Security Mechanism in Alumni Portal

Vikrant Pawar, Sagar Date, Suraj Iyer, Chhaya Narvekar.

Department of Information Technology,
Xavier Institute of Engineering, Mahim (W), Mumbai, India.

Abstract— **Alumni Portal is an online medium used by the alumnus, students, teachers and the management of the college to interact with each other for the benefit of each other. There are various security factors related to the alumni portal like phishing, integrity of data and authentication of the user. Various methods are adopted to counter these security issues.**

Keywords— **Alumni Portal, Anti-phishing, MD5, Hashing, Salting, Captcha.**

I. INTRODUCTION

The Alumni Portal is a website that enables the students to interact with the alumni of the college. It provides a platform for the students to connect and network with their peers, follow different threads and events and look for internship opportunities.

The Security mechanism provides various security features like:

1. Solution for Phishing Attacks: Using Code word generation technique, the user can authenticate whether the website is genuine thus protecting him from Phishing attacks.
2. Authentication and Password Security: The use of MD5 algorithm would enable security protection as the password provided by the user will be stored in the form of a hash value. Turing Test: CAPTCHA is a public Turing test that allows the system to distinguish between humans and computers.

The Alumni portal provides the students with functionalities such as:-

1. Profile viewing
2. Private Messaging
3. Connecting and Networking with different alumni
4. Follow current threads and events
5. View internship opportunities provided by the alumni.

II. RELATED WORK

There are many websites which have similar functionalities as that of the alumni portal. Some of these websites are:-

1. Stupidsid:-

It is a website where users can login and can access a variety of resources available on the website. It is a website mainly used for college students. The users have to login to the website in order to access most of the resources. The users can also interact and discuss on various topics on the forum like admissions, MS in US and college life[1]. Attacks against phishing cannot be prevented in this website. The website also does not implement CAPTCHA.

2. LinkedIn:-

LinkedIn is the world's largest professional network with 300 million members in over 200 countries and territories around the globe [2].

The basic functionality of LinkedIn allows users (workers and employers) to create profiles and "connections" to each other in an online social network which may represent real-world professional relationships. Users can invite anyone (whether a site user or not) to become a connection. However, if the invitee selects "I don't know" or "Spam", this counts against the inviter. If the inviter gets too many of such responses, the account may be restricted or closed [2].

- Obtaining introductions to the connections of connections (termed *second-degree connections*) and connections of second-degree connections (termed *third-degree connections*)
- Users can find jobs, people and business opportunities recommended by someone in one's contact network.
- Employers can list jobs and search for potential candidates.
- Job seekers can review the profile of hiring managers and discover which of their existing contacts can introduce them.
- Users can post their own photos and view photos of others to aid in identification.
- Users can follow different companies and can receive notifications about the new joining and offers available.
- Users can save (i.e. bookmark) jobs that they would like to apply for.
- Users can "like" and "congratulate" each other's updates and new employments.
- Users can see who has visited their profile page [2].

3. Pagalguy.com

Pagalguy is an online community which allows MBA aspirants to interact with each other, post questions on competitive exams like CAT, XAT, and CMAT etc. Since its inception in 2002, pagalguy has a user base of over 750,000 users with more than 4 million posts. It is one of the most vibrant and dynamic web portals dedicated for MBA students. Pagalguy has a huge gamut different users ranging from inexperienced users to veterans with years of experience. Apart from providing practice for competitive exams, it also contains threads and posts on various GD- PI experiences in different colleges and also keeps the users updated with the admission process in different colleges [3].

III. CONCEPT REVIEW

A. Anti Phishing

In phishing attacks, the attacker generates a phished page that looks like exactly same as legitimate webpage but that is a fake one .There are a lot of phishing detection and preventive techniques being used which have their own advantages and disadvantages. In [4], the authors have proposed an Anti-phishing method developed using Code Word generation Mechanism. In maximum no. of Phishing cases, phisher's aim is to acquire the credential from victims, and in order to accomplish this phisher make phishing pages in such a way that pages only has submission query which submits user's data to the database and does not retrieve any information related to user or website.
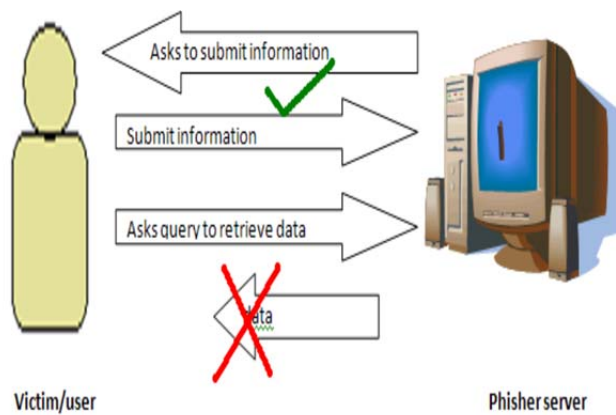

