 ISBN: 978-81-927230-0-6

# "Challenges & Problems in Security Testing of Web based Applications: A study of software companies in Pune city"

*Dayanand Patil*
*Research Scholar*
*M.Phil, Shivaji University Kolhapur*

***Abstract - Security testing for web-based applications is different from functional testing and usability testing in a number of ways. This fact should impact how we test web applications for security. In order to devise an effective methodology for Web Application Security Testing, we must first understand its unique challenges and problems .Therefore in this paper researcher has decided to attempt "Challenges & Problems in Security Testing of Web based Applications: A study of software companies in Pune City:.Researcher hopes that this information will serve as useful input for developers, security testing team and test managers while developing and testing the project.***

## *I. INTRODUCTION*

As more and more vital data is stored in web applications and the number of transactions on the web increases, proper security testing of web applications is becoming very important. Security testing is the process that determines that **confidential data stays confidential** (i.e. it is not exposed to individuals/ entities for which it is not meant) and users can perform only those tasks that they are authorized to perform (e.g. a user should not be able to deny the functionality of the web site to other users, a user should not be able to change the functionality of the web application in an unintended way etc.).

Now days, organizations engaged in software development have been increasing attention to application security issues during the SDLC. Several initiatives propose a secure development methodology that is baked into the software development process itself. For example, The Open Web Application Security Project ("OWASP"), a non-profit organization, regularly maintains a list of "Top 10 Web Application Security vulnerabilities" on its websites that developers can attempt to guard against another example is Microsoft now requires that its development teams include "Security Threat Model Analysis" in the design and coding phase. Organizations have become sensitized to the need for a dedicated effort designed to test web applications specifically for security issues. These are very positive developments In this paper, researcher identify the unique challenges and problems of Web Application Security Testing, and suggest some suggestions that may be beneficial for security testing teams as well as for developers developing tools for Web Application Security Testing.

## *II. OBJECTIVES OF STUDY:*

1. To study different challenges & problems faced by selected companies in security testing of web based applications.
2. To identify the different factors that software companies may need to consider while security testing of web application.

## *III. SCOPE OF THE STUDY*

**Geographic Scope:** The Geographic scope of the present study is confined to the boundaries of Pune City. The Topical scope focuses on study of challenges & problem in testing of web based applications with special reference to Pune city
**Analytical Scope:** The Analytical scope covers fulfilling the objectives set out of the study.

## IV. *SIGNIFICANCE OF STUDY*

The wide diffusion of Internet has produced a significant growth of the demand of Web based applications with more and more strict requirements of reliability, stability, inter-operability and security. Due to market pressure and very short time, the security aspect of Web-based applications is often neglected by developers while coding the web application, as it is considered too time-consuming and lacking a significant payoff. This depreciable habit affects negatively the security of the applications and, therefore triggers the need for adequate, efficient and cost effective security testing approaches for verifying and validating them. So it is important to study what are the different challenges & problems to test web applications security & to find out some important factors which may be useful input for developers, security testing team and test managers while developing and testing the project.

## *V. RESEARCH METHODOLOGY*

For the present study the data will be collected by using the primary & secondary methods.

**Primary Data**

The primary data is collected with the help of extensive questionnaire & interview techniques.

**Secondary data**

The secondary data is collected by using published & unpublished information like books, journals, magazines etc.

**Sampling Design**

For the present study the data will be collected by using the primary & secondary methods. The primary data is collected with the help of extensive questionnaire & interview techniques. The secondary data is collected by using published & unpublished information like books, journals, magazines etc.

The relevant data for the study will be collected from both the primary & secondary sources. The primary data will be collected through field survey by using structured questionnaire, personal interviews, discussions & mails. The required sample is collected by using ***simple random sampling & Cluster sampling techniques***.

***Simple random sampling***: A randomly selected sample from a larger sample or population given all individuals in the sample an equal chance to be choosen.

***Cluster sampling:*** With cluster sampling the researcher divides the population into separate groups called clusters. Then simple random sample is selected from the population.

For the present study total population is 265 .Out of that 75 companies are doing web development & web testing. Out of 75 web development & web testing companies Researcher have selected 50 companies for the present study. So, the ***sample size is 50*** software companies from Pune city.

## VI. *HYPOTHESIS*

1. Test Coverage of the web application is dependent upon Security aspects of web application
2. Organizations are not having sufficient awareness of web site security testing.

