

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

Web Based Applications and Their Testing Approach

Gaurav Kumar Tak, Anurag Singh Tomar

Dept of Computer Science and Engineering, Lovely Professional University, Phagwara, India

ABSTRACT: Internet is perhaps the most popular medium of sharing information today and its popularity is growing day by day. People refer to it for almost all sorts of reasons, and with growing usage the concept of security risks arises. Security risks arise mainly because the internet is a two-way medium. Personal information is shared over the internet through web-based applications which we use for many useful purposes like applying for passports, online ticket booking, online testing sites, social networking sites, etc. To ensure that the web-based applications offer full productivity and good security of the users' information it is important that the development procedure of these applications be redefined keeping things like feasibility, security aspects, and problems that are likely to be faced during future maintenance in mind. We are proposing a novel and scientific technique for designing ideal web-based applications. This technique includes various testing methods like white-box testing, black-box testing, etc. to make sure that the application is working as required, and that the limits or bounds on its constituent variables and functions are not violated. It must be made sure that confidential data such as passwords are properly encrypted using latest technologies like md5, and the special users of the application like Master user/admin user are provided with secured privileges. It must also be ensured that the application is compatible on various modern browser platforms. We have tested the method and found it to be quite up to our expectations. Thus, if the proposed method is followed properly it shall not only increase the security aspect of the applications but also reduce efforts required for the maintenance of the application in future.

KEYWORDS: CAIN; LDAP; SDLC; SSL; White Box Testing

I. INTRODUCTION

Nowadays internet is the most important part of our life; it is the fast growing medium over the world. Internet can be described as a system of interconnected networks (wired / wireless) that use the standard Internet Protocol Suite (Transmission Control Protocol /IP) to serve information worldwide and its standards are used globally[1].

In Current scenario, Internet is fastest medium of communication. Internet is widely used for many purposes like E-shopping, E-banking, online ticket booking, business purposes, social networking, video-conferencing, medical services, chat services and many other applications. In this scenario, there are a lot of security attacks which are carried out over the internet to make the disturbance of human life and peace. Now this time, in most of the works, internet or usage of internet is involved [1].

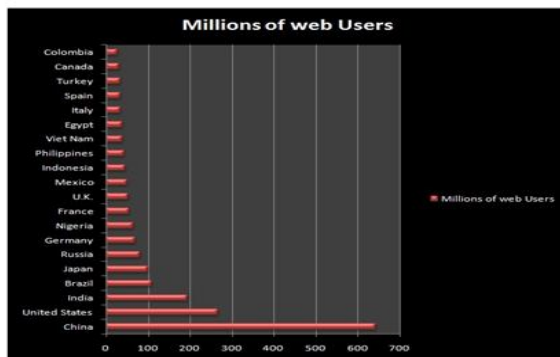


Figure 1: Top 20 Countries with Highest Number of Internet Users

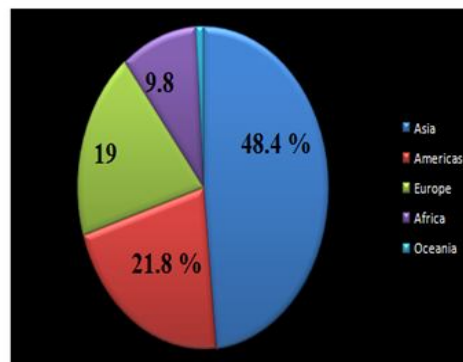


Figure 2: Percentage of World Web Users.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

In [6], the top 20 countries worldwide with the highest number of web users listed. India has 4th rank worldwide [6] which would be on 3rd rank by 2013[7].

Due to huge popularity of internet and its applications, there are a lot of security issues and attacks are available to make disturbance in the human life. Spam attacks, phishing attacks, Password cracking, hijacking (Interception of TCP-session), ip-spoofing, malware attack, SQL injection, script injection etc. are common and popular attacks over internet [2][3].

