Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 12, December -2017

# A Critical Analysis on Different Vulnerabilities in Web Application

[1]Narendra M Kandoi, [2]Dr. Vilas M Thakare

[1]*Research Scholar, Computer Science & Engineering, S.G.B. Amravati University Amravati, Maharashtra, India*
[2]*Research Guide, S.G.B. Amravati University Amravati, Maharashtra, India*

**Abstract-***Web application developers start by modeling the functionalities of the application modules and its security necessities using dedicated UML diagrams. Web mashups comprise of a hosting page, for the most part called the integrator, and various outsider segments regularly called gadgets, gadgets, blocks, or pipes. Aspect Oriented programming (AOP) makes it conceivable to segregate this and different issues that were already indistinguishable into modules. An instance of a mashup-based application is a site that merges the information on open flats from one source with the representation usefulness of another source to make an easy to-use delineate. In this paper we develop an efficient aspect oriented programming aided information flow based access control model and automatic classifier based vulnerability prediction model to enhance mashup security. We developed a vulnerable online application, to test the proposed approach. First we tried all sorts of SQL Injection and XSS attacks to see how the application behaved.*

***Keywords****: Web Application, Aspect Oriented Programming, Mashup, UML Diagrams, Vulnerability Detection, Security.*

## I. INTRODUCTION

The Web is presently part of everybody's life and it constitutes the essential methods for access to numerous helpful services with strict security requirements [1]. Therefore, vulnerabilities on the web platform may empower vicious attacks with catastrophic outcomes, extending from financial misfortunes, e.g., on account of attacks against payment providers like PayPal, to protection infringement, e.g., on account of disgraceful exposure of electronic health records [2]. Security-basic services are increasingly provided online today and this expands the need of viable defenses for the web platform.

Tragically, it is extraordinary that ensuring on the web administrations is troublesome by any extend of the imagination, given the inherent multifaceted nature of the Web [3]. The web ecosystem is variegate and incorporates a substantial number of various segments and advances, thus the attack surface against web applications is amazingly huge: security blemishes in the web program may uncover verification certifications and delicate information stored in web pages; vulnerabilities of web protocols may break the confidentiality and the integrity of the communication session; and mistakes in the web application code may prompt the consideration of malignant content in generally trusted site pages [4]. Indeed, even experienced web engineers and security specialists experience considerable difficulties at restraining this complexity, prompting the expansion of security ruptures.

## II. ASPECT ORIENTED PROGRAMMING

AOP is a tolerably new programming perspective and it grows in light of challenge situated programming worldview. It manages those worries that cross-cut the particularity of traditional programming instruments and it goes for diminishment of code and to give higher attachment. Aspect Oriented programming (AOP) makes it conceivable to segregate this and different issues that were already indistinguishable into modules. And furthermore the aims and objectives of the proposed research work in building an AOP based programming framework to create concrete philosophy an approach to isolate the security angle from the fundamental logic of the framework [5].

Another well known domain identified with web application is web mashup which are for the most part utilized for less important assignments, for example, customized queries and map-based perceptions; in any case they can possibly be utilized for more basic, sophisticated and complex requests in combination with business forms in not so distant future as a result of this situation web mashup investigate is picking up a considerable measure of force in both the academic and industry groups [6]. "Mashup" has turned out to be one of the most popular expressions in the Web applications domain and many organizations and establishments are racing to give mashup arrangements (or to dependable existing coordination arrangements as mashup apparatuses). But, the fundamental obstacle is security and modularity which is up most vital [7].

## III. WEB MASHUP

A mashups develop in prominence, the issue of securing data stream between mashup parts turns out to be progressively vital [8].

Web mashups comprise of a hosting page, for the most part called the integrator, and various outsider segments regularly called gadgets, gadgets, blocks, or pipes. An instance of a mashup-based application is a site that merges the information

 

on open flats from one source (e.g., Craigslist) with the representation usefulness of another source (e.g., Google Maps) to make an easy to-use delineate. The quantity of web mashups is quickly expanding. For instance, a registry benefit for mashups programmableweb.com enrolls by and large three new mashups consistently. This catalog contains more than 4000 enrolled mashups and 1000 enlisted content provider API's. [8].