## *VII. ANALYSIS (IMPIRICAL STUDY*

**Table No 7.1**

Table showing Challenges of Security Testing of Web Application

| *Sr. No.* | *Challenges of Security testing* | *Rating* | | | | | *Mean Score* |
|---|---|---|---|---|---|---|---|
| | | *1* | *2* | *3* | *4* | *5* | |
| 1. | Difficulty in Automation security testing | 0 | 2 | 11 | 16 | 21 | 4.1 |
| | | 0% | 4% | 22% | 32% | 42% | |
| 2. | Difficulty in finding skilled testers with the right competencies | 0 | 2 | 22 | 15 | 11 | 3.4 |
| | | 0% | 4% | 44% | 30% | 22% | |
| 3. | Reflected cross site scripting vulnerabilities | 0 | 3 | 10 | 31 | 6 | 3.8 |
| | | 0% | 6% | 20% | 62% | 12% | |
| 4. | Most vulnerability is high-priority | 0 | 4 | 23 | 8 | 15 | 3.4 |
| | | 0% | 8% | 46% | 16% | 30% | |
| 5. | Browser level security, the browsers have vulnerabilities, & need to be all the times | 1 | 6 | 9 | 26 | 8 | 3.6 |
| | | 2% | 12% | 18% | 52% | 16% | |

Source: Survey Data So, it is concluded that, in case of Security Testing Challenges, Majority of 44% Software Companies are facing Difficulty in finding skilled testers with the right competencies as average critical challenge as mean score is 3.4 & 46.00% Software Companies are facing as Most vulnerability is high-priority as average critical Challenge as mean score is 3.4, Where as other Challenges shown in table No 8.1 are highest critical Challenges faced by Software Companies.

**Graph No 7.1**

Graph Showing Challenges of Security Testing of Web Application.(critical level 1-Lowest & 5-highest)

