I.J. Information Engineering and Electronic Business, 2016, 5, 1-8
Published Online September 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2016.05.01

Vulnerabilities Assessment of Emerging Web-based Services in Developing Countries

Abdus Satter
Institute of Information Technology, University of Dhaka, Dhaka 1000, Bangladesh
Email: bit0401@iit.du.ac.bd

B M Mainul Hossain
Institute of Information Technology, University of Dhaka, Dhaka 1000, Bangladesh
Email: raju@du.ac.bd

***Abstract*—**To cope up with the pace of digitalization all over the world, like developed countries, developing countries are also offering services to its citizens through various online portals, web applications and web sites. Unfortunately, due to the lack of consideration on vulnerability issues during the development phase, many of those web based services are suffering from serious security threats. For these developing countries, vulnerability statistics are required to have insight about the current security status of the provided web services. That statistical data can assist the stakeholders to take appropriate actions against cyberattacks. In this work, we conduct a survey to observe the responses of web based services against four most commonly found web attacks called Man in the Middle, SQL Injection, Cross Site Scripting and Denial of Service. We carry out the survey for 30 websites (applications) of Bangladesh as the country has been focusing on digitalization of government services for the last few years and has already been offering various online services to its citizens. Among the 30 websites of several categories, result shows that approximately 77% sites are vulnerable to Man in the Middle attack whereas 3% are vulnerable to SQL Injection and Cross Site Scripting.

***Index Terms*—**Man in the Middle, Denial of Service, Cross Site Scripting, Web Vulnerabilities, SQL Injection.

I. Introduction

Nowadays, web has become one of the common ways of broadcasting information throughout the world. Both government and non-government organizations are automating their operations using web based applications and websites. By taking advantage of this fact, first world countries are thriving day by day. On the other hand, to keep up with the pace, third world countries need to progress in this sector. Although the developed countries are far ahead in utilizing Internet and web based technologies, developing countries have also started to incorporate web based technologies.

Unfortunately, when developing countries are paying attention to web based technologies, various web attacks have been discovered at the same time that might cause serious damage to the target websites or web applications. Clearly, this situation is orthogonal to the motivation of using web based technologies. Therefore, study to assess the vulnerabilities against various web attacks, in the incorporated web-based technologies of developing countries, is very important. Previous analysis on the web portals of Asian region countries has already shown the lack of necessary attributes, including security, during the implementation phase [1].

Moreover, due to the rapid development of websites and web applications, sometimes vulnerability issues are totally ignored during the development phase. Added to that, there exists limitation on budget for the security aspects of a project. Managerial departments do not pay much attention to it since the security issues are not visible immediately, but those are there only to be revealed later. As a result, today or tomorrow, security of those vulnerable websites are breached which ends up in significant amount of financial loss; most importantly, data is compromised.

To keep these sites safe from cyberattacks, statistical data is required which will assist security specialists and intended authorities to gain insight about the vulnerability status. For example, statistical data on vulnerable websites in different sectors with possible cyberattacks can help the policy makers to allocate budget for security aspects.

Throughout the rest of the paper, we use the term ‘website’ to refer to the technologies used various web services, i.e., web site, web application, web portal etc. In the following, we give a little context of four web attacks that we consider for this work.

A. Man in the Middle (MITM)

Man in the Middle (MITM) attack is usually performed to get or alter information between two parties. The attacker can perform both active and passive attack using this approach where active attack involves altering the original message and passive attack involves just obtaining the copy of the message. A possible scenario of MITM attack is illustrated in Fig. 1.

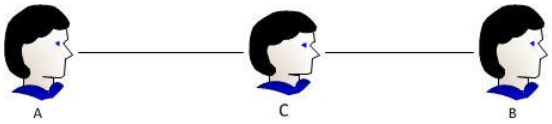

Fig.1. A scenario of Man in the Middle attack

Suppose, A and B are the legitimate users and C is the attacker. A sends a message to B and C captures the message during the propagation of the message from A to B. In case of active attack, C alters the message and send the altered message to B. Upon receiving the message, B thinks that the message has come from A without knowing that the message has been altered somewhere in the middle and thus, both A and B turn out to be the victims of the attack since private communication between A and B has been compromised.

In case of passive attack, C just captures the message, reads the content of it and pass an unaltered copy of the original message to B. In this case, even though the attacker has not changed anything, but it could still be a serious security breach since attacker can see what A and B are communicating about.