To ensure all the reliabilities, Internet follows the CAIN architecture of systems. CAIN consists four features in itself those are *Confidentiality, Authenticity, Integrity, and Non-Repudiation* [4].

Nowadays web applications are fixing their legs in each place due to some features like user friendliness, easily accessibility, easily availability. In offices, web applications are used to perform official tasks (to generate some reports monthly basis/weekly/yearly, track each office activity). Web and web applications are playing a good role in our life because they are available on 24x7 bases. There are various web technologies are in the development such type of applications. Popular technologies like PHP, MYSQL, HTML, JAVASCRIPT, AJAX, CSS, HTML5, FLASH, ORACLE, ASP.net, C#, VB-Script, JSP etc. Some Technologies like PHP, MYSQL, JSP are Open Source and also support Object- Oriented programming approach. Some of the advantages of open source technologies are following [17][18][19][20][21][22]:

- ✓ Easily availability of the source code and user has the rights to modify it.
- ✓ Users have rights to redistribute modifications, customization of code and any improvements to the code.

Web based application development can be described as the implementation of applications/software that can be accessed over internet as the singular application interface, and encompasses both Business-to-Business (B2B), and Business-to-Customer (B2C) solutions. Web enabled software can be globally accessible (internet) or locally deployed (intranet). The reality is that web applications' usage has already stretched far beyond early adopters, and is moving rapidly worldwide. The usage is moving not only in the corporate sector but also in home computers [6].

Currently, Web applications are so popular but people are afraid of security risks over internet and its usage. Many times some attacker are able to capture the information of web users (Sometimes information are confidential and sometimes not). Some web attacks like SQL attacks, SQL injection, code cracking, phishing attacks, spam attacks, Nigerian scams, fraud theft, information warfare, malware attacks, virus intrusion, DOS-attacks. Phishing attackers act as passive attacker to capture some information submitted by the web users. Many times, Web applications don't have proper authentication procedure, proper database management to store the users' information, proper password storing schemes, proper coding etc [2][3][4][8]. Now this stage, security of web users of a specific country also reflects the technical growth of the country, technical educational level of population, awareness of the peoples towards various web attacks, service sectors growth etc. Currently in news paper and media, hacking of banking accounts, E-commerce site cracking, SQL cracking, Phishing sites (like 19 people arrested in UK for hacking thousands of bank accounts, FBI Arrests at Least 10 in Global Bank Hacking Scheme, Computer hacking gang arrested etc.) of many social networking sites are very common news[9][10][11].

Development of web applications also follows software engineering steps. Software engineering focuses on the less time-efforts, high quality and minimum cost in designing an application. Mainly software development life cycle (SDLC) consist 5 steps which are as follows requirement gathering, designing, coding, testing, and maintenance. Various models like waterfall model, prototyping model, spiral model, RAD model, incremental model etc. have been already proposed for the SDLC [23]. But these models are proposed so earlier not suitable for this growing software and web environment.

As we all know that 60 % efforts are consumed in the maintenance step of SDLC. It can be reduced after following proper requirement gathering, better communication between clients and develop, proper testing methods etc. Reducing the maintenance work can be beneficial for project completion on time, better feedback from client side after the delivery, managing good relations between client and company.

Due to higher popularity and growing the usage of web applications, we need to propose some new methods for the better development of web applications, for the efficient testing of web applications. Here we are proposing a good and complex approach towards testing of web application which involves all security checks, analysis of various attacks.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

II. RELATED WORK

Many Articles and research has been published related to software engineering and testing approach of software engineering. But only few testing approaches are available for the testing of web applications. As the growing internet and web applications, we have to find some good approach to protect all the information, data, files, documents etc. over web.

