The impact of information security data breach in Community College of Qatar and its countermeasures

Gowher Mushtaq[1], Abdullah Al-Siddiqi[2]

1. ABSTRACT

As the number of attacks from hackers is increasing every day, by finding out the data breaches and targeting on the network. The attacks on networks are very dangerous as they can be a very big loss to the companies, Colleges, Schools, Universities. In educational institutions, we used to store the information of our students on the web servers their Grades, Name, Passport details. According to a survey based on survey monkey, more than 80% of CCQ feel that their confidential information is not safe on the web server of CCQ. The purpose of this research is to provide the fully secured network system by finding the critical issues in the web server of Community College Qatar (CCQ). The practical background of this research was drawn using the tool OWASP-ZAP. The tool was helpful to find out the data breaches in the server of CCQ. The terminology has been given to secure the web server by taking the necessary steps to fix the critical issues in the server. This research provides a list of recommendations based on the output of data breaches found on the server, to safeguard the server and its storage.

KEYWORDS

Cybersecurity, data breaches, CCQ, OWASP, Survey Monkey, GCC

2. INTRODUCTION

This work provides an important opportunity to advance the understanding of data breaches and resulting in customer security threats, such as Name, Credit Card details, QID, Passport details, etc. Data breaches happen when a valued client or

student data is stolen or lost by hackers and can result in the loss of millions of confidential records (e.g., local schools, Colleges, Universities, Agencies). According to U. S. Marketers, for the profit-making survey of the market price, research elected 120 openly transposed firms that experienced a data breach involving the loss of client and personal information. This research chased the ratio value for 30 days preceding to the publication of the information breach and 90 days ensuing the data breach [1]. In this major work, the details of CCQ will be covered and the data breaches and use the necessary measures to counter those breaches, which will help us to make our servers are more secure and safe from attacks will be revealed. Recent pieces of evidence suggest that data breaches are the main factors of security to be targeted so research needs to take the necessary steps to secure systems. As noted by Ping Wang, a cybersecurity proceeding is defined as an incident that literally or potentially results in conflicting outcomes to (adverse effects on) (potential threat to) an information system, or the information that the system stores, operates and transmits and that may need a counteraction to reduce the threats [2]. In early 2015, Fraudsters were seen utilizing credit card information stolen from Domestic Warehouse and Target to make Apple Pay accounts and after that utilizing false accounts to buy and offer expansive - ticket things at higher costs. Commenting on this, Malhotra states that target has been beneath attack by programmers of current era after the final major information breach, the risk on deals was exceptionally expansive and long-lasting. It seemed too soon to be compromised again [3]. Drawing on an extensive range of sources, the history of data breaches with all the latest updates with latest data breaches is identified and our work is to find out the data breaches and carry out the preventive measures. In the next part of this

project, researchers have given background information.

With each application, Site and social organizing locales inquiring us to “Allow” them the get to your phone, contacts, online clouds and more you'll think of the permitting diversion are more than what I bother to pay consideration to. It is now well established from a variety of studies, that this particular information breach was particular since it happened on the organization which was transcendently involved in maintaining, collecting, and combining personal data, albeit. The ChoicePoint occurrence was not the primary event of its kind Subsequently, the information breach uncovered numerous data records and pulled in an awesome promise of media consideration. Furthermore, broad investigate has appeared that information brokers had pulled in generally minor government administrative consideration with regard to the potential for recognizing the burglary until this occurrence. That being the case, as it were many states, most eminently California, had enactment in put ordering divulgence of such breaches. Taking after the ChoicePoint occurrence, states embraced forceful activities to seek after enactment in this range. As of May 2008, 42 states had embraced enactment with regard to protecting of client and/or worker information [4]. Equifax, one of the three biggest customer credit detailing organizations within the Joined together States, declared on September 2017 that its frameworks had been breached and the touchy individual information of 148 million Americans had found the center ground. The information that had been breached included names, domestic addresses, phone numbers, dates of birth, social security numbers, and driver’s permit numbers. The credit card numbers of around 209,000 buyers have moreover been breached. Equifax breach is unparalleled in scope and seriousness. One

longitudinal consider found that there have been bigger security breaches by other companies within the past, be that as it may, the affectability of the individual data held by Equifax and the size of the issue makes this breach unparalleled [5]. In the next phase of this project, I have provided information about our problem statement and motivation.