B. SQL Injection Attack (SQLIA)

SQL Injection Attack (SQLIA) is another popular attack which facilitates the attacker to gain access to database. In this attack, attackers inject malicious code in the form of a database query and the attacker's intended data is returned by the database engine once the query is executed. For example, consider the following query:

```
"SELECT * FROM users WHERE
  name = '" +userName+ "';"
```

Here, the statement is used to retrieve all data from `users` table where name matches with the given `userName`. However, to perform SQL Injection, attacker can try to append the following malicious code with the original query.

```
' OR '1'='1
```

If the attacker is successful, the actual query is changed into the following query and the attacker retrieves all data from the `users` table once the query is executed.

```
"SELECT * FROM users WHERE
  name = '" +userName+ "' OR '1'='1';"
```

C. Cross Site Scripting (XSS)

Cross Site Scripting (XSS) is the most popular and widely carried out website attack [2]. As it is shown in Fig. 2, usually, attacker injects malicious script to the client end (i.e. browser) to steal important data like session, cookie, etc. from the browser.

To inject scripts, attacker finds some vulnerable websites where scripts can be easily injected and those sites do not check whether the input value contains malicious code or not. When the victim user browses those websites, all the malicious scripts injected there are executed by the victim's browser. Such execution assists the attacker to gain access to session value, cookies, credentials, etc. of target user. In fact, the malicious code often contains server `url` of attacker and credentials, session, cookies of victim are transferred through that `url`.

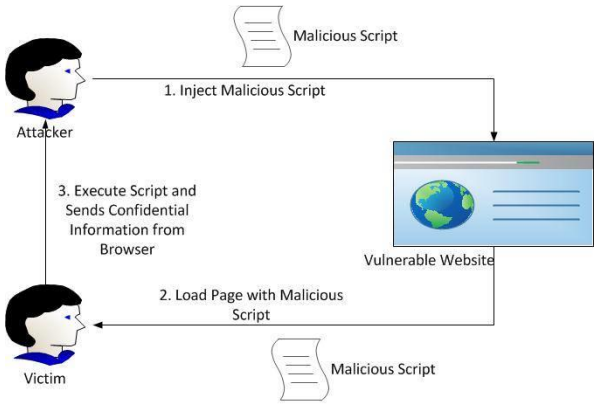

Fig.2. A scenario of XSS attack

D. Denial of Service (DoS)

Denial of Service (DoS) attack prevents the legitimate users to receive service from a server. There are several forms of DoS attacks such as SYN flood, HTTP flood, ICMP request, and so on. Usually, attackers keep the server busy by sending simple request from anonymous clients with different IP addresses. Upon receiving the requests from the clients, server starts to send responses to the clients. As there are no existence of such clients and responses are not expected by those clients, server keeps itself busy by sending unnecessary response packets to the anonymous clients. Since, server has a limit on maximum number of client requests it can handle, the legitimate clients are refused to get services if the server already exceeds that limit and doesn't not have enough resources to handle further requests. Usually, DoS attacks are done by using many zombies that continuously send requests to the target server from fake IP addresses.

In this work, we conduct a survey on the websites of a developing country, Bangladesh, to assess the status of those sites against MITM, SQLIA, XSS and DoS attacks. Our work makes the following contributions:

- We simulate MITM, SQLIA, XSS and DoS attacks against 30 different websites from diverse application domain in Bangladesh and report the statuses of those sites in response to these attacks.
- We provide statistical data that could be used to have an insight about the type of attacks that are most probable and need immediate attention to be addressed properly.

The rest of the paper is organized as follows. Section II contains related works. Our approach to assess the vulnerabilities is presented in Section III. We also

describe the procedures of carrying out each attack under Section III. Section IV gives the experimental results and analysis. Conclusion with discussion is presented in Section V.

II. Related Works

Many studies have been conducted on different types of security vulnerabilities and attacks in the literature. Johari and Sharma conducted a survey on SQL Injection Attack (SQLIA) and Cross Site Scripting (XSS) [3]. In this study, different ways of conducting SQLIA and XSS in web applications are discussed.