## IV. LITERATURE SURVEY

| NO | Year | Algorithm/Method | Application | Advantage | Disadvantage |
|---|---|---|---|---|---|
| 1 | 2009 [9] | Privacy-aware Identity Management method | Client-side Mashup Applications | Low cost | - |
| 2 | 2010 [10] | Mash-IF method | cross-domain communications within a browser | Efficiency | More insufficient data |
| 3 | 2012 [11] | SOAP secure service Approach | Mobile devices | Optimal solution | - |
| 4 | 2013 [12] | Dynamic runtime monitoring method | Securing web-clients | Efficiency and simplicity | Array and String objects can cause genuine security issues |
| 5 | 2014 [13] | Web based Interactive River Model | client-side web application for interactive environmental simulation modeling | Quickly rising in popularity and usage | - |
| 6 | 2015 [14] | Risk Filtering Data Mining algorithm | Removing most of the false risks in web application | Accuracy and true positive rate | - |

 

| | | | | | |
|---|---|---|---|---|---|
| 7 | 2016 [15] | REST services method | End-user development of REST client applications on smart phones | Minimal effort | Memory limitations |
| 8 | 2016 [16] | End-User Development method | Web mashup | Efficiency result | - |
| 9 | 2016 [17] | Automated UI Interaction algorithm | Discovering and Exploiting Private Server-side Web APIs | High efficiency and accuracy result | - |
| 10 | 2017 [18] | Live-Streaming architecture | To satisfy the requirements that relies on Redis to achieve high scalability | High scalability | - |

## V. PROPOSED WORK

In this paper we develop an efficient aspect oriented programming aided information flow based access control model and automatic classifier based vulnerability prediction model to enhance mashup security.

The proposed secure access control model consists of three key objective stages. Web application developers start by modeling the functionalities of the application modules and its security necessities using dedicated UML diagrams. These charts are then automatically translated into a formal question situated language portrayal appropriate for thinking about data trustworthiness checking as well as for the deduction of a dependable usage of website pages. Further, a formal refinement process is connected on the created question arranged language determination to get a social functionalities web application module which is then converted into an AOP execution, associated with a MySQL Server social database framework. Such an age is performed following the perspective situated programming worldview which allows a partition of worries by making a reasonable qualification amongst practical and security angles.

Moreover, the automatic classifier based vulnerability analysis technique is applied on proposed secure access control model to evaluate the vulnerability prediction forecast capacity in light of composes, for example, SQL infusion, charge infusion, misconfiguration weak passwords, logic errors and so forth. The programmed classifier takes after Fuzzy-Extreme Learning Machine (F-ELM) for powerlessness location and characterization.

The proposed model will incorporates the accompanying steps for implementation.

- First, the developer modelling the functionalities of the application modules and its security necessities using dedicated UML (Unified Modelling Language) diagrams.
- The UML outlines are then consequently converted into a formal object oriented language portrayal appropriate for thinking about information trustworthiness checking as well as for the induction of a solid implementation of web pages.
- Further, a formal refinement process is connected on the created question situated dialect particular to acquire a social functionalities web application module. which is then translated into an AOP implementation, connected to a MySQL Server relational database system.
- Finally, the automatic classifier based vulnerability analysis technique is applied on proposed secure access control model to evaluate the vulnerability prediction capability.

 

The proposed secure access control model will be evaluated through the help of one case study web application program. Moreover, the proposed model will be implemented JAVA platform and the performance is evaluated and compared with existing mashup web security models.To ensure the productivity of the proposed approach we do basic analysis in view of the distinctive powerlessness writes, for example, SQL injection, way traversal, file upload, document incorporation, summon infusion, misconfiguration, delicate data introduction, broken access control, weak passwords, logic errors, unvalidated redirects, targeted hack events, and other attacks.

