ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

Detecting Privilege Escalation Vulnerabilities in Web Application and Cyber Defence

Kavita Sawant[1], Sharmilee Dhokale[2], Pooja Naik[3], Aarati Patil[4]

B.E Student , Dept. of Information Technology, Bharati Vidyapeeth's College of Engineering For Women Savitribai Phule Pune University, Pune, Maharashtra, India[1]

B.E Student , Dept. of Information Technology, Bharati Vidyapeeth's College of Engineering For Women Savitribai Phule Pune University, Pune, Maharashtra, India[2]

B.E Student , Dept. of Information Technology, Bharati Vidyapeeth's College of Engineering For Women Savitribai Phule Pune University, Pune, Maharashtra, India[3]

B.E Student , Dept. of Information Technology, Bharati Vidyapeeth's College of Engineering For Women Savitribai Phule Pune University, Pune, Maharashtra, India[4]

ABSTRACT: Vulnerabilities are typically caused by missing or incorrect authorization in web application. As we know now a days the various sites are available on internet globally and the people uses the sites in large amount .In those sites some are the discussion forum sites, and the many people join the posts and start to discuss on that topic. But some of people comments by using very bad words and the other people get disturbed and because of these words the people leave the discussion in between. To avoid these problems we are going to develop a discussion forum with high security and high authentication. Main purpose of this project is to ensure only authorized users can perform allowed actions within their privilege level and control access to protected resources using decisions based upon role or privilege level.

KEYWORDS: Access Control, Web Security, Authorization, Authentication, Vulnerability Analysis.

I. INTRODUCTION

Online discussion forums are well suited for collaborative learning systems. Much of the currently available research indicates that effectively designed collaborative learning systems motivate and enhance learning experiences of the participants which in turn lead to enhanced learning outcomes. As we know now a days the various sites are available on internet globally and the people uses the sites in large amount. In those sites some are the discussion forum sites, and the many people join the posts and start to discuss on that topic.

In the now day's forums the discussion is done on the various topics and many comments are thrown by the various peoples. These comments are good and sometimes they are in very bad manner, means the unwanted comments are also thrown. Sometimes the posts are also on various bad topics, this may lead to bad affect on other people. To avoid these problems we are going to develop a discussion forum with high security and high authentication. This is also informative site, so that user can upload the audio, video and images from their account and can download also.

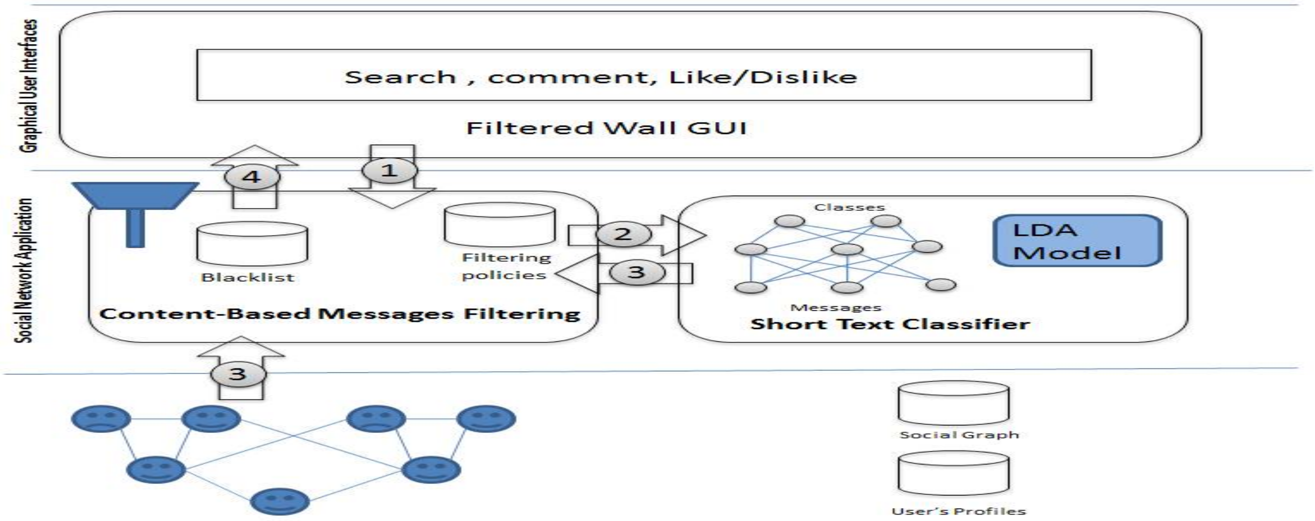
Our main contributions are as below:

1.In our system we are introducing the new concept to prevent the discussion forum from the malicious posts and comments. With facility of uploading and downloading audio, video and images files. Identifying the vulgar comments and posts and removing those from the discussion forum, it is the main goal of our project.

2. The aim of the present work is therefore to propose and experimentally evaluate an automated system, called Filtered Wall (FW), able to filter unwanted messages from OSN user walls. We exploit Machine Learning (ML) text categorization techniques to automatically assign with each short text message a set of categories based on its content

II. PROPOSED SYSTEM

Our scheme mainly consists of three phases:
1) User Registration
2)Posting
3)Filtering
Now we describe each of these phases in detail.



1..User Registration

In User Registration, User can register with their personal information. User can enter the Email id, Password and DoB, Gender. User Uses the Email id as a User_Name and entered Password as a Private key.