Obfuscation based technique, by combining static and dynamic analysis, has been proposed to detect the presence of possible SQL Injection Attacks (SQLIA) in a query before submitting it to a DBMS [4]. Classification of various SQL injection attacks and analysis on the basis of risk associated with each attack are also discussed recently [5].

Feature extraction algorithm to extract basic and context features from the source code of web applications for predicting context-sensitive Cross-Site Scripting (XSS) security vulnerabilities has been proposed [6]. Tool has been developed to automatically analyze web applications to find the XSS vulnerabilities [7]. Static taint analysis and pattern matching techniques have been proposed along with an implementation of prototype tool [8].

For example, Wireless Intrusion Detection System (WIDS) has been proposed to detects the MITM attack using ARP poisoning and IP Spoofing. This system works correctly when the attacker is static and under the coverage of a single sensor during the complete period of attack [9]. Moreover, MITM attack on the newly emerging 3G mobile technologies, Universal Mobile Telecommunication Standard (UMTS), has also been performed [10].

Techniques like multivariate correlation analysis [11] has been employed to identify DoS attack. A variety of definitions and aliases of low DoS are summarized and simulation of attacks are investigated in a survey [12]. A Survey on distributed DoS attack tools has also been conducted along with the trace back mechanisms to trace the attacker [13].

However, none of the studies provide specific and combined statistics on MITM, SQLIA, XSS and DoS attacks, for the websites of a developing country where the new sites are emerging on a continuous basis. To the best of our knowledge this is the first initiative that focuses on collecting the statistical data of a developing countries against these attacks.

III. Our Approach

Our approach to perform MITM, SQLIA, XSS & DoS attacks, along with the environmental setup, are described in the following.

A. Procedure of MITM Attack

MITM can be performed when sender or receiver does not use any encryption technique while transferring secret information. In this study, those sites are selected as vulnerable which do not have any signature but takes secret information from the users.

To perform MITM, two machines have been used where one is considered as victim machine and another is for performing the attack. Kali Linux 2.0[1] is used for the attack. Kali Linux comes with a software named `Ettercap` which is used for this attack. Another tool named Wireshark[2] is used to capture the victims packets. These packets are then analyzed to obtain secret information like user name, password, etc. of the victim.

B. Procedure of SQLI Attack

SQL Injection attack can be accomplished when websites or web applications take user input without checking whether the input value contains malicious SQL code or not. To detect security hole for this attack, we select the URLs of a website that are used to submit `form` data to the server and the database operation is performed based on that submitted data. Usually, a website becomes exposed to the vulnerability when `'HTTP GET'` verb is used to transmit data from the client to the server and that data is directly used in the database query.

In this study, A tool named SQLMAP is employed to carry out this attack. SQLMAP is a built-in application in Kali Linux 2.0. This tool takes the vulnerable `url` as input and executes the attack. This tool is so powerful that it automatically detects the database engine and after getting access to the database, it starts to run SQL query given by the attacker.

C. Procedure of XSS Attack

A website suffers from Cross Site Scripting attack when user input is directly displayed in the website without validating the input value. As a result, attacker creates malicious scripts which can steal cookies, session data or credentials from a browser and injects that scripts as input to the website. Therefore, when the victim user browses the vulnerable page, these malicious scripts are loaded and executed in the victim's browser. In this study, websites that do not check for the malicious scripts, but directly insert those scripts in the page are considered as vulnerable websites against this attack.

In order to simulate this attack, vulnerable websites are detected by simply putting the following `JavaScript` code in the input field.

```
<script>alert('This site is
vulnerable for XSS')</script>
```

After submitting this to the server, browser is refreshed or redirected to the page which is responsible to view that data. If the page shows the alert having text "`This`

[1] https://www.kali.org, last verified Jun 28, 2016
[2] https://www.wireshark.org, last verified Jun 28, 2016

`site is vulnerable for XSS`", the website is considered as vulnerable against XSS.

D. Procedure of Denial of Service Attack

Three types of Denial of Service (DoS) attack are considered in this study. Those are SYN flood, HTTP flood and Slowloris. To perform SYN flood and HTTP flood, we use MetaSploit[3] which is a built-in tool in Kali Linux and specially designed to perform DoS attacks. For Slowloris, we use an open source `perl` script[4].