James A. Whittaker et al. presented a testing scheme for the software engineering which is based on statistical analysis in intended environment. This testing certification consists 2 Markov chains. In first chain, computations allow for through analysis of expected usage patterns. A second Markov chain is based on the result of applied test cases. Their methodology provides a better reliability during testing analysis [12]. Andy Ju An Wang presented a security testing techniques for the software engineering course. In the paper, a lot of software security testing tools (like MOPS, ESC/JAVA, Splint, Flaw Finder, RATS) had been described. It properly describes the importance of security testing with addition of functional testing [13]. In [15], Dimitrios S. Kolovos et al. proposed a unit testing model. They described various steps Common Sources of Problems, Model-to-Model Transformation, Model Validation, Model-to-Text Transformation, Model Comparison, and Model Merging for the complete unit model based testing [15]. Many time developer use frameworks for the designing of new applications/ softwares. In those cases, they need some formal testing methods for the code specifications, grey box behavior etc. Benjamin Tyler and Neelam Soundarajan presented a black box testing approach towards grey box behavior of the applications which is based on object-oriented frameworks [24]. Pieter Koopman et al. described about the testing and validating techniques for the measurement of quality of specifications. The techniques perform the analysis using domain specifications and state specifications. But the methodology not solves all issues of system [14]. Various papers also described some approaches for the authentication security, data security, balancing usability and security requirements of text password, encryption schemes for the user data etc.

Currently phishing attacks, spam attacks, hijacking also popular web attacks, many times they happen due to little awareness of users towards internet, and internet security. Dhananjay Kulkarni also described a novel web based approach for the protection of test passwords.. He presented a new scheme for the password management which helps balance a strong and supports all security aspects of the passwords [7]. In [5], Gaurav Kumar Tak (2009) et al. also proposed a new scheme for the password protection and secure authentication of genuine users. They described 3-way Handshake approach which provides a more secure platform to the end users for their online transactions. In this methodology, attackers can't attack on the email and SMS simultaneously. Information stealing will be minimized and more secure communication (transmission) will occur using the proposed methodology. If any intruder wants to peek into the transmission of the confidential data, he will not be able to recognize the patterns of encrypted data [5].

Inspection Effectiveness in Software Development:

Tzvi Raz and Alan T. Young described the Inspection analysis which involves all steps of a software inspection like conducting meeting, proper documentations, design change requests(DMC), feedback, review etc. It measures all identifiers for finding the inspection effectiveness using the neural network approach[16].

III. PROPOSED METHODOLOGY

Before proposing a new methodology for testing techniques for web applications, we have to consider all the facts of software engineering and all the testing strategies of software. New proposed testing methodology can be helpful to improve time complexity, efficiency, improve security etc. Here we propose a new compound chain model methodology for the above that is based on the same chain can be executed parallel.

Our system uses some previously proposed software engineering techniques for the testing. The new methodology is responsible for the error in flow of data, data loss, data stealing, testing of authentication schemes of users, privilege distribution etc. It also provides the better storage scheme of data.

Many times, Web applications have some security loop holes after its final execution so this testing strategy is very efficient way to test all security aspects of web application before its final delivery to the customer.

Proposed testing approach for web applications, follow the few steps which are as follows:

- A. *Database Configuration Security:* As the Testing purpose, in this step, we need to test all configuration setting of database and their security. Database security also depends upon the strength username and password. For the better configuration security, passwords should contain some alphabets, some digits, and some special characters in it. Long and strong password are difficult to remember but more secure (security is the main

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

issue with the web applications or over the internet). Currently there are many password cracking tools(some are available with backtrack OS) available, which can easily guess a majority of weak passwords. Strong password is the first step to give a better security to the web applications. In testing phase, we have to look all the issues of configuration manager then give the better solutions for the security.

Database configuration security is the most common issue this stage, because database contains much sensitive information itself. A loop hole in database security can be cause of misuse of data, loss of data, stealing of data, and distribution of private data.

In privileges level security, tester should be carrying all the tests regarding unauthorized access of confidential data of a web application, proper classification of tasks/access of the web application etc. Most experienced attackers first collect all the information of victim database server, web server configuration, their loop wholes etc. The common ways to find the information are the search engines, port scanning, SQL ping etc.