Fig. 1 Phishing [4]

On the basis of the above theory the authors in [4] have suggested a prevention technique. The main objective of the authors is to make web page to be able to retrieve some unique information from the server for every user whenever he visits the link. By the use of this technique users can get ensured themselves that they are logging on actual websites and not on the phished one. To use this technique one is required to get oneself registered on the website which has implemented this technique.

The technique works in two phases mentioned below:-
1. Sign In Phase
    *   User manually visits the original legitimate site for initial registration process.
    *   Organization provides the registration form.
    *   User fills the registration form and creates its user id and password.
    *   On the basis of code generation techniques (explained below) organization generates unique code and saves it with user details.
    *   Organization provides code to user.
    *   User has to remember the code along with user id and password.
    *   Registration process is complete.
2. Sign Up Phase
    *   User gets page link via email or any other method.

*   User enters his/her user id and then she/he needs to enter any two digits (randomly generated sequence no.) of his unique code.
*   After that if digits entered by user is correct then full unique code is retrieved from server and then displayed on the user's screen.
*   User verifies the code and check that whether the same code is displayed which was created for user at the time of registration.
*   With this, user becomes sure of legitimacy of the page and can freely enter his/her other credentials.

The authors in [4] have suggested a method for the generation of code word.
1. Code Generation Technique
In this technique the code is generated via calculation method using simple mathematics as follows:
X = no. of characters of user id+ no. of characters of password
    Y=date (date) + month (date)
    Code = concatenation of values of x and y that is xy.
Note:
Here no. character in user id and password is not less than five characters and if the sum of date and month is less than 10 then add ten in sum of date and month. After code generation first four digits are chosen by user for pattern making. The code word generated is unique to each user. After generation of code word, each digit of code word is displayed in four cells as shown below:
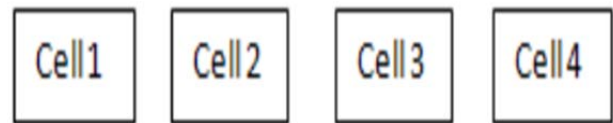

Fig. 2 Code Generation Technique for Anti-Phishing [4]

Whenever the user logs on the websites, after entering his userid (uid) he is asked to enter any of two digits (randomly chosen sequence no.)of his unique code. If the digits matches with the unique code saved in database then his complete unique code is displayed on the screen. Then User needs to verify that code for ensuring himself that he/she is logging on the actual website not on a phished website.

For example: if the codeword is 5678 and user enters values of 2nd and 4th cell then server automatically generates complete code by inserting values of cell 1st and 3rd cell as shown below[4].
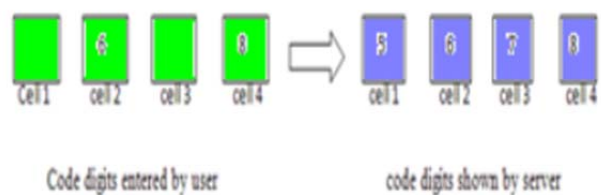

Fig. 3 Obtaining the code for Code Generation. [4]

B. Hashing and Salting

In encryption passwords require a decryption key to decrypt the data. Handling the key secretly is one of the major issues in encryption. Hashing is comparatively better when used with a randomly generated salt. Hashing is analogous to a juicer which converts fruit into juice and not vice versa. Similar group of letters will have a similar hash value. Here the password can be hashed using a hashing technique. Here the hashed value cannot be converted into plain text again. Hence the use of key is not required. In [5], the authors have mentioned a password protection technique using hashing and salt. Salt is a random string used to modify a password hash and can be added to the hash to prevent a collision by uniquely identifying a user's password, even if another user in the system has selected the same password. Salt can also be added to make it more difficult for an attacker to break into a system by using password hash-matching strategies because adding salt to a password hash prevents an attacker from testing known dictionary words across the entire system. The intruder has to produce every possible salt value, which would take both a significant amount of time and space. The length and complexity of the salt value directly affects the time taken for a rainbow table attack [5]. If the salt is longer and more complex, the greater time is required for the intruder to attack the password. The authors have suggested a method to generate salted hash.