Ten machines are used to execute each type of attack where each machine is equipped with Intel Core i3 processor and 4GB RAM. These machines are used as zombie that we use to fake client requests and send unnecessary packets to the server. Besides, we use another machine that is connected to a network different than the network where zombies are connected. This machine is used to simulate a legitimate user and request is sent from that machine to the target website. For each website, response time for the legitimate user is calculated before and after the DoS attack carried out by the zombie machines.

E. Dataset Selection

In order to conduct this study, Bangladesh is chosen as a representative of developing countries and 30 Bangladesh centered websites from six different categories are considered. The categories are: Governmental, Banking, Job Portals, e-Commerce, Academic and Blogging. A summary of the dataset is shown in Table 1. Ranking of each website is obtained from the popular web traffic data provider site Alexa[5].

In case the site is not ranked because of its comparatively new appearance in the web or for some other reasons, we put not applicable (N/A) as the rank value. To make the selection process distributed, we choose both low and high ranked sites. In this study, the rank of the sites vary from 15 to 29627. Moreover, we choose several websites that have been developed recently or used occasionally by the users and not ranked yet.

IV. Results and Analysis

Four types of attack that have been described earlier are performed on the websites chosen for the study. A summary of the result (i.e. which website is affected by which attack) is depicted in Table 2. Analysis of the results for each type of attack has been discussed in the following paragraphs.

As it is shown in Fig. 3, 77% websites are vulnerable to MITM. Only one website among all listed in Table 2 is found uses certificates for secure communication purposes. However, other websites do not use any encryption technique to transfer secret information such as login credentials, identification numbers, and other sensitive information. As a result, by employing MITM, attackers can easily obtain all of these secret information which can be used for the purpose of admission or grading tests in various educational institutions, authentication in online job portals or online visa applications. These information is adequate enough to harm the victim user.

3% of the websites are found vulnerable for SQL Injection attack as it is shown in Fig. 3. From Table 2, it is seen that the vulnerable website is the website of an educational institution which manages different secret contents, and the users need to be authenticated to work with that contents. For the rest of the websites, we found them tolerant against our attack.

Fig. 3 shows that 97% of the sample dataset are free from Cross Site Scripting attack. According to the summary illustrated in Table 2, XSS attack has successfully been performed on a blog site. The site which is vulnerable against XSS attack, offers the visitors to comment on published topics. After receiving input from the user, it does not check the existence of malicious script as the input value. Rather, it directly stores input data in the database. As a result, when the page is reloaded or browsed, the malicious scripts are also executed in the browser. For this reason, this site is marked as vulnerable in our study.

In case of Denial of Service (DoS) attack, we report the results only for those websites that we are able to take decision deterministically. That means, we can draw the conclusion on whether the site is victim of DoS attack or not. In case of the nondeterministic behavior, we report the result as undecided (N/A in Table 2). This is because of the nature of the DoS and distributed DoS attacks. It is not always easy to conclude decisively about the impact of the DoS attack. For those sites where the result is undecided (N/A), we observe a little interruption in service. But, we cannot confirm that if that interruption of service is because of DoS attack or some other factors like slow Internet connection, using few number of machines to simulate the attack, etc. As it is shown in Fig. 3, we cannot take the decision for 50% of the websites. As a result, we find 23% of the websites are vulnerable against DoS attack, whereas 27% websites are resistant against the DoS attack carried out by our approach.

A. Result Analysis

An overall analysis of the results of this study shows that all the governmental sites are vulnerable to MITM whereas these sites are used for managing sensitive information like providing passport services, printing and publishing governmental documents, issuing national IDs, etc. Besides, all academic sites, assessed in this survey, are also vulnerable to MITM due to not employing any certification mechanism.

Five different discussion forums, including both personal and community blogs, are analyzed and only one of those blogs is found using SSL certificate for secured communication.

Nowadays, job seekers search jobs and, drop their resumes and relevant confidential information through

[3] https://www.metasploit.com, last verified Jun 28, 2016
[4] https://github.comllaera/slowloris.pl (Jun 28, 2016)
[5] http://www.alexa.com, last verified Jun 28, 2016

different job portals. Considering the importance of job portals, the study includes five well known job sites. Unfortunately, none of these portals use any sort of encryption techniques for sensitive data transmission, which may influence the attackers to exploit MITM.

Five e-commerce sites are studied to observe the security measures against MITM. We find three of the e-commerce sites out of five use SSL certificates to prevent web attacks, given that some of these sites need to deal with financial activities including online payment service.