- B. *Privileges Level Security:* For the privileges level security, we need a proper testing to provide more security towards web applications. Before execute the testing phase, first it has been decided that how many types of users/privileges needed in the web applications. In testing phase, it is clearly tested that all the privileges and their security should be preserved in the web applications and their usage, authorities are properly managed.

In the CAIN properties of a system also describes some privileges security of applications but sometimes CAIN is also unable to test all the security issues which are related to Privileges level [4]. Using the Privileges features all the DML, DDL, storage statements can be controlled for the different users.

- C. *User Validation Security:* For the Testing purpose, user validation process is also described in CAIN section of system. In the testing, need to test all the pages or features of web applications. Before testing, need to perform the analysis of SRS (system requirements module) for the study of user level authorities, their access features, and their limitations. Many times features of web applications are classified according to the user level. Many features /pages are accessible for the admin or master users but not for the common users or data entry users.

Validation process is incurred using username and password scheme. Most of the times, passwords are stored in encrypted form, so that database administrator are not able to read the password field of any users. This policy provides a better security to the users. Username and password authentication is executed using some hashing function or any other better cryptographic techniques.

For example, Ldap Tree Directory is also used to store some information of users like username, name, alias and password etc. In the Ldap tree structure password is also stored in encrypted form so ldap admin can't access/read the user password.

This user validation security plays an important role in testing phases of web applications. Because in the web application user validation should be properly managed because data access level also depend on the user type, their privileges etc[25].

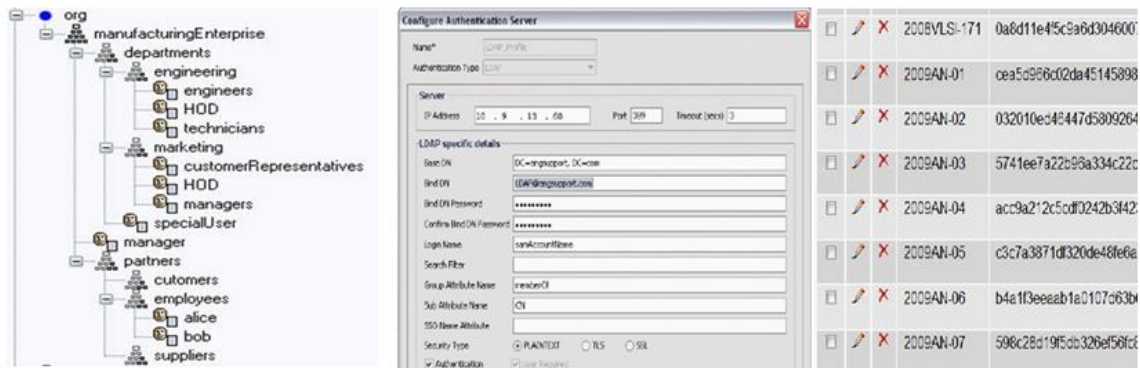


Figure 3.4.5 : LDAP tree structure, LDAP configuration server and MD5 Storage of Password.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

In the above figure 6 ,2nd column of the database table 'login' represents the password field with the md5 storage,md5 storage of password provide the view security of password or other confidential information from the database administrator.

Password and encryption security plays a tremendous role in many web applications likes online ticket booking, online payment gateways, Online shopping mart which is also described in CAIN properties.

- D. *Code Testing*: In the proposed testing methodology of web applications, coding testing involves all the process testing, syntax testing, logical testing, include file testing, package existence and their testing, functional testing.

In the proposed approach, all the testing steps must be executed using the predefined methods of code testing. White Box testing also helpful to test the web application at coding level. This type of testing needs involvement of technical and programming expert, to find the coding error and for debugging them.

There are a lot of approaches have been described for the code or logical testing of an application, white box testing also describes the same which is full internal structure oriented.

Code- testing is critical stage of software development, because many times logical errors generate some unpredictable result, data loss, wrong conversion of data.