This project is motivated by an alarming upward trend in cybersecurity breaches in the recent past. The community college of Qatar handles sensitive student information, including their date of births, credit card information, grades, etc. the integrity of this information is vital for the institution to continue attracting more students. Nevertheless, the recent past has uncovered a drift where hackers are winning the war despite the increased security investments. In order to prevent this damage, business is investing a lot in security. However, the investments do not seem to bear any fruit. The conventional security viewpoint of some organizations is that it is important to work harder to create a robust perimeter defense. Nonetheless, this type of perimeter defense is not sufficient to safeguard cyber assets and adding partners who facilitate more efficient business processes extends the data perimeter. With these partners coming into contact with more sensitive information, it is imperative to concentrate on the risks posed by these vendors to the data environment. The costs of data breaches are significantly high and are expected to increase even further [6]. Data breach costs an average $3.86 million albeit there are some big breaches that may cost much more than this. Cybercriminals posture a major danger to corporate and individual data. Tall profile information misfortune episodes at Honda, NASDAQ, Sony, and government temporary workers, RSA Security, Lockheed Martin, as well as notices from a few national governments almost information security has started to increase

concern inside organizations. Information security is now not an extra work duty for the data innovation division, or maybe, it has developed into a critical chance administration part inside the company [6]. These studies clearly indicate that data breaches have exposed the online credentials and personal data of millions of users across the Internet. In the year 2017, several studies revealed that criminals had stolen usernames and passwords for 3 billion Yahoo users, the financial details of 143 million Americans collected by Equifax [7], and private data belonging to 57 million Uber users. Once stolen, this data becomes readily accessible via black markets and previous studies identified that over 3.3 billion credentials from breaches freely traded in the underground along with credit cards and other financial data. Exposure puts victims at further risk of account takeover, financial theft, identity theft, or worse [7].

3. Literature Review

According to Ashley A. Hall and Carol S. Wright [8] defined an information breach as ill-conceived get to touchy, secured, or secret information which comes about in compromise or potential compromise of privacy, keenness, and accessibility of the tormented data. Delicate, secured, or secret data may comprise of actually identifiable data, wellbeing information, exchange codes or mental property and budgetary information. Due to the acceleration within the sum of buyer actually identifiable data (PII) that organizations collect, there are also possibilities of increment within the dangers related with shielding the data and keeping up client security [8].

In accordance with the report [9], businesses within the Middle East endured a noteworthy downfall than other districts within the world past year owing to cyber occurrences, with 85% respondents within the region compared to a worldwide normal

of 79%. Around 18% of respondents within the locale have experienced more than 5,000 such assaults around, compared to a around the world normal of as it were 9% which places the Middle East higher than any other locale. It is obvious that information breaches within the Center East have hoisted from 16.67% to 21 in 2016 when compared to 18 in 2015 and 45.2 million information records are arranged, which was 38.5 million a year prior. As per the Gemalto's Breach Level List report, 1,792 information breaches over the globe cleared way for to nearly 1.4 billion information records conciliation amid the calendar year of 2016, a surprising increment of 86% when compared to the past year.

Concurring to tech mammoth WEBM Security, the normal add up to taken a toll of an information breach in Saudi Arabia and the UAE combined is $5.31 million, an upsurge of 7.1 percent since 2017.

After a seminal study by Bokyung Kim, the ITR characterizes an information breach as "an occurrence in which a person title in conjunction with a social security number, driver's permit number, therapeutic record or money related record (credit/debit cards included) is possibly put at chance as a result of divulgence. A wide run of businesses has confronted information breaches such as the medical/health care industry (42.5% of occurrences), commerce (33.0%), government/military (11.7%), instruction (7.3%), and banking/credit/finance. Character robbery asset center breach reports [10].

A series of research carried out by Ashish Garg, Jeffrey Curtis, and Hilary Harper revealed security companies' value in the market was positively affected by a data breach. Data breaches to a firm with higher, market-to-book ratios tend to have larger negative returns while firm size and subsidiary status also play a major role in assuaging the negative effects of a breach [11].

According to [12], Cases of cyber wars have been on the verge of an increase in Saudi Arabia and the UAE in recent years and the year 2009 marked one of the cape stones when a computer worm, Stuxnet was used to try on attacks on the Iranian nuclear facilities with the predominant goal of intending to harm Iran's enrichment program of Uranium.

OWASP is the inbuilt tool of Kali Linux, which is a very powerful tool to find out the data breaches on the basis of XSS, SQL Injection and other several options are available in it. The OWASP Zed Attack Proxy is one of the world's most prevalent free security instruments and is effectively kept up by hundreds of worldwide volunteers. It can assist you consequently discover security vulnerabilities in your Web applications whereas you're creating and testing your applications.

A research work carried out by Aishwarya Baby, in which she implemented a fluffy unique finger impression strategy that increases information security whereas data-leak discovery operations. The information proprietor preprocesses and plans fluffy fingerprints and uncovers the fingerprints to DLD supplier. The DLD supplier gages fingerprints from the organize activity and distinguishes potential spills in them. To avoid the DLD supplier from gathering correct data almost the touchy information, the collection of potential spills is composed of genuine spills and clamors. She educates all information spill alarms to the information proprietor and they post-processes the potential spills given by the DLD supplier and decides whether there's any genuine information spill or not [13].