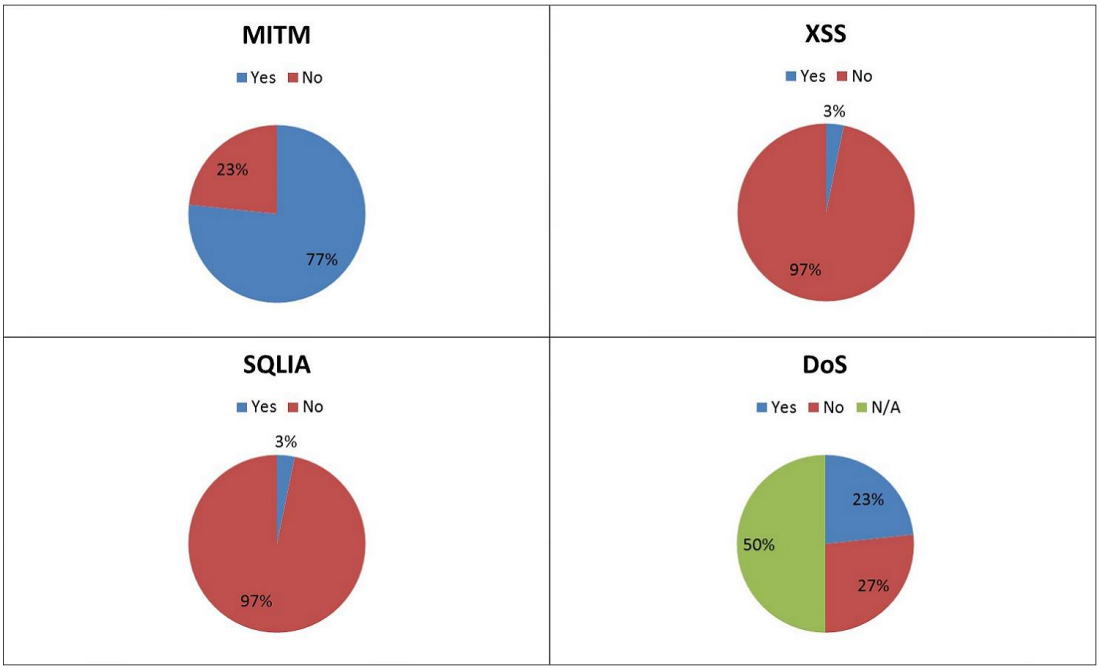

Fig.3. Percentage of websites vulnerable against each attack (Yes = Vulnerable, No = Not Vulnerable, N/A = Undecided)

The scenario does not change for banking systems as well. Although, all banking or financial institutions should use `https` connection for online services, this study finds that still some of the banks (both public and private) provide online banking services without using any encryption techniques, which might encourage attacker to carry out MITM attacks on those sites.

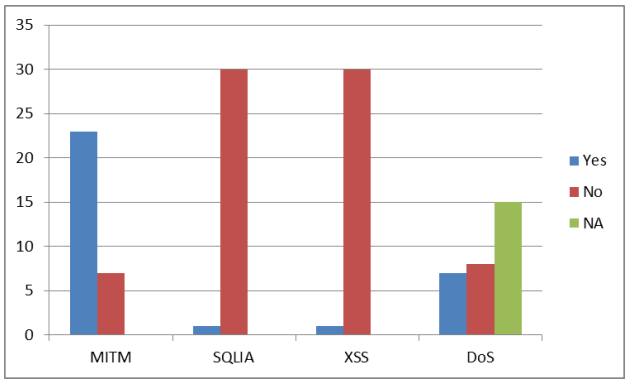

Fig.4. Comparative results for all four attacks (NA = Undecided).

On the plus side, 97% websites of this study are found protective against SQLI and XSS. One of the reasons could be that, these websites employ different kind of frameworks (i.e., Entity framework, Zend framework, etc.) during the development phase, which offer features to defend attacks like SQLI and XSS. Moreover, it is worth mentioning that we performed very basic kind of SQLI and XSS attacks. There are many sophisticated versions of these attacks which might reveal more vulnerabilities in the websites of this study. A comparative results for MITM, SQLIA and XSS attacks are shown in Fig. 4.