The method is as follows-
*   Get password.
*   Generate Salt using trusted random functions/method.
*   Append salt to original password.
*   Generate Salt Hash password using appropriate hash function.
*   Store salt and salt hash in the database.

Advantages of using Hashing and Salting:
*   Hashing and Salting would be a more appropriate mechanism since we want don't want the intruder to identify what the password is
*   Hashing techniques such as MD5 is easy to implement in PHP
*   If a sat is added to the password and is then hashed, it creates a bigger and complex hash value which makes the password less detectable.

C. CAPTCHA

In [6] authors, discusses the need of CAPTCHA to recognize the user as a human and not as a bot. Further, different types of CAPTCHA techniques have been shown and comparative study has been done between them.

The following is the comparison between different types of CAPTCHAS mentioned in the paper-

TABLE I
Comparisons between different types of CAPTCHA[6]

Types of Captcha	Security	Usability	
		Usable for visible impair people	Easy or difficult to use
Text-based Captcha	Good	No	Average
Image-based Captcha	Good	No	Easy
Video-based Captcha	Good	No	Difficult
Audio-based Captcha	Good	Yes	Difficult
Puzzle-based Captcha	Average	No	Difficult/Easy

Also, the paper mentions, the issues related to CAPTCHA, for example the despaired visual sight of a human is not considered and that might not allow the person to verify itself as a human user. Sometimes, the naked eye might find it difficult to comprehend the obscured images. CAPTCHA helps to distinguish a human user from a bot and thus preventing the bot from entering malicious code in the website. The following are the problems associated with CAPTCHA –

*   Human with visual disability are unable to pass the test easily.
*   Image –based CAPTCHAs are sometimes difficult to figure out, especially to the users having low visibility.
*   Video-based CAPTCHAs have large size and take time to load.
*   Puzzle CAPTCHAS are time consuming and they can irritate the user, if he or she is in a hurry [6].

Advantages of CAPTCHA are as follows-
*   Text-based CAPTCHAs are easy to implement and can prevent dictionary-based attacks.
*   Image-based CAPTCHAs even eases the effort of typing, since image is to be recognized with a single click.
*   Video-based CAPTCHAs prevent Optical Character Recognition (OCR) attack, possible in the above two methods.
*   Audio-based CAPTCHA is useful to authenticate people with visual impairment.
*   Puzzle-based CAPTCHAs are brain taxing and fun for the user [6].

D. Private Messaging System

A stand out feature of the Alumni Portal would be the private messaging function, which will allow registered users to send private messages to each other and start chat conversations.

In order to send a private message or start a chat with another user, it is mandatory for the users to be registered with the website to make sure that only proper authenticated users may utilise this system.

Such a private messaging system can be implemented by using PHP and MySQL as the main working engine and CSS can be used to make the chat application look better. Currently many websites such as Facebook, Pagalguy have implemented a chat application whereas LinkedIn provides a private messaging facility.

The main working principle behind the messaging system would be to retrieve the message from one user and post it into the MySQL database. Immediately, retrieve this message from the SQL database and display it to the second user. This methodology forms the basis of the private messaging system.

The following are the steps involved in creating a Private Messaging application:-

1. Creating a Table in the MySQL database:

The first step would be to design a table in the MySQL database that can hold the user id, the senders id, the message that needs to be sent and the time and date of message etc.

This can be done by using the php My admin to create a User table in the database which can have column names like user_id, sender_id, message, time and date etc [7].

TABLE II
A sample table

Sr. No	User_ID	Sender_ID	Message	Time Stamp
1	suraj15	vikrant411	Hi !	2014-10-15 03:34:20
2	vikrant411	suraj15	Hi Friend!	2014-10-15 03:35:00
3	suraj15	sagard24	Welcome	2014-10-16 06:45:00

2. Connecting to the MySQL Database:

In order to start the working of the messaging system, it is necessary to set a connection to the MySQL database. Here we use the mysql_connect() to connect to the localhost, and we pass the parameters such as username, password etc. Once the connection is established, the user can select the database using the mysql_select_db() and in this function we pass parameters such as database name and connection variable defined earlier. Once this is done we can pass queries to the database and store and retrieve information to and from the database [7]