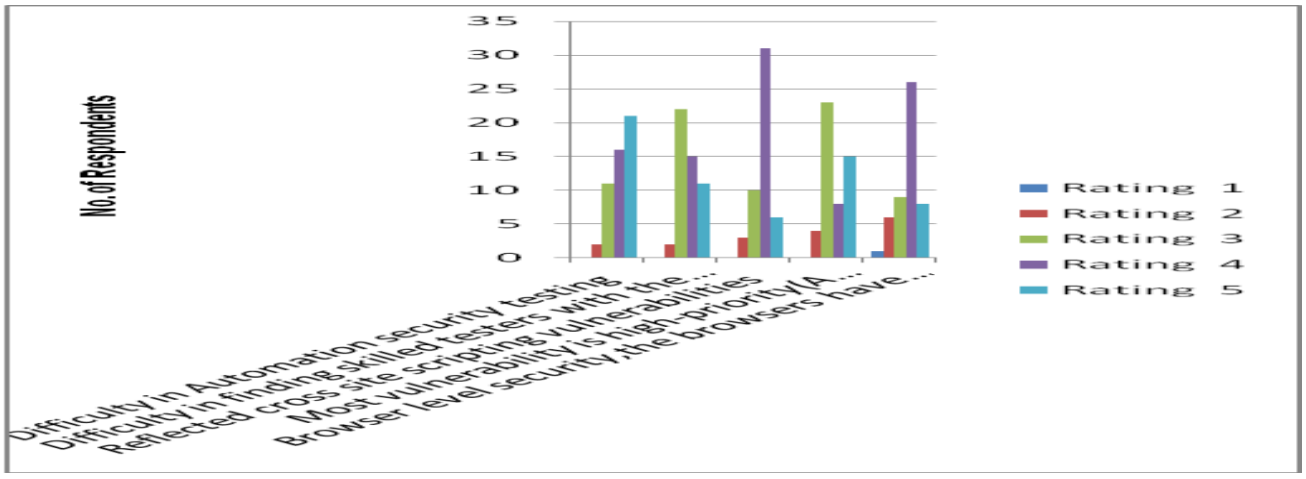


**Table No.7.2**
Table showing Problems of Security Testing of Web Application

| Sr. No. | Problems of Security Testing | Rating | | | | | Mean Score |
|---|---|---|---|---|---|---|---|
| | | *1* | *2* | *3* | *4* | *5* | |
| 1. | Choosing the right tool for Web application Security testing | 0 | 7 | 12 | 27 | 4 | 3.5 |
| | | 0% | 14% | 24% | 54% | 8% | |
| 2. | Design-level vulnerabilities | 0 | 3 | 12 | 10 | 25 | 4.1 |
| | | 0% | 6% | 24% | 20% | 50% | |
| 3. | SQL Injection | 1 | 5 | 15 | 12 | 17 | 3.7 |
| | | 2% | 10% | 30% | 24% | 34% | |
| 4. | Shell Injection | 2 | 8 | 13 | 18 | 9 | 3.6 |
| | | 4% | 16% | 26% | 36% | 18% | |
| 5. | Phishing | 2 | 3 | 6 | 14 | 25 | 4.1 |
| | | 4% | 6% | 12% | 28% | 50% | |

Source: Survey Data So, It is concluded that, in case of security testing problems, Majority of Software Companies are facing the problems shown in table No.8.2 as highest critical problems as mean score of all problems belongs to 4. Whereas very few software companies are facing these problems as least critical.

**Graph No.7.2**
Graph showing Problems of Security testing of Web Application. (critical level 1-Lowest & 5-highest)

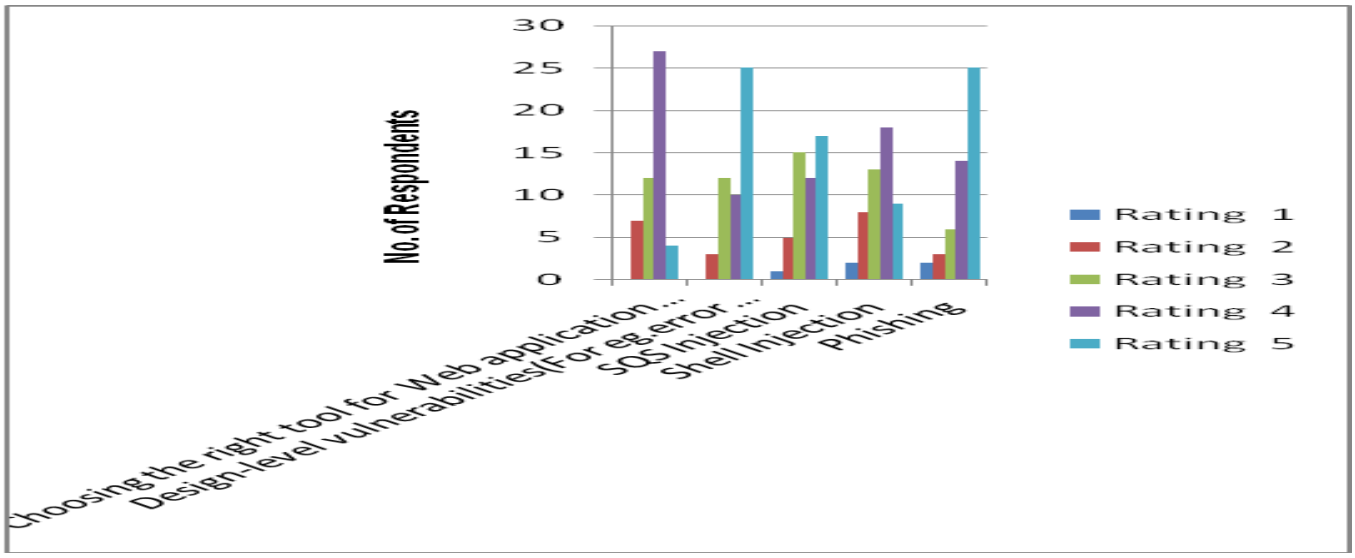



**Table No. 7.3**
Table showing Other Challenges of Security Testing of Web Application

| *Sr. No.* | *Challenges of Security Testing* | *Rating* | | | | | *Total Respondent* | *Percentage (%)* |
|---|---|---|---|---|---|---|---|---|
| | | **1** | **2** | **3** | **4** | **5** | | |
| 1. | XSS (Cross Site Scripting) | | | | 1 | | 1 | 2 |
| 2. | Meet regulatory compliance | | | | | 1 | 1 | 2 |
| 3. | To stop network monitoring hackers | | | | 1 | | 1 | 2 |
| 4. | Data encryption algorithm | | | 1 | | | 1 | 2 |
| 5. | Skilled labor | | | | 1 | | 1 | 2 |
| 6. | Third party component | | | | 1 | | 1 | 2 |
| 7. | Upgrading knowledge continuously with latest tools , security | | | | 1 | | 1 | 2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | areas of testing | | | | | | | |
| | Total | 0 | 0 | 1 | 5 | 1 | 7 | |
| | Percentage (%) | 0 | 0 | 2 | 10 | 2 | | 14 |