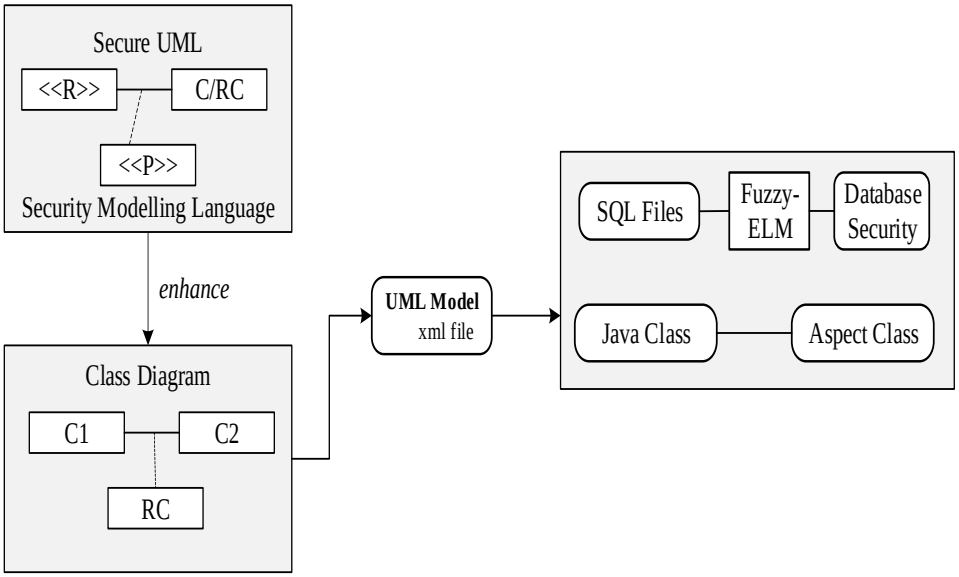


**Fig. 1. Proposed Approach flow diagram**

## VI. RESULTS ANALYSIS

### 1. Experimental Results of Vulnerability Detection

The proposed approach has been experimented on one online application case study program in that demonstrate that the improvement of an apparatus grants to free the developers from monotonous and error-prone tasks since they have simply to push a catch to create the AspectJ code of an application which consists of several hundred of lines. Moreover, the application of the proposed approach on the cases studies permitted to point out security rules violations that are related to operation sequencing and also the occurrence of a forbidden operation before the execution of the corresponding secure one. What differs from one case study to another is the number of classes, associations, attributes and rules that implies more/less JAVA classes to generate; the complexity of the obtained code remains similar.

We developed a vulnerable online application, to test the proposed approach. In the first place we attempted a wide range of SQL Injection and XSS attacks to perceive how the application carried on.

For instance, let accept than an attacker tries to include the accompanying input with a specific end goal to acquire data as a framework administrator:

Select * from clients where login='admin'- - and ‘pwd=’; the query will not be processed by the database because it contains a commentary inside it.

The SQL analyzer will distinguish it and will decline to pass it to the database supervisor. In another example the attacker will try to obtain information using a query that contains a statement that is always true. Select * from clients where login='admin' and pwd='' or 1=1; The analyzer will identify that there is an announcement that dependably is valid and will decline to process it.

The system Aspect J, will achieve our objective, however since we want to keep the angle working without the need of the source code, the runtime weaving sounds as a superior choice. Along these lines, regardless of whether we don't approach the source code we can at present enhance our applications' security.

In the wake of extricating the fuzzy rule based features, an appropriate classifier model must be chosen to arrange these vulnerabilities into various defenselessness writes. In this paper fuzzy based ELM classifier is proposed for defenselessness recognition in addition the proposed classifier is contrasted with conventional Naive Bayes, Support Vector Machine (SVM) and Random Forest algorithms have been utilized as a part of numerous security zones. In the wake of looking at the outcomes in the segment VI among various algorithms, we at long last picked the Random Forest classifier to order the vulnerabilities, for example, SQL injection, XSS, File upload, File include,Command injection and weak password.

 

**Table 1 Statistical result analysis of vulnerability detection**

| | Fuzzy-ELM | | SVM | | Random Forest | | Naive Bayes | |
|---|---|---|---|---|---|---|---|---|
| | Precision | Recall | Precision | Recall | Precision | Recall | Precision | Recall |
| SQL inject | 0.98 | 0.97 | 0.96 | 0.95 | 0.92 | 0.93 | 0.86 | 0.90 |
| XSS | 0.96 | 0.95 | 0.94 | 0.92 | 0.90 | 0.88 | 0.83 | 0.85 |
| File upload | 0.93 | 0.94 | 0.92 | 0.91 | 0.88 | 0.86 | 0.81 | 0.83 |
| File include | 0.91 | 0.92 | 0.90 | 0.89 | 0.85 | 0.83 | 0.79 | 0.80 |
| Command injection | 0.89 | 0.90 | 0.88 | 0.86 | 0.84 | 0.82 | 0.75 | 0.74 |
| Weak password | 0.87 | 0.86 | 0.84 | 0.83 | 0.84 | 0.82 | 0.79 | 0.80 |

From Table 1 results shows the proposed Fuzzy-ELM classifier efficiently classify the vulnerabilities compared to the other classifiers such as fuzzy-ELM, SVM, Random Forest, Naive Bayes. We leverage the proposed fuzzy ELM based classifier is suitable to build a model for classifying vulnerabilities and enhance mashup vulnerabilities.

## VII. CONCLUSION

The web ecosystem is variegate and incorporates a substantial number of various segments and advances, thus the attack surface against web applications is amazingly huge. Web application developers start by modeling the functionalities of the application modules and its security necessities using dedicated UML diagrams. These diagrams are then automatically translated into a formal object oriented language representation suitable not only for reasoning about data integrity checking but also for the derivation of a reliable implementation of web pages. Moreover, the application of the proposed approach on the cases studies permitted to point out security rules violations that are related to operation sequencing and also the occurrence of a forbidden operation before the execution of the corresponding secure one.