Clearly, MITM is the most dangerous attack in compare to XSS, SQLIA, and DoS attacks for the developing countries (i.e. Bangladesh). One of the major reasons for huge vulnerability against MITM attack could be that almost every important website takes login credentials or share secret information without employing any certificate or involving any certification authorities. So, messages are passed as plain data throughout the Internet and attacker can easily grab the messages by performing MITM.

B. Measures Against Attacks

There are various techniques to defend the websites against these kind of attacks. Depending on the service that the website provides, the authority can take appropriate preventive measures. MITM attacks succeed when sender or receiver of data does not use any encryption technique while communicating with each other. If proper encryption mechanism is employed, the intruder will not be able to decrypt the message to read or alter without knowing the secret key. Different SSL certificate authorities provide certificates to prevent this kind of attack by employing encryption on secret information.

Table 1. List of Websites Used for Vulnerabilities Assessment

Category	Serial No.	Websites	Rank in Bangladesh
Governmental	1	http://www.passport.gov.bd	730
	2	http://www.nidw.gov.bd	1787
	3	http://www.mofa.gov.bd	1525
	4	http://www.dpp.gov.bd	1525
	5	http://fellowship.ictd.gov.bd	15
Banking	6	https://www.bb.org.bd/	N/A
	7	https://www.agranibank.org/	4285
	8	https://rupalibank.org/	1568
	9	http://www.janatabank-bd.com	N/A
	10	http://ebl.com.bd	N/A
Job Portals	11	http://www.bdjobs.com	3419
	12	http://www.chakri.com	542
	13	http://www.bd-career.com	5404
	14	http://www.jobsbangladesh.com	264
	15	http://www.bd4jobs.com	333
e-Commerce	16	http://www.priyoshop.com	723
	17	http://bikroy.com	4062
	18	https://chaldal.com	24002
	19	https://easy.com.bd	N/A
	20	https://rokomari.com	6650
Academic	21	http://www.du.ac.bd	190
	22	http://www.northsouth.edu	866
	23	http://www.cse.du.ac.bd	21456
	24	http://www.uiu.ac.bd	29627
	25	http://www.wub.edu.bd	9789
Blogging	26	http://www.amrabondhu.com	1525
	27	https://saiftheboss.com	5156
	28	http://www.shafaetsplanet.com	653
	29	http://addaablog.com	11231
	30	http://www.bishorgo.com	23

Table 2. Status of the Studied Websites against MITM, SQLIA, XSS and DoS Attacks. Yes, No and N/A indicate whether the corresponding attack was successful, not successful or undecided (for DoS only).

Serial No.	Websites	MITM	SQLIA	XSS	DoS
1	http://www.passport.gov.bd	Yes	No	No	Yes
2	http://www.nidw.gov.bd	Yes	No	No	N/A
3	http://www.mofa.gov.bd	Yes	No	No	N/A
4	http://www.dpp.gov.bd	Yes	No	No	N/A
5	http://fellowship.ictd.gov.bd	Yes	No	No	Yes
6	https://www.bb.org.bd	No	No	No	N/A
7	https://www.agranibank.org	No	No	No	N/A
8	https://rupalibank.org	No	No	No	N/A
9	http://www.janatabank-bd.com	Yes	No	No	N/A
10	http://ebl.com.bd	Yes	No	No	N/A
11	http://www.bdjobs.com	Yes	No	No	N/A
12	http://www.chakri.com	Yes	No	No	N/A
13	http://www.bd-career.com	Yes	No	No	N/A
14	http://www.jobsbangladesh.com	Yes	No	No	No
15	http://www.bd4jobs.com	Yes	No	No	No
16	http://www.priyoshop.com	Yes	No	No	No
17	http://bikroy.com	Yes	No	No	N/A
18	https://chaldal.com	No	No	No	N/A
19	https://easy.com.bd	No	No	No	N/A
20	https://rokomari.com	No	No	No	N/A
21	http://www.du.ac.bd	Yes	No	No	Yes
22	http://www.northsouth.edu	Yes	No	No	No
23	http://www.cse.du.ac.bd	Yes	Yes	No	Yes
24	http://www.uiu.ac.bd	Yes	No	No	No
25	http://www.wub.edu.bd	Yes	No	No	No
26	http://www.amrabondhu.com	Yes	No	No	Yes
27	https://saiftheboss.com	No	No	No	Yes
28	http://www.shafaetsplanet.com	Yes	No	Yes	Yes
29	http://addaablog.com	Yes	No	No	No
30	http://www.bishorgo.com	Yes	No	No	No

Attackers use SQLIA attack when they find that the vulnerable site does not verify input value that is directly used in the SQL query. In order to defend this attack, input fields which are used to take values that is executed as part of database query must be checked whether the value of that fields contain malicious SQL code or not. If such code is detected, the value of the corresponding input field should not be used and the query should not be executed.