According to the research conducted by (Li, 2017), as mentioned earlier, progressing Web innovation makes individuals much closer than ever some time recently, and hacking overseas has ended up a commonplace movement. Perhaps, The Modern York Times detailed that since 2013,

a worldwide cybercriminal bunch has stolen up to $1 billion from more than 100 keeping money and budgetary teach over 30 nations around the globe. Furthermore, these cyber-attacks maintained for two a long time without the acknowledgment of banks, controllers, or law authorization [14]. As programmers come from distinctive geological locales, the level of control over such assaults shifts appropriately and prepared with progressed innovation (e.g., IP concealing, mysterious surfing, etc.), programmers can stow away their IP addresses from discovery, which hoists the trouble of being caught by firms [14].

According to Orszag, cyber-attacks are an progressively noteworthy danger to the field of exchange and commerce, with hazard officers posting cybersecurity as their major concern and roughly 2,200 affirmed information breaches in 2017, as per the data given by a later report from Verizon [15]. The features around hacking as a rule center on potential hurt to shoppers whose information is stolen, but there hadn't been a successive examination of the impacts of cyber-attacks on a company's deals, showcase valuation and other measurements [15].

As stated by Frenkel in 2018 from San Francisco that Facebook was as of now confronting investigation over how it taken care of the private data of its clients and an assault on its computer arrange had uncovered the individual information of 50 million clients [16].

Frenkel, after his wide run of inquire about, expressed that the breach found at that point of time was the biggest within the company's 14-year history. The assailants abused a include in Facebook's code to get to user accounts in arrange to require control of them [16].

Agreeing to an arrangement of inquire about conducted by Haran, a tremendous collection of records from Qatar National Bank, headquartered in Doha was

spilled and posted online on the location Cryptome, one of the whistleblowers around the world on April 26, 2016. The spilled information of 1.4 GB in add up to clearly included inner corporate records and touchy monetary information of the bank's clients [17]. Cryptome detailed that the spill comprised 15,460 records which included points of interest of the account holders, counting passwords, PINs, and installment card information of hundreds of thousands of the bank customers' accounts. A few specialists within the field have too analyzed the information and from now on detailed that it showed up to be genuine. Be that as it may, Cryptome advertised no bits of knowledge on how the information were gotten, for occasion, on the off chance that it was through an outside hack assault, or an insider's work [17].

As stated by Magee in the year 2019 after a wide extend of inquire about, Mumsnet clients suddenly logged into the accounts of outsiders after a botched program alter that was portion of the company's move to the cloud. Within the evening of 5 February and within the morning of 7 February 2019, any clients logged into the location may have had their account information swapped with other individuals logged in. This would clear the way for them to get to the other user's mail address, account subtle elements, posting history and individual messages, but not their passwords as these are scrambled [18].

Finally, I came to know that nothing is impossible and based on the literature review, I will be preparing the work to use the tools which are going to help me find out the breaches in https://www.ccq.edu. After writing a very excellent literature review now it is the time to implement our Methodology. In the next stage of this project, research will be implementing my Research Methodology.

4. Research Methodology

The research starts with a survey on CCQ based on questions with respect to the security and impact of data breaches on the web server(https://www.ccq.edu.qa) of CCQ. This survey is based on 20 questions. In accordance with the survey carried out on Survey Monkey, the research has been carried on using the website https://www.surveymonkey.com/. It has been started by creating a question bank and has been shared with all the students of the Community College of Qatar through a web link. The survey has been shared with more than 200 students of CCQ which consists of both male and female students and we have received around 60 responses. The hyperlink for the survey is https://www.surveymonkey.com/r/JMVYSTN. The responses have been analyzed using the features of Survey monkey as the website is also providing the features of surveys and data analyzation.

After going through the survey and analysis based on the survey, it clearly shows that there are several necessary steps to be undertaken for safeguarding the confidential information using the guidelines provided by the CIA. In order to achieve the goal of securing the web server of CCQ, one should focus on three important terms which are confidentiality, integrity, and availability. While following the guidelines of the CIA, the first step of this research will be finding out the data breaches in the web server of CCQ where information of more than 600 students is stored. In this research, OWASP-ZAP has been used to find out the data breaches which is an inbuilt tool of Kali Linux.

Extensive research has shown that there is a significant threat of data breaching in our Community College in Qatar (CCQ) which paved the idea to work on finding the data breaches as CCQ is one of the best colleges in the Middle East. A large number

of students from Qatar have registered therein various courses and in our Website server ccq.edu.qa, details of all the students are stored in the database like Names, Grades, Reports, emails, etc., which pose a threat of data breaches to occur. Therefore, I have decided to find out the data breached on our Web server ccq.edu.qa and take the steps to secure those data breaches.