Coding Testing can be also defined as the process of executing a program with the intent of finding a logical error. A good code testing case is one that has a high probability of finding an as-yet-undiscovered error.

There are a lot of other testing approaches (path testing, program flow graphs etc.) also proposed for the code testing to ensure coding quality of the system or web application. Any methodology can be adopted based on the requirement analysis of the web application.

- E. *Data type validation and Input fields validation*: Data type and input fields validation are also the essential requirements of any web based system. Both provide great security against web attacks and other security attacks. Proper Data type also save memory storage and manage the stored data in efficient way. Proper data type selection is also one of testing steps to evaluate the working of any system. There are a lot of data types in database storage; each defines its use and storage capacity.

In most of the web applications, attacks happens using some input fields for some SQL injections, attacks' strings, some attack commands, finding vulnerabilities. Input type of fields decides the input values validation from the users. There are a lot of input types which are used in the web application according to the requirements. Like TEXT input type is used to take input of text, PASSWORD input type is used to take password input.

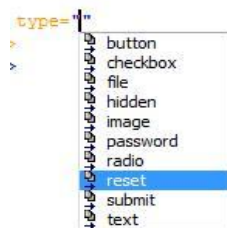


Figure 8: Input Type Selection for input fields.

Each input type has its specific use. Figure 10 represents some of input types which are commonly used in various web applications with html tags.

Proper Input field selection easily prevents the DOS (Denial of Service) Attacks and Brute force method of password cracking. It easily manages the some security of web applications.

- F. *Query level Security and Web Attack Security*: It is the most important step of testing because it provides an additional layer of security testing against several web attacks.

Integrity, availability, confidentiality and non-repudiation are the four salient features of secure system [13]. A vast number of web applications, especially those used by enterprises to e-commerce purposes must fulfill these four requirements to provide the better support. Such web applications are implemented using dynamic scripting languages such as JSP (Java Servlet Pages) or PHP or ASP.net coupled with HTML which facilitates establishing connection to data storage, fetching data and displaying them on web pages based on the executed query and requirements.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

Query is the way to retrieve some information from the database. Many web attacks happens at query level. Mainly there are 4 types of web attacks which are Cross Side Scripting attacks, SQL Injection attacks, Remote Command Execution, Path Traversal. These attacks can be categorized into three categories :1) attacks of Runtime HTTP Requests ,2)Attacks of Design-time web Application Source Code,3) Attacks of Runtime Dynamically Generated SQL Statements.

In the testing, we have to test all the cases of attacks using some historical analysis of attacks and artificial techniques to secure the web applications. In testing phase, proper testing should be carried out for Cross Side Scripting attacks, SQL Injection attacks. SQL Injection attacks can be happened like the following queries.

```
$sqlstring= "Select *from login where userid= '$username' or 'a'= 'a' and password = " ";
```

```
$sqlexecution=mysql_query($sqlstring) or die("Query execution failed");
```

- G. **Browser and Interface testing:** This testing step is based on the outer view of the web applications. Currently, there are a lot of browsers are present and each browser has its own unique features. But there are a few browsers which are so popular, during this step the web applications should be tested in all popular browsers like Firefox, Internet Explorer, Google Chrome, Opera, and Netscape Navigator etc. A perfect web application should be independent of browsers.

The View and functionality would be same in all browsers (like Mozilla firefox, internet explorer, Opera etc.).Presently, there are a lot of softwares available which can easily validate HTML tags, CSS-design view, JAVA Script syntax etc.

Web developers and tester can easily execute this type of testing using Firefox Add-on Web Developer 1.1.8.This Add-on provide all the information of html forms, CSS design. It also validates all html tags, feed, links, css-design etc.

Figure 11 represents all the functions of the form tools of above firefox add-ons.

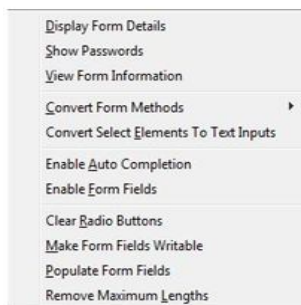


Figure 9: HTML form information using the Firefox add-on Web Developer 1.1.8.