A website or web application can be protected against XSS attack if injection of malicious scripts is stopped. This can be achieved by checking whether user input contains any script or not. If malicious scripts are found, the input should not be taken from the attacker who is trying to inject the malicious scripts.

Different validation frameworks are currently available for checking input values and validating the input. Using one of these frameworks can also reduce the XSS attacks. There exists technique to prevent Reflected Cross-Site Request Forgery (CSRF) by checking browser specific information [14]. An adapted version of this approach can also be tried to prevent XSS attacks. A runtime monitoring mechanism could also be used to verify the safeness before executing any script like it was used earlier in the field of Database Management Systems to prevent database deadlocks [15].

Finally, it is really very difficult to protect a system from DoS attacks. However, certain measurements can be taken to prevent this kind of vulnerability. For example, Internet Service Provider can check the validity of IP addresses while sending packet to other networks. Syn cookies work well as a countermeasure against SYN flood attack. The deployment of reverse proxy can defend the HTTP flood attack. Because of the nature of it, all of these initiatives, mentioned above cannot always stop DoS attack totally, but at least they can make it hard for the attackers to attack the system.

C. Recommendations

Considering the present scenarios, we make the following two recommendations for the respective authorities or institutions of the developing countries.

Recommendation 1: All websites that deal with sensitive information of users (citizens) and that involve monetary transactions should immediately start using digital certification (SSL certification).

Recommendation 2: There should be a central coordination and communication system to be used by the administrators of the same type of organizations.

The reason for the Recommendation 1 is to ensure the encrypted communication between the server (website) and browser (user's computer).

Recommendation 2 comes out of the observation of our study. Since, many of the websites are implemented by using some sort of frameworks, a central communication system for similar type (class) of organizations can help in case of an emergency. For example, an instant communication mechanism among the administrators of the governmental websites could help reducing the damage whenever a security hole of a framework is revealed. Because, administrators could respond to the situation immediately as they are supposed to be notified about the risk through central coordination system. We believe these recommendations can help to increase the security level of web-based services and hence, reduce the damages caused by the attacks presented in this work.

V. Conclusion

In this study, it has been seen that most of the websites are vulnerable to MITM in compare to XSS, DoS, and SQLIA. These websites share sensitive information without employing any encryption techniques. Most of the websites do not use any certificate while transferring secret information. This security hole paves the way to the attackers to obtain secret information through MITM.

On the other hand, we found only one educational websites that is vulnerable against SQLIA and one blog site vulnerable against XSS. Usually, blog sites are considered as common choice for the attackers to perform XSS attack since the users like to visit those sites frequently. Websites developed for business purposes are found mostly protective against this attacks due to using different SQL injection and XSS defending frameworks.

This study is conducted on 30 different websites in Bangladesh and four types of attacks are crafted to find different security vulnerabilities. In future, we plan to study more websites with other types of vulnerability both in Bangladesh and other developing countries. We also plan to assess the vulnerability status for the websites of developed countries and compare it with the status of developing countries.

References

[1] S. Chander and A. Kush, "Web portal analysis of asian region countries," IJIEEB, vol. 4, no. 5, pp. 25–32, Oct. 2012.

[2] D. Turner, S. Entwisle, O. Friedrichs, D. Ahmad, D. Hanson, M. Fossi, S. Gordon, P. Szor, E. Chien, D. Cowings et al., "Symantec internet security threat report: trends for July 2004-december 2004," Retrieved July, vol. 30, p. 2005, 2005.

[3] R. Johari and P. Sharma, "A survey on web application vulnerabilities (sqlia, xss) exploitation and security engine for sql injection," in Communication Systems and Network Technologies (CSNT), 2012 International Conference on. IEEE, 2012, pp. 453–458.