A number of cross-sectional studies suggest that data breaches have occurred with the use of Kali Linux as an OS and OWASP-ZAP as a tool to launch an attack on CCQ. Finding a data breach is not so easy in this world of the Cyber Age. OWASP-ZAP is the inbuilt tool of Kali Linux, which is very powerful to find the breaches on the basis of XSS, SQL Injection and other several options are available in it. The OWASP Zed Attack Proxy (ZAP) is one of the world's most popular free security tools and is actively maintained by hundreds of international volunteers. It can help us automatically finding out security vulnerabilities in our Web applications while we develop and test our applications. Kali Linux is an OS which is specifically designed for penetration testing, information gathering, and Wi-Fi Cracking. It has more than 600 tools built in for the user security analysis and hacking.

Using the tool OWASP-ZAP the attack has been launched on CCQ web server (https: www.ccq.edu.qa) and it took nearly about 45 minutes to get the required output with the data breaches.

After implementing the fact-finding methodology, Research came to know that are several data breaches. Those breaches can be very dangerous and insecure. The first data breaches that were found in our Web server https://www.ccq.edu.qa is containing a mixture of secure and insecure pages which means some are https and some are HTTP. Another breach that was found on the Web server is "cross-domain JavaScript source file inclusion". Also, the research found a data

breach “Web browser XSS protection is not enabled”. In the next phase of this research, the results of the methodology are shown with the steps to counter the data breaches to secure the web server.

5. Results

In order to get a clear understanding of the project, it was very much important to research and analyze the data and information stored on the servers of CCQ. So, a survey has been carried out based on 20 questions using the website survey monkey. Responses to both male and female students have been received which we analyzed and got the results for each question.

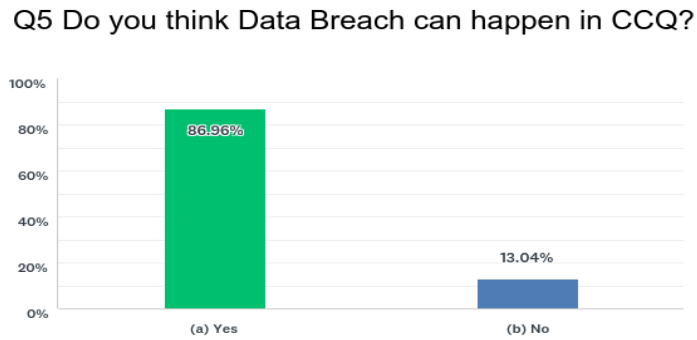

Figure 1. Distribution of Data breach in CCQ

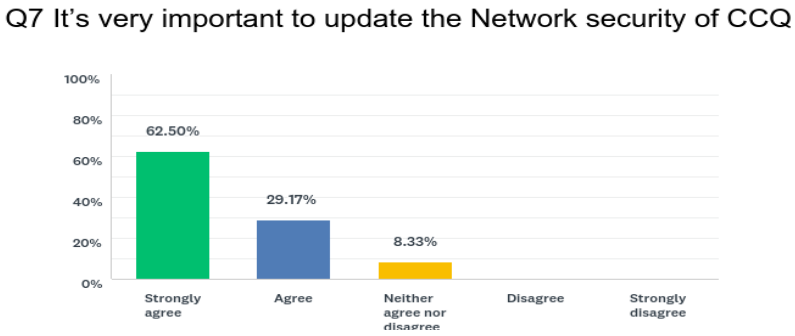

Figure 2. Distribution Related to Network Security of CCQ

Consequently, as per analysis and research based on survey found that there is a very big threat to occur in CCQ as it shows in the figure1. The ratio of data breaches to occur in CCQ is 86.96%. Only 13.04% of students think that data breach can't occur in the web server of CCQ. In the next question of the survey, the analysis found that 62.5% of students think that the network security of the CQQ needs to be updated as shown in figure 2. The ratio of more than 62 % of students Strongly agrees with updated network security.