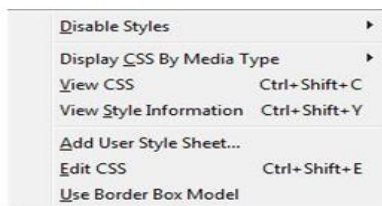


Figure 10: CSS-editor functions using the Firefox add-on Web Developer 1.1.8.

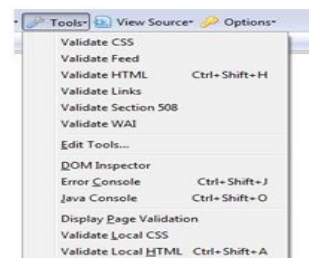


Figure 11: Multiple Validator of Firefox add-on Web Developer 1.1.8.

CSS-design editor is used for the interface and design testing in the above step. Using Firefox CSS-editor add-on, design view easily customized.

Figure 10 represents CSS-editor of the firefox add-on.

During this testing step, validators are also used to validate and test the html tags, feed, form tags, Java Script syntax, links with proper design and functionality.

IV. IMPLEMENTATION AND RESULTS

To implement and execute all testing steps of proposed methodology, Layer architecture would be followed. All the testing steps should be execute before the integration and installation step of Software Development Life Cycle(SDLC).After the installation and integration, testing is a complex task which consume more efforts, manpower, resources etc. This approach also reduces the maintenance work of developer team of the web application.

Figure 12 represents the layered architecture of proposed methodology. This web applications' testing approach decreases the time complexity of testing step of SDLC. It also improves the performance of web applications and gives

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

the better results. After executing the testing with the help of all layers which are shown in below figure, application is integrated with all the modules. Integration always creates some kind of errors or bugs in the web application which can be due to design view, images folder, supporting javascript files.

Web application needs some maintenance to fulfill all the requirements of the users. After completion of all steps, we application can be launched as final versions for users.

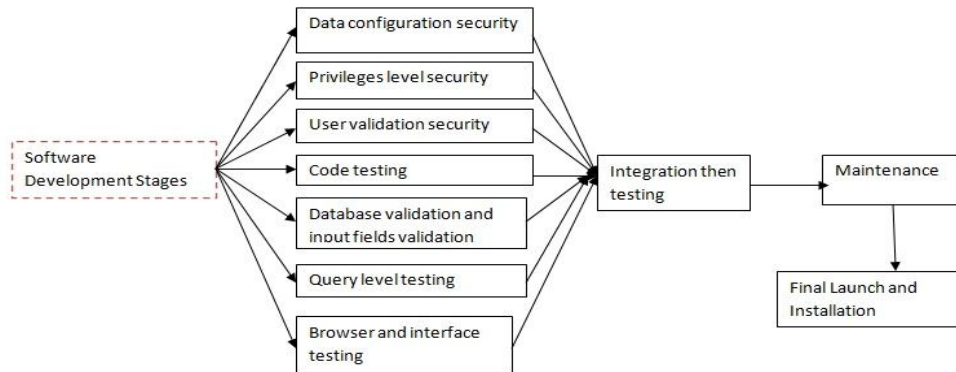


Figure 12: Layered Architecture of Proposed Approach.

We have already executed the above steps on 2 web applications: 1) *Online Testing Arcade* (implemented in Career Launcher Gwalior, Madhya Pradesh, India.) and 2) *Academic Registration Portal* (implemented in Indian institute of Information Technology and management Gwalior, Madhya Pradesh, India.).

On both web applications, the proposed methodology has been provided better performance, better functionalities and also an additional layer of web security. The proposed approach also prevents the cyber attacks and cyber crimes.

Description of tested web applications is as follows

67 % efforts are not optimize solution of the SDLC. Using the proposed methodology, we are reducing the maintenance efforts and optimizing all the resources (time, man, and machine) which are used in SDLC.

