# NEW APPROACH TO WEBDOC SECURITY

Abhishek Purohit, ShubhamWankhede ,Subham,Shekhar ,Mukesh Kumar

*Comp Engg,SKNSITS,Maharashtra,India*

**ABSTRACT**

*In this project, we are going to provide security for the personal documents. By providing the secured website for the storage of the personal data. This approach not only provides the website security but also preserves the users privacy by maintaining the UID(Users identification).This UID can be used at the time of forgotten password, missing cell phone and provides every assistance required for getting the documents. In case of hacking of the account on the website, UID and the security questions plays the vital role. Hence, the authorized user can access their data securely.*

**KEYWORDS:** *SQL Injection, XSS(Cross-site Scripting) , UID(User Identification Code),Personal Document Security*.

## I. INTRODUCTION

Web security testing tells us whether Web based applications requirements are met when they are subjected to malicious input data. Chess and West adopted the static analysis for identifying vulnerabilities was initially proposed as a way to support manual inspection Initially called type-state analysis, taint analysis has been largely adopted to detect inadequate or missing input validation, resulting in cross-site scripting , SQL-injection and buffer overflow vulnerabilities

Cross-Site Scripting (XSS) is a polymorphic category of attacks that may infect web applications as well as their clients, in many different direct and indirect ways. Many countermeasures can be deployed to face this threat: these security mechanisms are located in the internal parts of web applications (e.g. validation checks), on external security components (reverse-proxies, web application firewalls (WAF) like Mod Security ) or even on client-side web browsers. The technical contribution of this paper is a method to systematically test the impact of a large set of XSS vectors on web browsers, including mobile browsers (e.g. on Android).Our test driver, called XSS Test Driver executes a code within the web browser equivalent to the one ran by victims under XSS attacks

## II. RELATED WORK

**1)** Secure Electronic Transaction [2010] :This paper explores promising alternatives offered by applying biometrics in the management of sessions. A secure protocol is defined for perpetual authentication through continuous user verification.

**2)** Continuous and Transparent User Identity Verification for Secure Internet Services [2013]: The paper describes how SET was predicted, designed, and rejected by e-commerce end-users. PKI issues utilized with SET in e-commerce are studied. E-commerce end users being concerned about dominant factor than security issues, usability is a more dominant than security for a secure system project to be adopt by the users .

**3)** Three-Tier Security Model for E-Business: Building Trust and Security for Internet Banking Services[2010]:This paper aims to find various types of flaws in the security of online banking that results in loss of money of account holders and financial institutions.

**4)** Hands-On Teaching of Software and Web Application Security [2011] :This technical paper provides a discussion on present trends in technology and how exactly, simple carry-to-use devices play a vital role in day-

to-day life. Using the present technological devices, how an efficient and smart notice board can be made is explained in this paper.

**5)** Online Banking Security Flaws: A Study[2010]:It explain the Easy SMS protocol is successfully designed in order to provide end-to-end secure communication through SMS between mobile users. The analysis of the proposed protocol shows that the protocol is able to prevent various attacks. The transmission of symmetric key to the mobile users is efficiently managed by the protocol. This protocol produces lesser communication and computation overheads, utilizes bandwidth efficiently

## III. PROPOSED SYSTEM

In the Web Doc Security project, we are dealing with the different attacks like SQL Injection ,XSS attacks and normal databases attacks and making the use of the new algorithms to curb the threats on the website uploaded documents of users.

Providing the UID number in case of missing of mobiles and any other problems. Our system provides the simple GUI views of our project to make users to use the site without ambiguity. Elgamal and Aho-Corasic algorithms have been used in proposed system. Site is made to keep the important documents safe and retrieve from net whenever needed provided user should have internet connections.