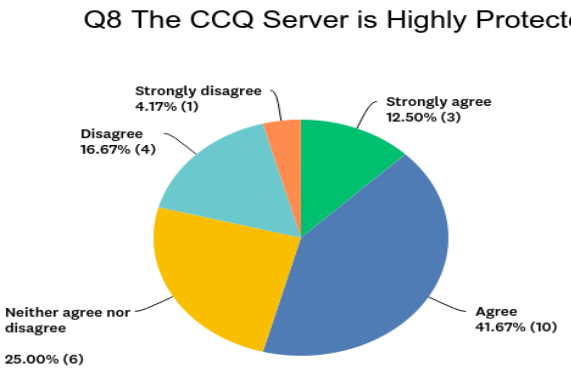

Figure 3. Distributions for CCQ server

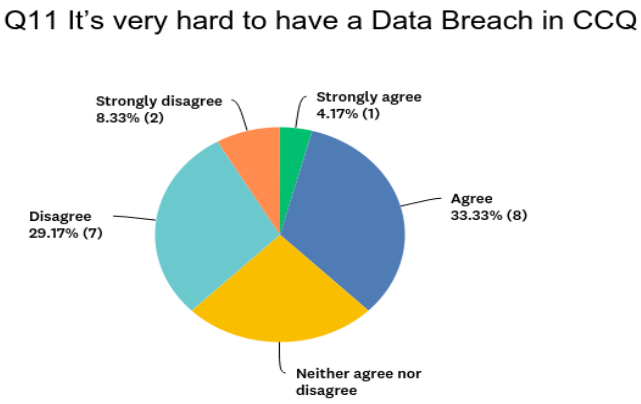

Figure 4. Distributions for Data Breaches in CCQ

Furthermore, according to the survey and analysis of survey monkey, only 41.67% of students of CCQ think that the web server is highly protected as shown in figure 3. While 29.17% of students disagree with it so it means the ratio is more but still 60 percent of students feel that the server is not highly protected. In figure 4, 33.33% of students feel that it is very hard to have a data breach in CCQ server while 29.17% think that are the chances of having a data breach in the server.

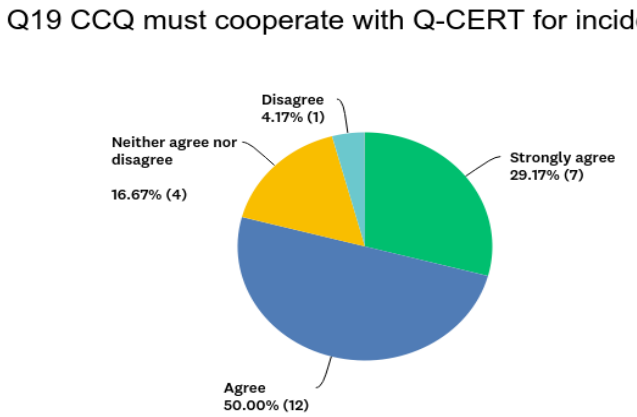

Figure 5. Distributions in cooperation of CCQ with Q-CERT

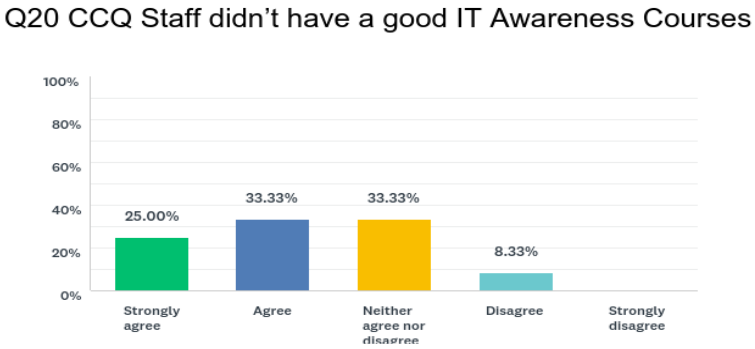

Figure 6. Distributions in IT Staff Awareness in CCQ

Furthermore, as the web server has the information of students stored in the database. The information of students like grade cards, QID's, etc. need to be secured.

In this figure 5. 50% of students of CCQ found that the college should cooperate with Q-CERT (Qatar National Information Security Centre) for incident response to make sure that the confidential information is secured. Q-CERT was the first-ever CERT to be set up within the Center East. Plans for Q-CERT were to begin with reported on December 2006 after ictQATAR and the CERT Coordination Center entered into an association. It marked a participation understanding with the SANS Organized to supply preparing courses in cyber security for IT specialists in Qatar's government. On November 2016, the primary GCC cyber penetrate was held beneath the support of Q-CERT and was locked in in by web security masters from four GCC nations.

Therefore, With the survey and analysis, it was very important to start gathering information about the web server of CCQ and find the data breaches to counter the data breaches in the server and make sure that the data is secure.

Consequently, the last question of survey 33.33 % agree and 25% of students of CCQ feel that IT Staff of CCQ doesn't have good IT Awareness Courses. In order to secure the network, it is very much mandatory that the IT Staff should be very aware of every security tool to protect the network and Information within the network.

Furthermore, after implementing the methodology, the research found several data breaches in the targeted website https://www.ccq.qa which are shown in figure 7 below.