[4] R. Halder and A. Cortesi, "Obfuscation-based analysis of sql injection attacks," in Computers and Communications (ISCC), 2010 IEEE Symposium on, June 2010, pp. 931–938.

[5] C. Sharma and S. C. Jain, "Analysis and classification of sql injection vulnerabilities and attacks on web applications," in Advances in Engineering and Technology Research (ICAETR), 2014 International Conference on, Aug 2014, pp. 1–6.

[6] M. K. Gupta, M. C. Govil, and G. Singh, "Predicting cross-site scripting (xss) security vulnerabilities in web applications," in Computer Science and Software

Engineering (JCSSE), 2015 12th International Joint Conference on, July 2015, pp. 162–167.
[7] T. S. Rocha and E. Souto, "Etssdetector: A tool to automatically detect cross-site scripting vulnerabilities," in Network Computing and Applications (NCA), 2014 IEEE 13th International Symposium on, Aug 2014, pp. 306–309.
[8] M. K. Gupta, M. C. Govil, G. Singh, and P. Sharma, "Xssdm: Towards detection and mitigation of cross-site scripting vulnerabilities in web applications," in Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on, Aug 2015, pp. 2010–2015
[9] V. Kumar, S. Chakraborty, F. A. Barbhuiya, and S. Nandi, "Detection of stealth man-in-the-middle attack in wireless lan," in Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on, Dec 2012, pp. 290–295.
[10] V. A. Vallivaara, M. Sailio, and K. Halunen, "Detecting man-in-the-middle attacks on non-mobile systems," in Proceedings of the 4th ACM Conf. on Data and Application Security and Privacy, ser. CODASPY '14. New York, NY, USA: ACM, 2014, pp. 131–134. Available: http://doi.acm.org/10.1145/2557547.2557579
[11] K. K. More and P. B. Gosavi, "A survey on effective way of detecting denial-of-service attack using multivariate correlation analysis," in 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Oct 2015, pp. 246–250.
[12] Q. Zhu, Z. Yizhi, and X. Chuiyi, "Research and survey of low-rate denial of service attacks," in Advanced Communication Technology (ICACT), 2011 13th International Conference on, Feb 2011, pp. 1195–1198.
[13] R. K. P. Arun and S. Selvakumar, "Distributed denial-of-service (ddos) threat in collaborative environment - a survey on ddos attack tools and trace back mechanisms," in Advance Computing Conference, 2009. IACC 2009. IEEE International, March 2009, pp. 1275–1280.
[14] O. A. Batarfi, A. M. Alshiky, A. A. Almarzuki, and N. A. Farraj, "Csrfdtool: Automated detection and prevention of a reflected cross-site request forgery," IJIEEB, vol. 6, no. 5, pp. 10–15, Oct. 2014.
[15] M. Grechanik, B. M. M. Hossain, U. Buy, and H. Wang, "Preventing database deadlocks in applications," in Proceedings of the 2013 9th Joint Meeting on Foundations of Software Engineering, ser. ESEC/FSE. New York, USA: ACM, 2013, pp. 356–366. [Online]. Available: http://doi.acm.org/10.1145/2491411.2491412

Authors' Profiles

Abdus Satter is a graduate student at the Institute of Information Technology (IIT), University of Dhaka, Bangladesh. Currently, he is pursuing his Master of Science in Software Engineering (MSSE). He earned his Bachelor of Science in Software Engi-neering (BSSE) from the same institution with the top score in his class. His core areas of interest are software engineering, web technologies, systems and security. He has numerous awards in various national and international software and programming competitions, hackathons & project showcasings.

Dr. B. M. Mainul Hossain is Assistant Professor at the Institute of Information Technology (IIT), University of Dhaka, Bangladesh. He received his Ph.D. degree in computer science from University of Illinois at Chicago, USA. Before that, he earned his Bachelor of Science and Masters degrees from the department of Computer Science & Engineering, University of Dhaka, Bangladesh. He has the experiences of working both in industry and academia. He worked as a Software Engineer in Microsoft Corporation (Redmond, USA) & Accenture Technology Lab (Chicago & California). His core areas of interest are software engineering, security, data mining and machine learning.

How to cite this paper: Abdus Satter, B M Mainul Hossain,"Vulnerabilities Assessment of Emerging Web-based Services in Developing Countries", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.8, No.5, pp.1-8, 2016. DOI: 10.5815/ijieeb.2016.05.01