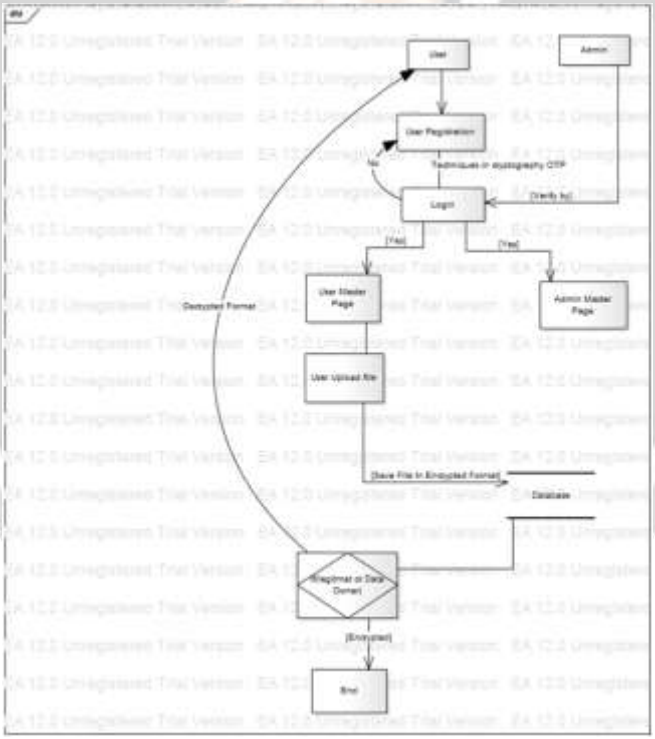


**Fig. Architecture Diagram**

## IV. ALGORITHM

Step I:

Start with login page fill the details and check whether the user is valid or not if not valid output that user is invalid ,else ask them to register.

Step II:-

If the user wants to register go the register page get the information and store that information in the database.

Step III:-

If the user is administrator go to the administration page and authenticate the user who can upload their documents safely.

Step IV:-

If the user is administrator he can also go through all the database details of user uploading and deleting of documents along with time and date preferences.

Step V:-

After the user has been authenticated the user can send the notice after approval by the administrator from the compose page the administrator can also send the notice through compose page

Step VI:

If the user has forgotten their password they can ask to retrieve the password from the forget password page.

Step VII:-

If the user wants to change the password he can change the password from the change password page.

Step VIII:-

User can upload their documents and if they want to retrieve it they can do via downloading the documents from the sites

## V. FUTURE WORK

This WEBDOC Security approach is extremely beneficial in future world as the Google providing the security can be easily breached and the type of security provided by us is not being hacked also we do not have the use of cloud and its better safe than rest of the threats and basically provides security against the main common attacks which is very much vulnerable in today's world . Thus this system provides a secure uploading of the documents of users with best possible security.

## VI. CONCLUSION

In this project ,we list the main targets and content of Web security testing, and also introduce two important tools .Most important, this paper illustrates XSS and SQL injection attacks and also gives some methods and suggestion to defense these attacks. It is estimated that companies lose between 0.5 and 2.5 percent of their revenue because of security-related losses and downtime. Web security testing is really important for enterprises; not only code developers but also QA should take corresponding responsibilities for Web security testing. In the future, we will improve our methods to cope with more and more complex security attack and develop an automatically testing tool to solve XSS and SQL injection attacks.

## VII. REFERENCES

[1] G. Wassermann and Z. Su, Static detection of cross site scripting vulnerabilities, in ICSE 08: Proceedings of the 30th international conference on Software engineering. New York, NY, USA: ACM, 2008, pp. 171 to 180.

[2]J. Bozic, B. Garn, I. Kapsalis, D. E. Simos, S. Winkler, and F. Wotawa, Attack pattern-based combinatorial testing with constraints for web security testing, 2015, submitted for publication.

[3]. J. Bozic and F.Wotawa, XSS pattern for attack modeling in testing, in Proceedings of the 8th International Workshop on Automation of Software Test (AST), 2013...

[4]. W. Chang, B. Streiff, and C. Lin, Efficient and extensible security enforcement using dynamic data flow analysis, in CCS 08: Proceedings of the 15th ACM conference on Computer and communications security. New York, USA: ACM, 2008, pp. 39 to 50.

[5]. J. Bozic, B. Garn, I. Kapsalis, D. E. Simos, S. Winkler, and F. Wotawa, Attack pattern-based combinatorial testing with constraints for web security testing, 2015, submitted for publication.