**Source: Survey Data**

Table No.8.3 revels that Other Challenges of Security Testing of Web Application. Only 2% respondent companies are facing each challenge shown in Table No. 7.3. So, Majority of 98% respondent companies are not facing each individual Other Security challenge shown in Table No.7.3. Total 14% respondent organizations are facing other challenges of Security Testing shown in Table No.7.3. So, it is concluded that majority of 86% Respondent organization are not facing other challenges of Security Testing shown in Table No.7.3 whereas total 14% respondent organizations are facing other Challenges of Security Testing shown in Table No.7.3.

**Graph No.7.3**

Graph showing Other Challenges of Security Testing of Web Application. (critical level 1-Lowest & 5-Highest)

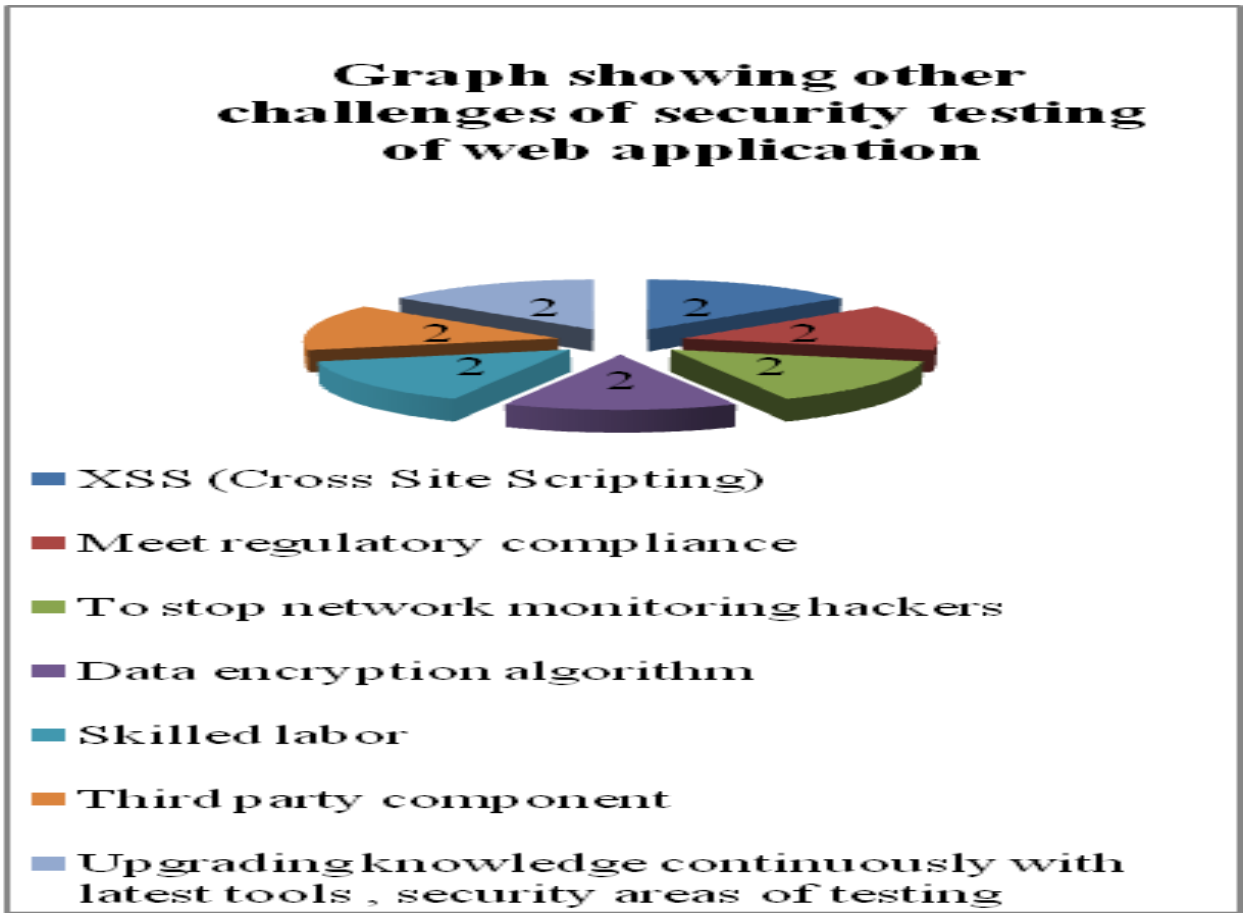


**Table No.7.4**
Table showing Other Problems of Security Testing of Web Application

| *Sr. No.* | *Problems of Security Testing* | *Rating* | | | | | *Total Respondent* | *Percentage (%)* |
|---|---|---|---|---|---|---|---|---|
| | | **1** | **2** | **3** | **4** | **5** | | |
| 1. | Proactively secure sensitive customer records | | | | | 1 | 1 | 2 |
| 2. | Over 3000 legacy and new applications | | | | 1 | | 1 | 2 |
| 3. | Cookies, session hijacking | | | | 1 | | 1 | 2 |
| 4. | Exhaustive testing if not done, leaves security concerns | | | | | 1 | 1 | 2 |
| 5. | Minimum agreement on security related issues – what type of security, levels to be provided. | | | 1 | | | 1 | 2 |
| | Total | 0 | 0 | 1 | 2 | 2 | 5 | |
| | Percentage | 0 | 0 | 2 | 4 | 4 | | 10 |

Source: Survey Data