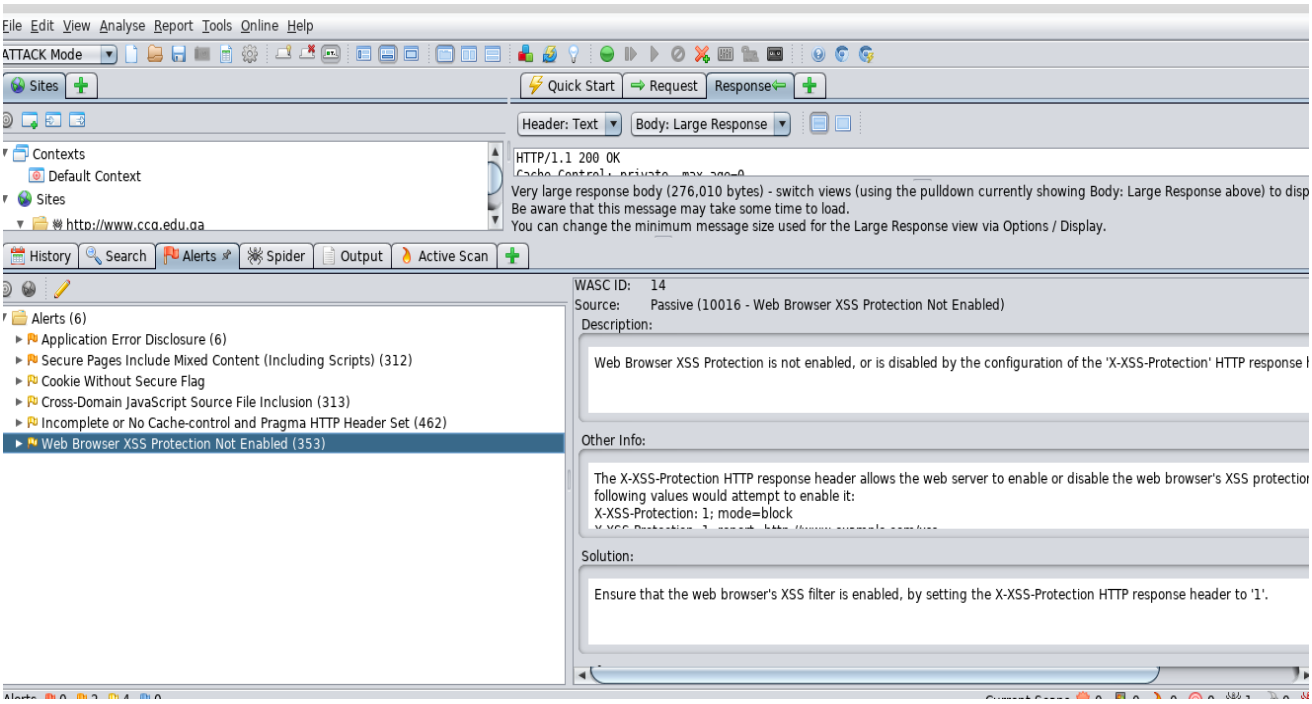

Figure 7. Data Breaches Found in CCQ

Furthermore, the next part will suggest countermeasures to encounter these data breaches or vulnerabilities. In order to make the web pages secure as research found that there is a mixture of HTTP and https pages used in the target server.

Implementing the measures to secure this breach. So, the steps that I have taken to secure that pages are mentioned below.

1. By using the SLL certificate is the easiest path to secure the Web server or an address. But there are several other factors that can be done to prevent the hackers and malware from compromising the Website.
2. To secure the net server one should keep our Web server continuously update. Failing to update the computer program, security, and scripts are perfect way">the most perfect way to allow programmers and malware to assault your location. By upgrade, the server one will get patches through which one can make

secure the net pages and the whole web server. Besides, the server supervisor ought to moreover keep the net server's advanced certificates continuously up to date.

3. Server director must introduce a security device. There is a parcel of site firewalls accessible, but the leading one that a supervisor can select is Sucuri Firewall which is paid one for the most excellent security apparatus for approaching activity.
4. The Security Engineer has got to introduce the SLL Certificate so that all the pages on the Net server are secure.

Furthermore, another breach that was found on the Web server is "cross-domain JavaScript source file inclusion". Browsers secure web pages of one domain from reading Webpages in other domains. But they do not secure pages of a domain from referencing resources in other domains. Most regularly, they permit pictures to be rendered from other spaces and scripts to be executed from other spaces. An included script doesn't have it possess security setting. It runs within the security setting of the page that included it. For example, if www.ccq.edu.qa includes a script hosted on www.google.com then that script runs in the evil context, not in the Google context. So, any user data in that script will leak.

