in security flaws, misplaced or displaced graphics and text, errors in presenting the data etc. Those web sites are destructive rather than beneficial for the companies they represent.

In general, based on the quality of the web sites one can come up with the, rather safe, conclusion that the maturity and effectiveness of the web design strategies of their respected company executives is highly questionable. Companies and any business, government or other entities in general should better realize soon that a website is not a luxury nor something that once created there is no need to be dealt with again. It needs constant care, continuous update with new and fresh material, change of topics an themes reflecting the current trends and, most important, keep it up to date in addressing new security threads. Update all software involved to the latest version, install all updates and patches and use mechanisms of continuous monitoring it.

Additionally, the web site developers and admins should realize that the user’s rights and privacy have to be protected and safeguarded since trust is something easily lost but very difficulty to gain back again.

References:


Appendix:

Table 3: Evaluation template - Dimension III: Accessibility, Availability, Hardware/Software requirements

| 1. | Is the Web site accessible (Platform Compatibility) |
| 2. | Is the Web site optimized for users with a mental or physical handicap? |
| 3. | Hardware/Software/Network requirements |
| i. | Time required loading the Web site’s home page? |
| ii. | Web site displayed properly, i.e. no horizontal scrolling mechanisms, no twisting of objects, etc., in different display resolutions? |
| iii. | Option to download and install “third party” components required to view the Web site, e.g. activeX, flash players, different fonts, etc. |

Table 4: Evaluation template - Dimension IV: Security, Privacy

| 1. | Security |
| i. | Authentication required to login into possible intranet part of the site? |
| ii. | If transactional or interactive what protocol are they using (None, SSL, SET, Other)? |
| iii. | What is the cipher strength? |
| iv. | On-line anti-virus scanner available? |
| v. | Web site expires after a pre-defined amount of idle time? |

| 2. | Privacy |
| i. | Avoid the use of tracking/identifying mechanisms i.e. cookies, spyware, etc, without the consent of the user? |
| ii. | Privacy statement? |
| iii. | Masked e-mail addresses through scripts, forms, buttons, etc? |