## REFERENCES

[1] Heba Kurdi A. Computer Science Department Imam Muhammad Ibn Saud Islamic University Riyadh, Saudi Arabia. Review on Aspect Oriented Programming" International Journal of Advanced Computer Science and Applications. 2013; 4(9):22.
[2] Jose Felix M. Principality of Asturias, Computer Science Department, Oviedo, Spain Francisco Ortin, University of Oviedo, Computer Science Department, Oviedo, Spain, Aspect-Oriented Programming to Improve Modularity of Object-Oriented Applications. Journal of Software. 2014; 9(9). doi:10.4304/jsw.9.9. Pages 2454-2460
[3] Cinzia Cappiello, Politecnico di Milano, Florian Daniel, Maristella Matera Cesare Pautasso Itely and Switzerland "Information Quality in Mashups Int'l Journal, Internet Computing. 2010; 14(4):14-22.
[4] Website Brent Ashley. Shaping the future of secure Ajax mashups Available at http://www.ibm.com/developerworks/library/x-securemashups/ Pub 3-4-07 accessed on 8 Nov 2010
[5] Georg, Geri, Indrakshi Ray, KyriakosAnastasakis, BehzadBordbar, Manachai Toahchoodee, and Siv Hilde Houmb, "An aspect-oriented methodology for designing secure applications", Information and Software Technology, Vol. 51, No. 5, pp. 846-864, 2009.
[6] Anjomshoaa, Amin, A. Min Tjoa, and Andreas Hubmer, "Combining and integrating advanced IT-concepts with semantic web technology mashups architecture case study", In Asian Conference on Intelligent Information and Database Systems, Springer, Berlin, Heidelberg, pp. 13-22, 2010.
[7] Rao, Kamisetty Ramamohan, Zoran S. Bojkovic, and Dragorad A. Milovanovic, "Wireless multimedia communications: convergence, DSP, QOS, and security", CRC Press, pp. 1-289, 2008.
[8] Jonas Magazinius, Andrei Sabelfeld Chalmers, Aslan Askarov Cornell University: A Lattice-based Approach to Mashup Security. Proc of Int' l conf ACM. 2010, 15-23.
[9] .SamanZarandioon, Danfeng Yao, and VinodGanapathy, "Privacy-aware Identity Management for Client-side Mashup Applications",DIM'09, 2009.
[10] Zhou Li, Kehuan Zhang, XiaoFeng Wang, "Mash-IF: Practical Information-Flow Control within Client-side Mashups", IEEE/IFIP International Conference on Dependable Systems & Networks (DSN), pp.251 - 260, 2010.
[11] Jens Bertram, CarstenKleiner, "Secure Web Service Clients on Mobile Devices",Procedia Computer Science, vol.10, pp. 696-704, 2012.
[12] EjikeOfuonye, James Miller, "Securing web-clients with instrumented code and dynamic runtime monitoring",Journal of Systems and S/w, vol.86, no.6, pp.1689-1711, 2013.
[13] Jeffrey D. Walker, Steven C. Chapra, "A client-side web application for interactive environmental simulation modeling",Environmental Modelling & Software, vol.55, pp. 49-60, 2014.
[14] Ahmed Patel, Samaher Al-Janabi and Ibrahim AlShourbaji, "A novel methodology towards a trusted environment in mashup web applications", computers & security, vol.49, pp.107 e122, 2015.

 

[15].GebremariamMesfin, Tor-Morten Grønli, DidaMidekso, "Towards end-user development of REST client applications on smartphones",Computer Standards & Interfaces, vol. 44, pp.205-219, 2016.
[16] Giuseppe Ghiani, Fabio Paternò, LucioDavideSpano, "An environment for End-User Development of Web mashups", International Journal of Human-Computer Studies, vol. 87, pp.38-64, 2016.
[17].Jia Chen, Xingmin Cui, Ziming Zhao, "Toward Discovering and Exploiting PrivateServer-side Web APIs",IEEE International Conference on Web Services, 2016.
[18] Luis Rodríguez-Gil; Javier García-Zubia; Pablo Orduña; Diego López-de-Ipiña, "An Open and Scalable Web-Based Interactive Live-Streaming architecture: The WILSP Platform", IEEE Journals & Magazines, IEEE Access, vol. 5 pp.9842 - 9856, 2017.

 