Table No.7.4 revels that other Problems of Security Testing of Web Application. Only 2% respondent companies are facing each problem shown in Table No.7.4. So, Majority of 98% respondent companies are not facing each individual other Security Testing Problem shown in Table 7.4.Total 10% respondent organizations are facing other problems of security testing shown in Table No.7.4. So, it is concluded that majority of total 90% respondent organization are not facing other problems of security testing shown in Table No.7.4 where as total 10% respondent organizations are facing other problems of security testing shown in table no.7.4.

**Graph No 7.4** Graph showing Other Problems of Security Testing of Web Application (critical level 1-Lowest & 5-highest)

**Table No 7.5**
Table showing information on Test coverage of web application dependency

| *Test coverage of web application dependent on which factor* | *Number of Respondents* | *In Percentage (%)* |
|---|---|---|
| Security Aspects | 1 | 2 |
| Functionality | 11 | 22 |
| Performance | 5 | 10 |
| Usability | 1 | 2 |
| All above | 32 | 64 |
| Total | 50 | 100 |

Source: Survey Data
Table No.7.5 revels that Majority of 64% respondent's opinion are Test coverage of web application dependent on all four factors i.e. Security aspects, Functionality, Performance, Usability. Whereas only 2% respondents opinion is Test coverage of web application dependent on Usability. So, it is concluded that, Majority of 64% respondents agree with Test coverage of web application dependent on all four factors i.e. Security aspects, Functionality, Performance and Usability

**Graph No 7.5**
Graph showing information on Test coverage of web application dependency

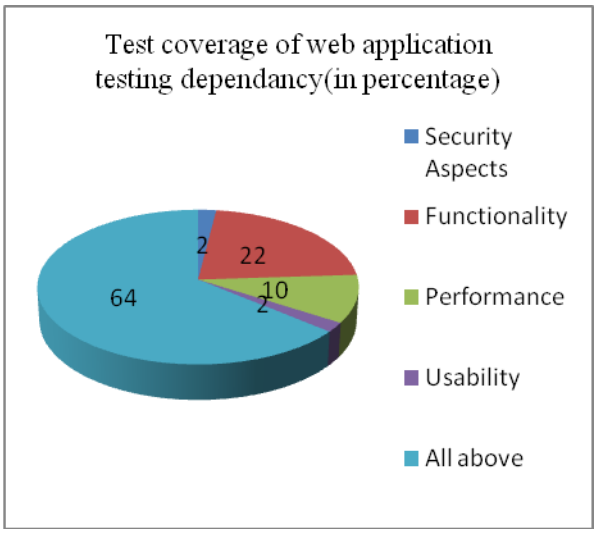
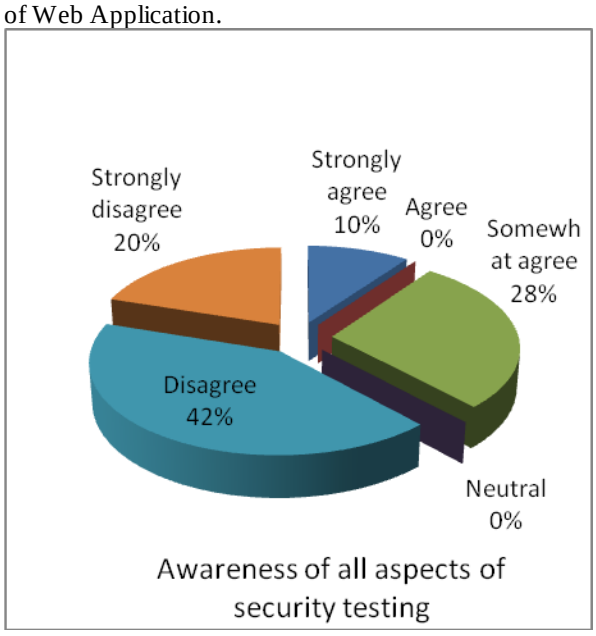