Hence, Guarantee JavaScript source records are stacked from as it were trusted sources, and the sources can't be controlled by conclusion clients of the application.

<script type="text/javascript" async defer id="gauges-tracker" data-site-id="4eab0ac8613f5d1583000005" src="//secure.gaug.es/track.js"></script>

Consequently, this is typically a problem if you are using JSONP to transfer data from one place to another. Let's Consider a Website which will have a domain A that uploads information from domain B.

The user needs to be authenticated to site A and B, and because the Same Origin Policy prevents older Web browsers from communicating directly with a different domain (B) than the current page (A), the developers decided to use JSONP. So, site A includes a script pointing to http://B/userdata.js which is something like:

displayMySecretData ({"secret":"this is very secret", ...})

Therefore, A defines a function called displayMySecretData, and when the included script from server B runs, it calls that function and displays the secret data to the user.

Consequently, the next breach that I found is “Web browser XSS protection not enabled”. Web Browser XSS Protection and security are not enabled, or it is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the Web server. The X-XSS-Protection HTTP response header permits the Web server to enable or disable the Web browser's XSS protection mechanism. The following values would attempt to enable it:

X-XSS-Protection: 1; mode=block

X-XSS-Protection: 1; report=http://www.ccq.edu.qa/xss

The following values would disable it:

X-XSS-Protection: 0

The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit).

Therefore, note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length). In order to Prevent this breach or get rid, make sure that the Web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.

Thereafter, implementing all these operations, I’m sure that Our web server will be very secure and these data breaches and vulnerabilities will be removed and the storage server will be secure.

In this project, our work was to find out the vulnerabilities or Data Breaches in the web server https://www.ccq.edu.qa. also, the necessary steps to be taken to secure the web server from those data Breaches. As mentioned in the methodology, research has used the following tools to implement our work and get the results.

OS ----Kali Linux

Tools used for finding Data Breaches: OWASP ZAP (Zed Attack Proxy)

Target Web Server: https:/www.ccq.edu.qa

6. Discussion

Overall, this research provided a way to gather information from the students of CCQ using a survey based on 20 questions. Responses from more than 60 students of the college have been received and analyzed. From the analysis and research based on responses given by the Male and Female students of CCQ, we got to know that the Web Server is not highly secure to protect the maintain confidentiality, integrity, and availability. The results of the survey contributed to protecting the web server by finding out the data breaches and implementing the mandatory measures to counter those data breaches. Although this research surveyed, only 60 students of CCQ but weblink has been shared to more than 100 students. Research is a key method that every individual should go forward to protect and safeguard their own private and public data. Following are some recommendations that research has received from the survey.

Furthermore, 86.66% of students of the college think that their chances of a data breach to happen in the web server of CCQ because they think the server is not secure as the research found it.

Consequently, 66% of students also feel that network security should be updated. It will protect the information within the network and students can secure the web very freely. By updating the network security

almost 80% security of the server will be covered.

Furthermore, 12% of students strongly agree and 47% agree that the web server is highly protected. Using the tool OWASP-ZAP we found that there more than 4 data breaches in the server, which is very dangerous in terms of information loss.

Henceforth, according to the survey on data breaches research found only 8% students feel that it is very hard to have a data breach in CQQ and it is true as we found several data breaches in the server of the Community College of Qatar.

According to the responses received from Students, 20% Strongly agree and 50% agree that CCQ should cooperate with Q-CERT for incident response. Because student information is very important it needs to be protected.

Based on the survey, almost 60% of Students of the college also feel that the IT Staff is not more aware of security and how to secure the network.

Finally, we implemented the tool to find out the data breaches based on the survey. The research found several data breaches and has given the countermeasures to implement them in the network of the Community College of Qatar.

7. Conclusion

The problems of data breaches are long-lasting in terms of identity theft and commercial standards. Hackers in the entire world are very much skilled to get the breaches in the network by breaking down the network. In this project, I have used my skills to find the most dangerous breaches in the web server https://www.ccq.edu.qa. As per the literature review, I have analyzed that security is the main part of our personal

belongings. So, I stepped in and started finding ways to find out the data breaches. The research found the data breaches and in the next phase, we gave the countermeasure to secure our web server from those data breaches. Finally, I came to the conclusion of this project I should always take care of our personal privacy as it is a part of securing your identity. After taking the measures to counter the data breaches my next step or my future will be physically implemented these measures on the Web servers https://www.ccq.edu.qa and makes sure that the data and information will be safeguarded for future and students and faculties and enjoy the browsing without any insecure sensitivity.

8. Recommendation

Cybersecurity or information security provides us the protection from theft or damage of hardware and software resources in the network. In this research, work has been carried to find out the critical issues in the web server of Community College Qatar. In this work, we found several issues or data breaches in the web server of CCQ which can be the threat to data stored in the server. Furthermore, in this research, a theoretical countermeasure has been given to safeguarding the data stored on the servers. The research recommends safeguarding the web servers physically by applying the necessary countermeasures to fully secure the network of CCQ.