Online Testing Arcade: Online Testing Arcade is web based application which is used to conduct online tests and provide results according to the students' performance over internet or intranet.

Using proposed methodology for the above system, we executed all following steps when we are at the delivery stage of the system.

- A. *Database configuration security and Privileges level security:* The system is validated using the database configuration settings over the database –server, web configuration setting to provide access through network. We have created some database users based on their privileges which were specified in the SRS of the system. We have tested and made proper configuration using phpmyadmin interface which provide several configuration setting features like *MySQL* connection collation, *MySQL* runtime information, Storage Engines, Privileges etc. We have created and tested for each database user for system with the different *MySQL* privilege.
- B. *User validation security:* We executed each operations, functions, pages and access features for the different type of users to gain the Confidentiality and authority properties of the above web application. Access and User levels are specified in the SRS of the system clearly. There are many user levels (Master. Admin, Data Entry, Student) provided according to their accessibility. Each User Level (except Master User) has some limitation over the above system.
All user validations have been tested using the login module of the application. Password and other private information (like contact no, email id) also been stored in the encrypted form to maintain all the security measures.
- C. *Code testing:* We had applied some coding testing strategies to validate the function result and output display. We have used white and black box testing for the same .Testing has been performed for all the



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

test cases. Code testing was essential to validate the calculation of obtained score, percentage of marks, accuracy in the test paper, some results of score cards display, searching result, query result etc. Code testing also verified all formulas, mathematical equations, and mathematical operations for the above system.

URL (Uniform Resource Locator) Validation are also tested during this step itself, It has been tested in URL validation that the pages are connect with the valid URL or not.

- D.** *Data type validation and Input fields validation:* The above system has many different modules for the different purposes. For the data base tables, all data columns have been tested properly for column length or size, column data type, column attributes etc. All testing operations have also been performed for other modules like registration, score, user details etc. In data type testing, it has also been tested that all the confidential information like password and others are stored in encrypted form to maintain all the security measures. Input fields have also been properly tested for different type of inputs.

There are several types of forms are available in the different web applications, all forms and their input fields should be tested properly before the integration of modules.

- E.** *Query level testing and Web attacks testing:* The above system is designed for online test execution for various students, so it should be properly tested before installation. Display results of all the query and their retrieved data are properly tested for the above system. All the warning message and error message of SQL queries are properly tested in the above system.

All the SQL queries are tested which are present in the above system. Mainly Select, Insert, Update, and Delete query are used so frequently in the code of system.

Web attacks are happened using some SQL injection and some code injection, some script injection etc. Using some popular attacks formats and attacks input set, the system is protected from various web attacks.

- F.** *Browser and Interface testing:* An ideal web application always runs and works properly in each browser and environment. Its interface is always remains same in all browsers. These all features and tested during the browser and interface testing, but it's really difficult or just impossible to design a ideal web application. The above system has been tested and designed as such that it can be executed in most popular browsers (like Mozilla Firefox, Internet Explorer, Google Chrome). Its interface and working are compatible with the mentioned browsers.

V. CONCLUSION AND FUTURE WORK

Using the proposed methodology, an additional layer of security can be provided to the web applications. This makes them significantly less vulnerable to cyber-attacks and other such security risks. In the testing phases of the given methodology, many security issues can be easily detected and resolved. This approach is highly beneficial in creating almost bug-free applications. In the given steps all the issues of database configuration settings, privileges' setting, and users' level settings, web security, SQL injections have been covered; making the resultant application designed using this scheme immune to many kinds of security attacks. It also makes the application stronger and smarter so that it doesn't go over its own technical limitations and thus prevents database crashes due to overloading of variables, or data type-mismatch. The proposed steps can provide support to decrease the maintenance efforts and resource utilizations. It makes the software more future-proof so that modifying it doesn't become a cumbersome procedure at some later development stage in future. It provides for better customer satisfaction after the launching of web applications. All the steps are well defined and properly structured. Thus, the approach is perfect for designing some of the smartest web applications.