**Table No 7.6**
Table showing respondent's awareness of Security Testing of Web Application.

| *Awareness of all aspects of security testing* | *Number of Respondents* | *In Percentage (%)* |
|---|---|---|
| Strongly agree | 5 | 10 |
| Agree | 0 | 0 |
| Somewhat agree | 14 | 28 |
| Neutral | 0 | 0 |
| Disagree | 21 | 42 |
| Strongly disagree | 10 | 20 |
| Total | 50 | 100 |

Source: Survey Data
Table No.8.6 revels that Majority of 42% respondents are disagree with awareness of all aspects of Security Testing of web application where as only 10% respondents are strongly agree with awareness of all aspects of Security testing of web application.
So, it is concluded that Majority of 42% respondents are not aware of all aspects of security testing.

**Graph No.7.6**
Graph showing respondent's awareness of Security Testing of Web Application.




**Critical factors need to consider while Security testing of web Application**

The following **factors needs to consider while security testing of** web application as **per the researcher recommendation**

**1. Secure Transmission**
a. Check SSL versions, Algorithms, Key length
b. Check for Digital Certificate Validity (Duration, Signature and CN)

**2. Data Validation**
a. Test for Reflected Cross Site Scripting
b. Test for Stored Cross Site Scripting

Check the Web application for XSS (Cross site scripting). Any HTML, such as <*HTML*>, or any script such as <*SCRIPT*> should not be accepted by the application. If it is, the application can be prone to an attack by Cross Site Scripting.

**3. Denial of Service**
a. Test for anti-automation
b. Test for account lockout

**4. Cryptography**
a. Check if data which should be encrypted is not
b. Check for wrong algorithms usage depending on context

**5. Risky Functionality – File Uploads**
a. Test that acceptable file types are white listed
b. Test that file size limits, upload frequency and total file counts are defined and are enforced

**6. Risky Functionality – Card Payment**
a. Test whether card numbers are stored

**7. HTML 5**
a. Test Web Messaging
b. Test for Web Storage SQL injection

**8. Information Gathering**
a. Manually explore the site
b. Spider/crawl for missed or hidden content

**9. Configuration Management**
a. Check for commonly used application and administrative URLs
b. Check for old, backup and unreferenced files

**10. Authentication**
a. Test for user enumeration
b. Test for authentication bypass

**11. Session Management**
a. Establish how session management is handled in the application (eg. tokens in cookies, token in URL)
b. Check session tokens for cookies flags (http Only and secure)

**12. Business Logic**
a. Test for feature misuse
b. Test for lack of non-repudiation

**13. Security Questions & Secret answer**
**a.** Security question should be designed in such a fashion that they are not obvious to be known (For eg. What's your pet's name? Don't frame the question like this).It would be good if user is provided with option of choosing customized security question.
**b.** Secret / security answers should be stored in database as hashes and not plain text.

**14. Captcha**
a. Captcha characters should not be displayed in cyclic fashion.
b. Captcha images should not be allowed to download at one time using add on like Down Them All.
c. Use http://free-ocr.com/ to see if captcha could be deciphered Every refresh of a webpage should display new captcha every time.
d. Do not show the absolute path names of the captcha that is being displayed because it is easy to put assertions identifying the URL and then entering the according characters to pass the captcha.
e. Usage of question and answers type of captcha in textual format is good but, not good enough Researcher personally insists on using Google recaptcha for your web application because it has not been cracked till date. There are many captcha third party services out there but, researchers do not recommend those.

