Information Security in modern way of education system in Pakistan

Syed Muhammad Raza Jafri, Abid Khan, Fauzia Talpur, Sobia Saeed, Muhammad Asim Khan
Faculty of Computer Science & Information Technology
Institute of Business & Technology (IBT)
Karachi, Pakistan
ariesraza@gmail.com, r03ky@yahoo.com

Abstract—Internet, and in particular the World Wide Web, have become one of the most common communication mediums in the World. Millions of users connect everyday to different web-based applications to search for information, exchange messages, interact with each other, conduct business, pay taxes, perform financial operations and much more. Some of these critical web-based services are targeted by several malicious users intending to exploit possible weaknesses and vulnerabilities, which could cause not only the disruption of the service, but also compromises the users and organizations information. Most of the times, these malicious users succeed in exploiting different types of vulnerabilities and the consequences can be disastrous. Most of these vulnerabilities are directly related to the web-based applications lack of quality as a result of a poorly implemented software development life cycle (SDLC). This paper will discuss the direct implication of the lack of security and the importance of quality on the SDLC, and the major factors that influence them.

Key Terms: Education, security, web communication

I. INTRODUCTION

Web application security is a branch of Information Security that deals specifically with security of websites, web applications and web services. At a high level, Web application security draws on the principles of application security, but applies them specifically to Internet and Web systems. Typically web applications are developed using programming languages such as PHP, Java EE, Java, Python, and Ruby, ASP.NET, and C #, VB.NET or Classic ASP. [1]

Web sites are unfortunately prone to security risks. And so are any networks to which web servers are connected. Setting aside risks created by employee use or misuse of network resources, your web server and the site it hosts present you’re most serious sources of security risk.[1] Web servers by design open a window between your network and the world. The care taken with server maintenance, web application updates and your web site coding will define the size of that window, Limit the kind of information that can pass through it and thus establish the degree of web security you will have. This is why that is very important subject which are not available to study in our education system losses from Phishing at $1.5 Billion in 2012." Two of the well-known phishing methods are Covert Redirect and Open Redirect. Following are the most common attacks by Hacker’s. That is found in most 70% of web application. In most government and bank sector’s official website, Due to unqualified about information security, even in top education sector official website. With the emergence of Web 2.0, increased information Sharing through social networking and increasing Business adoption of the Web as a means of doing business and delivering services, websites are often attacked directly. Hackers either seek to compromise the corporate network or the end-users accessing the website by subjecting them to drive-by downloading.[2]. As a result, the industry is paying increased attention to the security of the web applications themselves in addition to the security of the underlying computer network and operating systems. The majority of web application attacks occur through cross-site scripting (XSS) and SQL injection attacks which typically result from flawed coding, and fails to sanitize input to and output from the web application. These are ranked in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors. Phishing is another common threat to the Web application. "SA, the Security Division of EMC, today announced the findings of its January).[2, 3]

II. METHODOLOGY

2.1 THE MOST COMMON SECURITY VULNERABILITIES

There are some rule which is follow for common security vulnerabilities:

a. Injection flaws, such as SQL, OS, and LDAP injection occur when un-trusted data is sent to an interpreter as part of a command or query. The attacker’s hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization [3].

b. Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users’ identities.[3]

c. XSS flaws occur whenever an application takes un-trusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim’s browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

2.2 WEB OR SOFTWARE ENGINEER’S

Web Engineering is the application of systematic, disciplined and quantifiable approaches to development, operation, and maintenance of Web-based applications. It is both a pro-active
approach and a growing collection of theoretical and empirical research in Web application development. Note that there’s no any statement in above definition about their Security that how to do secure coding. And setup filtering, blocking user bad input SQL injection LFI RFI code blocker filter etc.. However the most faces should be on security level to improve our source code, but un formatly there is nothing to study for information security as a course just like we are studying other courses.[4]

2.3 IMPOTENT-I

Our education system is based on a simple outline of an old science, there is no any upgrade for the developer’s of the software engineer and web engineer’s, currently we are studying the same thing in the modern way of education 2015. However, few of subject are changed but according to software engineers those are not necessary for developer’s, just like MKT201 MKT202 those are A course which are now included in the CS student as well, but yet no any information security subject are added which are necessary for a developer. To do secure coding awareness of security flow’s block the user bad inputs, even we just study the simple outline of the whole degree program but nothing to learn about web security.[4]

2.4 INDUSTRIAL IMPACT

As we joined any industry for developing our career in software engineering or web engineering we faced a lot of issues during the interview as well as during development. We study the whole subject of development, but we are not studying any particular subject to security issue during development.