REFERENCES

1. T.Grandison;M.Sloman, 'A survey of trust in internet applications', Communications Surveys & Tutorials, IEEE, vol.3, no.4, pp.2-16, Fourth Quarter 2000.
2. W. Halfond and A. Orso, 'AMNESIA: Analysis and Monitoring for Neutralizing SQL Injection Attacks', 20th IEEE/ACM international Conference on Automated Software Engineering, pp. 174-183, 2005.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

3. Gaurav kumar tak, gaurav ojha 'Enhanced Query based Layered Approach Towards Detection and Prevention of Web Attacks', in Procedia Technology, Vol 4, pp. 500-505, 2012.
4. G.K. Tak, N. Badge, P. Manwatkar, A. Ranganathan, S. Tapaswi, 'Asynchronous Anti Phishing Image Captcha Approach towards Phishing', 2nd International Conference on Future Computer and communication, Vol 3, pp. 694-698, 2010.
5. Gaurav Kumar Tak, Ashok Ranganathan and Pankaj Srivastava '3-Way Handshake Approach towards Secure Authentication Schemes' Journal of computing, Vol. 2, 2010.
6. <http://royal.pingdom.com/2010/07/27/top-20-countries-on-the-internet/>
7. <http://www.internetlivestats.com/internet-users/>
8. Dhananjay Kulkarni "A Novel Web-based Approach for Balancing Usability and Security Requirements of Text Passwords", International Journal of Network Security & Its Applications, Vol. 2 Issue 3, p 1-16. , 2010.
9. <http://www.dailymail.co.uk/news/article-1316022/Nineteen-arrested-online-bank-raid-netted-20m.html>
10. <http://articles.latimes.com/2010/sep/30/business/la-fiw-cyber-scam-20100930>.
11. <http://www.telegraph.co.uk/news/uknews/crime/10322536/Barclays-hacking-attack-gang-stole-1.3-million-police-say.html>
12. James A. Whittaker and Michael G. Thomason 'A Markov Chain Model for Statistical Software Testing', IEEE Transactions on software engineering VOL. 20, NO 10. , pp 812-824,1994.
13. A.J.A Wang, 'Security testing in software engineering courses' Frontiers in Education, VOL 2, 2004.
14. Pieter Koopman, Peter Achten, and Rinus Plasmeijer,'Testing and Validating the Quality of Specifications', In Proceedings of IEEE International Conference on Software Testing Verification and Validation Workshop ,pp 41-52, 2008.
15. García-Domínguez, D.S. Kolovos, L.M. Rose, R.F.Paige, I. Medina-Bulo, 'EUnit: A Unit Testing Framework for Model Management Tasks' Model Driven Engineering Languages and Systems LNCS, Volume 6981, pp 395-409, 2011.
16. Tzvi Raz and Alan T. Young 'Factors affecting design inspection effectiveness in software development', Information and Software Technology, Vol. 39, issue 4, pp 297-305, 1997.
17. <http://www.php.net/manual/en/tutorial.php>.
18. <http://www.tutorialspoint.com/mysql/>
19. <http://html.net/tutorials/html/>
20. <http://www.tutorialspoint.com/ajax/>
21. <http://asp.net-tutorials.com/>.
22. <http://www.javatpoint.com/jsp-tutorial>.
23. A.M. Davis, E.H. Bersoff, E.R. Comer , 'A strategy for comparing alternative software development life cycle models', Software Engineering, IEEE Transactions on , vol.14, no.10, pp.1453,1461, Oct. 1988,doi: 10.1109/32.6190
24. Benjamin Tyler, Neelam Soundarajan,'Black Box Testing of Grey-Box Behavior', FATES 2003,LNCS 2931,pp 1-14, Springer Berlin Heidelberg, 2004.
25. <http://www.ibm.com/developerworks/cn/java/j-acegi2/>