References

[1] I. P. a. C. U.S. Marketers, "THE IMPACT OF DATA BREACHES ON REPUTATION & SHARE VALUE," Ponemon Institute LLC , USA, 2017.

[2] C. J. Ping Wang, "CYBERSECURITY INCIDENT HANDLING: A CASE STUDY OF THE EQUIFAX DATA BREACH," *Issues in Information Systems ,* pp. 150-159, 2018.

[3] Malhotra, "Risky business: The impact of data breaches," https://blog.kenan-flagler.unc.edu/risky-business-the-impact-of-data-breaches/, USA, 2018.

[4] K. M. Gatzlaff, "The Effect of Data Breaches on Shareholder Wealth," College of Business Florida State University , Florida , 2008.

[5] T. Wu, "https://www.epic.org/privacy/data-breach/equifax/," 14 April 2018. [Online]. [Accessed Feb 2019].

[6] K. Dane, "Considering Data Breaches: Public Information, Corporate Responsibility, and Market Valuations," University of Washington, Washington, 2019.

[7] K. T. E. B. a. O. C. G. Sowmya Karunakaran, "Data Breaches: User Comprehension, Expectations, and Concerns with Handling Exposed Data," in *USENIX*, Baltimore, 2018.

[8] C. S. W. AshleyA. Hall, "DATASECURITY: A REVIEW OF MAJOR SECURITY BREACHES BETWEEN 2014 AND 2018," *Federation of Business Disciplines Journal,* pp. 50-63, 2018.

[9] W. Fattouh, "Middle East highest region prone to cyber threats in the world," Saudi Gazette, Middle East, 2016.

[10] K. J. a. S.-Y. P. Bokyung Kim, "Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity," *Kim et al., Cogent Business & Management,* pp. 1-15, 2017.

[11] S. Mello, "Data Breaches in Higher Education Institutions," University of New Hampshire Scholars' Repository(https://scholars.unh.edu/honors/400), Hampshire , 2018.

[12] H. A. Q. J. B. I. Saeed S. Basamh, "An Overview on Cyber Security Awareness in Muslim Countries," *International Journal of Information and Communication Technology Research ,* pp. 21-24, 2014.

[13] H. K. Aiswarya Baby, "A Literature Survey on Data Leak Detection And Prevention Methods," *International Journal of Advanced Research in Computer Science,* pp. 2416-2418, 2017.

[14] Y. Li, "Information security research: External hacking ,insider breach, and profound technologies," https://lib.dr.iastate.edu/etd/15566/, Capstones, 2017.

[15] P. Orszag, "Insurancejournal (https://www.insurancejournal.com/news/national/2018/04/13/486383.htm)," 13 04 2018. [Online]. [Accessed 12 Feb 2019].

[16] M. I. a. S. Frenkel, "https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html (New York Times)," 28 9 2018. [Online]. [Accessed 12 Feb 2019].

[17] V. Haran, "https://www.bankinfosecurity.com/qatar-national-bank-suffers-massive-breach-a-9068 (Bank Info Security)," 2016 April 2016. [Online]. [Accessed 12 Feb 2019].

[18] T. Magee, "https://www.computerworlduk.com/galleries/data/most-significant-uk-data-breaches-3662915/," 8 Feb 2019. [Online]. [Accessed 12 Feb 2019].

[19] F. J. Kongnso, "Best Practices to Minimize Data Security Breachesfor Increased Business Performance," Walden University, USA, 2015.

[20] M. B. G. G. Maria Cristina Arcuri, "How does cyber crime affect firms? The effect of information security breaches on stock returns," in *First Italian Conference on Cybersecurity (ITASEC17)*, Venice, Italy, 2017.

[21] M. Q. K. G. M. L. A. Kutub Thakur, "An Investigation on Cyber Security Threats and Security Models," in *IEEE 2nd International Conference on Cyber Security and Cloud Computing (CSCloud 2015),*, New York, USA, 2016.

[22] D. Bisson, "Barkly," 3 July 2018. [Online]. [Accessed 3 April 2018].

[23] J. Sullivan, "Business Insider (https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12)," 30 Dec 2018. [Online]. [Accessed 30 Dec 2018].

[24] R. James, "https://www.itproportal.com/features/biggest-cyber-security-breaches-2018/," 27 Novermber 2018. [Online]. [Accessed 27 Nov 2018].

[25] I. Phenomenon, "THE IMPACT OF DATA BREACHES ON REPUTATION& SHARE VALUE," Centrify, UK, 2017.