2.Posting

In posting phase User can make post in the form of Video, Audio, Text, Image.

3.Filtering:

In Filtering phase, the system can filter the word according to dictionary. System block the vulgar contents

Basic Algorithm:

Following is the Basic algorithm for Checking Vulnerability:

1) Make Post
2) Checking for word in Dictionary
3) If match found don't upload post
4) Else upload post
5) Exit

Now we describe each of this Algorithms in detail.
1) Make Post:

After successfully login for user, user are allow to make a post in form of audio, video, text, image.

2) Checking for word in Dictionary:

If post is in the form of text, then content checking is done. The each word in the post is checked with the word in dictionary.

3) If match found don't upload post:

After checking if word in the post is matched with the words in dictionary, then post is restricted to upload and user will be notified that user is not allow to use that word.

4) Else upload post:

If words in post are not found in the dictionary then post will be uploaded.

5) Exit:

Uploading/Posting is done and now user is ready for another post.

III. IMPLEMENTATION

The proposed system is implemented using Visual Studio Platform. The MySQL database is used for storage purpose. The web portal mainly consists of five modules such as Register/Login module, Uploading of data module, Filtering of data module and blocking of user module. There will be a database server which will be used for storing the user's detail. The programming languages used are C#. There is a continuous need of internet connection for running this application.

IV. EXPERIMENTAL RESULTS

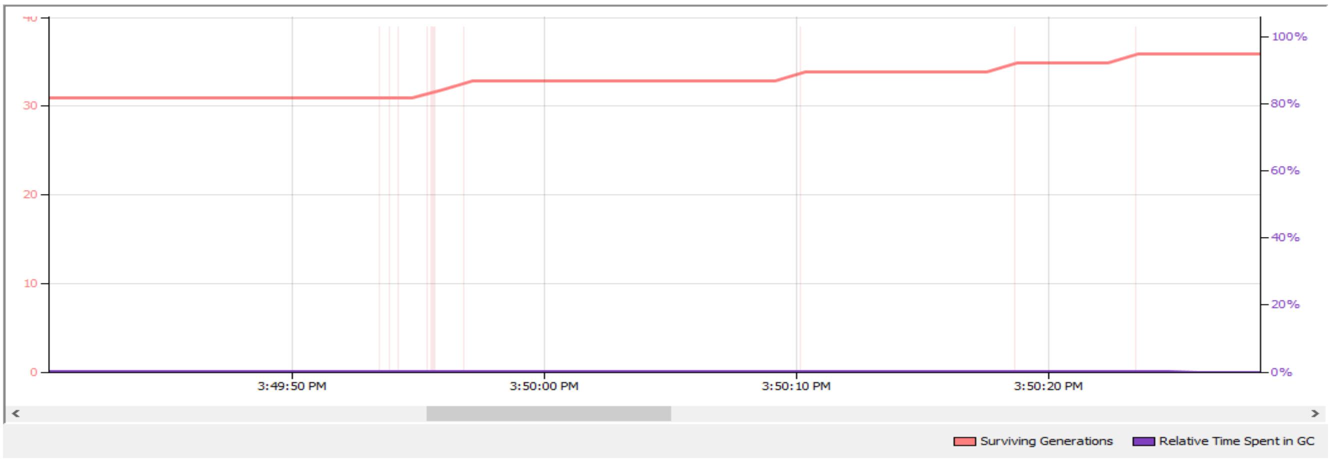


Figure: Memory Graph

V. CONCLUSIONS

We present, a project for automatic detection of authorization vulnerabilities in Web applications. The project is based on our study and characterization of different authorization attacks and the underlying vulnerabilities.

We keep track of vulgar words in our data structure. When such words appear again and again system identify them and supress the privilege level of that particular user who enters that post.

VI.ACKNOWLEDGMENTS

We take this opportunity to thank our project guide "Prof. Mrs. K.S.Sawant" and Head of the Department "Prof. Dr. Mrs.D.A.Godse" for their valuable guidance and for providing all the necessary facilities, which were indispensable in the completion of this project report. We are also thankful to all the staff members of the Department of Information Technology of "Bharati Vidyapeeth's College of Engineering for Women , Pune-43"for their valuable time, support, comments, suggestions and persuasion. We would also like to thank the institute for providing the required facilities, Internet access and important books.

REFERENCES

[1]Macro Vanetti,Elisabetta Binaghi,Elena Ferrari,Barbana Carminati and Moreno Carullo"A system to filter unwanted messages from OSN user walls." , IEEE Transaction on knowledge and data Engineering,Feb2013

[2]Carullo,M.Binaghi,E.Gallo " An Online document clustering technique for short web contents.In:Pattern Recongnition letters"(july 2009)

[3]manning.c, Raghavan.P,Schite.h"Introduction to information retrieval"(2008)

[4]M.Chau and H.Chen," A Machine learning approach to web page filtering using content and structure analysis ", decision support system(2008)

[5]Ali, B., Villegas, W., Maheswaran, M.: A trust based approach for protecting user data in social networks. In: Proceedings of the 2007 conference of the center for advanced studies on Collaborative research. pp. 288–293. ACM, New York, NY, USA (2007)

[6]sCarminati, B., Ferrari, E., Perego, A.: Enforcing access control in web based social networks. ACM Trans. Inf. Syst. Secur. 13(1), 1– 38 (2009)