3. Creating the messaging interface:

The messaging interface will be designed using HTML and CSS. With this the entire layout of the messaging application can be designed.
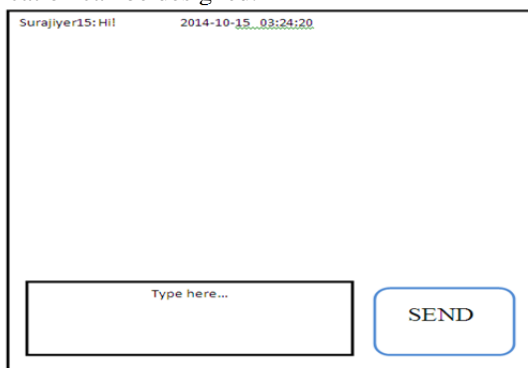

Fig. 4 Private Messaging Sample Layout

Implementing the PHP logic:

The basic logic, behind the messaging application is to get the message from one user, store it in the database and post it to the other user from the database. Initially, the user, types a message, and with the help of the GET method, the message is obtained and is stored in the database with the help of the INSERT query. After the message is in the database, with the help of the SELECT query it is retrieved and then is sent to the respective user. The entire messaging system logic will be implemented using PHP.

Advantages:

- Provides a very interactive messaging system.
- Attractive and easy to use UI.
- The messages sent and received will also be stored in the database thus a message log will be maintained.
- Only the registered users can send messages and initiate conversations.

IV. CONCLUSION AND FUTURE SCOPE

Innovation is a cognitive and creative activity. This innovation has continuously developed the web and its application. But along with this innovation, comes into presence the security factor. The threats that are present are ever-increasing and thwarting the growth of web.

In our project, we have considered the some of the many security issues that can affect a security portal like phishing, human authentication and securing user credentials and the possible solutions to these security issues. Our project, the alumni portal, will help to connect the students of our college with the passed out students who have turned out to be successful entrepreneurs or industry professional. This will help the students to get to know industry requirements while help it would help the professionals to hunt for the right talent. Thus, the alumni portal is a helpful outreach program which can be used to alleviate the quality of students.

Not only will the alumni portal be helpful to the students, but it will be also beneficial to the management as well. With the help of this website, the management can connect and network with the alumni and also invite them for various technical events, workshops or organise placement seminars etc.

It would also be beneficial to the teachers as it would give them an opportunity to interact with the industry professionals which would help them to refine the syllabus appropriately.

In future, many additional functionalities could be added like, Profile evaluation. This feature would help the students to evaluate their profile when they enter their marks in competitive exams like CAT, GRE etc. along with degree percentage and accordingly a cluster of college will be provided by evaluating the profile. This clustering can be performed using algorithms like K-means or K-medoids on the basis of the parameters mentioned above. Users could be relieved of filling tedious forms by logging in using their LinkedIn account. Lastly, a web page could be made which will help companies to carry out mock aptitude test or hacking competition on the website to easily absorb talent for the company as per requirement. Also, access control

methods could be used, so that users can decide who can view their profiles in the later stages of development.

REFERENCES

[1] "Stupid Sid," [Online]. Available: http://www.stupidsid.com/about. [Accessed 17 8 2014].

[2] "Wikipedia," [Online]. Available: http://en.wikipedia.org/wiki/LinkedIn. [Accessed 8 7 2014].

[3] P. Bajaj and P. G. N. Prabhu, "IIM Banglore," 10 11 2011. [Online]. Available: http://www.iimb.ernet.in/~gprabhu/pgcase.pdf. [Accessed 2014 10 1].

[4] M. Mishra, Gaurav and A. Jain, "A Preventive Anti-Phishing Technique using Codeword," *(IJCSIT)International Journal of Computer Science and Information Technologies,* pp. 4248-4250, 2012.

[5] P. N. Patel, J. K. Patel and P. V. Virparia, "A Cryptography Application using Salt Hash Technique," *International Journal of Application or Innovation in Engineering & Management(IJAIEM),* vol. Volume 2, no. Issue 6, pp. 236-239, June 2013.

[6] K. Kaur and S. Behal, "Captcha and Its Techniques: A Review," *(IJCSIT) International Journal of Computer Science and Information Technologies,* vol. Vol. 5 (5), pp. 6341-6344, 2014.

[7] "Stack Overflow," 21 7 2011. [Online]. Available: http://stackoverflow.com/questions/6420264/creating-a-threaded-private-messaging-system-like-facebook-and-gmail. [Accessed 21 7 2014].