2.5 IMPOTENT-II

As we have successfully developed any web application for an international company with very high cost as their demand, and after a few month that website got hacked and they're all important databases had been dumped on public place just like Facebook Yahoo, Google or got any misuse, so after that we can just imagine that’s how it affect our company career as well as our growing career in development, the company never waits to kick out that employ to whom that task was given.[5]

2.6 ANOTHER BAD EFFECT

That employ will join those institutions which are providing the core subject of Security step by step. So now this is a bit difficult to concentrate on all those subjects of “Security improvement” however, we need to focus on our daily life as well as our growing life in the market, so we cannot concentrate on both at this time. Therefore, we are unable to do that because of our old education system, if we study it during the bachelor of computer science or software engineering then we never fail to face those situations in our career as the most developers are facing. At the end, I will attach a few subjects, of course outline like web engineering-I web engineering-II of the most top ranked universities, even their own official website are vulnerable for the most top vulnerability attack. Our education system must have to follow the international standard, however, we have a master of researcher in Pakistan and we can Design these courses on our own basis and our younger generation can survive into their career as a securities programmer that no one can beat their source code without admitting of any external security courses at different institute as well as wasting their money etc [5].

2.7 Institute of Security Specialist

To join an institution to improve your code security you need to join a few of the institute who provide standard education in this specific topic of web engineering. According to my analysis of this research and knowledge, there are few of, who provide standard cyber security courses including web engineering disadvantage is their cost are high its bit of difficult to buy those courses or admit yourself to certified specially for the middle class of student who cannot afford more than their university fee, all those are provide international certification.[5, 6]

2.8 LEARN SECURITY

Based in Pisa, Italy and with offices in San Jose, California and Dubai U.A.E., e-Learn Security is a trusted source of IT security skills for IT professionals and Corporations of all sizes. E-Learn Security’s mission is to advance the career of IT security professionals by providing comprehensive and practical education. E-Learn Security has proven to be a leading innovator in the field of practical security training. Best of breed virtualization technology, in-house projects such as Coliseum Web Application Security Framework and Hera Network Security Lab, have changed the way students learn and practice new skills. [6]

Figure 1: Distributed Education System in Pakistan

2.9 MILE2 INTERNATIONAL

Mile2 is a developer and provider of proprietary vendor neutral professional certifications in the cyber security industry. Mile2® administers its certification exams through the MACS (Mile2 Assessment and Certification System) system via Mile2.com. Mile2 also provides Information Assurance services that meet
military, government, private sector and institutional specifications. Mile2 certification courses teach the fundamental and advance principles of cyber security and follows a course/certification track that leads to advanced hands on skills training for penetration testing, Disaster Recovery. [6,7]

III. DESIGN OF RESEARCH
In view of these variables and hypothesis, the Research Design followed for this thesis is Qualitative Research Design. Reasons for choosing this design:
- This design helps in identifying & controlling extraneous factors also.
- This design is efficient in using available resources.

IV. TARGET POPULATION
The sample of the IT user is selected for the research, those who are working for IS and on a whole we have taken almost 20 responses from different institutions. [6]

V. DATA ANALYSIS
The purpose of the research is to analyze the error which is affecting the study of education. The researcher selected the questionnaire for collecting the responses. The average graph of respondents is showing high requirement for including those courses which are related to Information security. [7]

VI. QUESTIONNAIRE GRAPHICAL ANALYSIS

IMPACT OF RESEARCH QUESTION
a. Time saving.


c. Error Reduction.

Figure 2: Impact of Process

Graph III

Figure 3: Impact of Time

Figure 4: Impact of information security in our Education

As we know that the World Wide Web has become one of the most common communication mediums in the world. Our research areas focus the education sector of web-based application in our country. We conclude that the analysis of this research work is that, there is a lack of awareness of new technologies and include new criteria of education. Unfortunately in our country focuses the old pattern of education system which is useless for the youth generation. We should introduced modern technologies based criteria of education system and add those courses which are based of professional life and relate on their field of education. Further we focus the modern techniques of web-based application, web security and tools of its security factor. [10, 11]
IX. References

1. Part 331 of title 7 of the Code of Federal Regulations (7 CFR part 331)

2. Part 121 of title 9 of the Code of Federal Regulations (9 CFR part 121)

3. Part 73 of title 42 of the Code of Federal Regulations (42 CFR part 73)


7. Security Guidance for Select Agent or Toxin Facilities, which is available at http://www.selectagents.gov/

8. Incident Response in Select Agent or Toxin Facilities, which is available at http://www.selectagents.gov/


10- Han, Y.Y., Carcillo, J.A., Venkatraman, S.T., Clark, R.S.B., Watson, S., Nguyen, T.C., Bayir, H.


FORE – Foundation of Research and Education (2005) Report on the Use of Health Information