**15. Password**
**a.** Set of rules for setting a password should be same across all the modules like Registration form, Change password, and Forgot password. If these rules differ than hacker might exploit it through brute force method.
b. Password enforcement of alphabets + numeric + special characters should be used in order to protect the account to a greater extent against brute force attack mechanisms.

**16. Forgot your password**
**a.** There need to be a restriction on number of forgot password requests sent per day or in "X" hours interval or have a captcha so that automated requests are not sent.
**b.** The URL has to expire on one use after being used to set new password.
**c.** The token associated with the URL should not be guessable or there should be any pattern which could be easily cracked.
**d.** If the URL is not used within "X" hours then it has to expire (Example: Once the URL is generated, if it is not used then it has to expire after "72 hours")
e. When new token is generated the old ones should expire even if they are not used. Example .com should not send the password via e- mails by resetting automatically
f. There has to be URL which should be used by end-user to set new password of his / her choice.
g. While typing secret answer in Forgot Password the secret answer needs to be masked (Secret Answer is also part of authentication which is similar to password, shoulder surfing or auto-complete stuff could be dangerous here compromising the end-user account).
**h.** Once the password is set, you might want to take end-user to logged in state or requesting him / her to login now with the hyperlink (I, personally would

recommend taking to login page and requesting him / her to login with new **Change Password)**

**i.** Once the password is changed successfully. User should not be able to login again with his old password & new password both.

j. Login using the credentials on Mozilla Firefox ,Login with the same credentials on Google Chrome Now, change password for the account in Google Chrome After this, refresh or try to navigate to some webpage which are allowed to be navigated only by logged in end-users Result: The end- user in Mozilla Firefox web browser has to log out as he / she is in the session which has old password

**17. Secure Data Accessibility by direct pasting URL without Login**

Test by pasting internal URL directly into browser address bar without login. Internal pages should not open.

## VIII. CONCLUSION

The present concluded of the study are based on the Primary data, discussion with the various Sources such as Quality Test Engineers, Software Quality Analyst, Software Developer, Software Engineer, Project Manager and other concern peoples and observation of the researcher while doing the Research.

1. Some of the Software Companies from pune city are facing Difficulty in finding skilled testers with the right competencies as average critical challenge in case of security testing
2. It is concluded that the Security Testing Problems shown in Table are highest critical problems faced by Pune city software companies.
3. In case of security testing challenges majority of Software Companies are facing as most vulnerability is high-priority as average critical challenge.

## IX. FINDINGS

1. Test coverage of web application dependent on all four factors i.e. Security aspects, Functionality, Performance and Usability.
2. Majority of the respondents companies are not aware of all aspects of web application security testing.

## X. SUGGESTIONS

1. Pune city software companies should have separate Security testing team to test security of web application, so if software companies have
2. Dedicated expert Security team then it will defiantly improve usability testing process.
3. Testing team should test Web Application on all types of browsers including all upcoming browsers as client my use different types of browser.
4. Pune city software companies should time to time give awareness training on importance of security testing and also expert sessions on web application security testing to testing team
5. Security Testing activity should start as early as possible and that should be part of SDLC
6. Try very hard to find the security bug ,As if you are testing only to break the application.
7. Testing team should prepare security test cases before start to testing, Researcher means give stress on the security test cases which includes major risk of the application.
8. Testing team should consider factors of security testing suggested by researcher while testing security aspects of web application
9. When you think that you have completed most of the test conditions and when you think you have tried then do some monkey testing.

## XI. REFERENCES:


1. *Di Lucca G.A., Fasolino A.R., Faralli F., De Carlini U.:"Testing Web Applications": in Proceedings of International Conference on Software Maintenance, IEEE Computer Society Press, Los Alamitos (CA):2002, pp. 310–319.*
2. *Ricca F. ITC-irst, Italy, Tonella P:"Detecting anomaly and Failure in web Applications": Published in MultiMedia, IEEE journal: 2006*
3. *Di Lucca G.A., Di Penta M.:"Considering browser interaction in Web application testing": in Proceedings of the Fifth IEEE International Workshop on Web Site Evolution, IEEE Computer Society Press, Los Alamitos, CA: 2003, pp. 74–83.*
4. *Andrews & Whittaker: How to break web software: Addison-Wesley: 2002.*
5. *Myers, G.: The Art of Software Testing: Wiley. (1979).*
6. *Bertolino Antonia by Software Testing Research: Achievements, Challenges, Dreams published in Proceeding FOSE Future of Software Engineering. '07 2007.*