International Journal of Multidisciplinary and Scientific Emerging ResearcH (IJMSERH)

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 9.274||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 12, Issue 2, April 2024 ||

Web Vulnerabilities Caused By Social Media Web Service Integration

Jasmeet Kaur[1]

Department of CSE, ITM University, Gurgaon, Haryana, India[1]

ABSTRACT: Social Media Integration has become vital for any public profit making industry to quickly publish and reach their customers. Even the integration respondents are quick enough to catch up the latest products by both hands. Social media integration simply meant to be the summation of social website buttons such as Facebook (FB), Twitter, LinkedIn, Google+ etc., on the most visited pages of your website. Companies are optimizing their presence in the online domain through social media integration and eagerly helping themselves to have more customer engagement to a whole new level. In the competitive era every organization is looking for social media channel to make their products popular among millions of online users across boundaries to make quick money out of their valuable services. Pause: Have we ever thought of the vulnerabilities involved in accessing the social media channels on sake of security threats of stealing their private information by hackers? Web services involved in integration of social media should be protected due to the vulnerabilities with each software components may have.

KEYWORDS: Vulnerability, Accountability, Susceptibility, Authentication, Authorization, Optimization.

I. INTRODUCTION

Social media integration by web services has posed a threat of personal information getting stolen by hackers. A User should be careful while logging in the Apps or Web Services that lets the User directly logged in using credentials associated with his Facebook, tumbler, Twitter, or Google account. OAuth 2.0 and OpenID has a security flow that could be compromised by an attacker who can easily place a redirection for your happy flow to a malicious site in no time and take over to your personal secured information for his sinful purpose. It is a side effect of using OAuth 2.0 and OpenID technology creates a vulnerability of using your login from Facebook, Google, etc to access other sites and services on your behalf. Since due to this flaw, attacker/hackers can create an illusion for a user that the user has logged in Via FB or Google & then redirect them to a malicious website owned by him or some another hacker. Now from there, based on the level of access granted and the authorization role, it can expose your contacts, friends list, personal information and also your bank details, or if the case is of Google Apps, it can steal images, stored data etc.

These security threats need to be paid attention to by the leading online players. Web services or Android and iOS apps are or can be easily accessed by these social channels, which allows customers to sign it to their accounts using their credentials on the cost of their security threats caused by hackers. Actually if the customers having account with big companies blindly trust associated third parties that use its login system to connect with web services. It ensures an ease for the development team because they don't need to make their own authorization system. Rather than that, they only depend on the security which is provided by OAuth 2.0 an open source developed protocol. In this way the customers may become easy targets for an online attacker.

II. LITERATURE SURVEY

In[1] Author has mentioned that social media integration is more complex than any other system integration. The reason being is that it connects the users across the world in billions of billion counts. The more it grows and penetrates in depth of the clod environment the more its vulnerability increases.

In [8] Author has mentioned that social media Facebook has provided its integration apis for various global websites like Time.com, Pandora.com & ESPN.com etc. few problems in the Facebook API has lead to rework for its developers and paved the way for Facebook Open Graph which has made the API little unpopular. Few security issues included: exposing privacy from user friends which allowed the Facebook users to get the personal events online of the current user. They can also see pending friends requests , online chat messages etc. Developers of Facebook have more control on the user data including public information of users and friends. Profiles are more easily searchable.

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 9.274||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 12, Issue 2, April 2024 ||

III. SECURITY FLAWS

Security flaws are not merely just the susceptibility in OAuth itself; it's also the accountability of the big companies, how they had implemented the OAuth 2.0.FB, for example, always suggests its developer team that they should effectively close the protocol vulnerabilities by limiting redirections to use safe and secure URLs. But many developers don't use it. It is very often that big companies might not take care of implementing security measures for each and every request. Big companies are working on to secure the social media integrations while being aware of the security issues of using Web Services. OAuth 2 is a protocol that allows applications to interact with a social media's APIs.

Companies are doing their investigation and as of now determined that the security threats are in the domain of a third party portal and they recommend victims to right away report the issue to the third party vendors, Instead they need to ask the developers to look into this serious issue. Until there's a fix available by these big companies, you need to be very careful whenever an application or a site ask you to connect via social media channel. To be aware of that if you are browsing at a site & get a blinking request to log in with your social media account when you're not at all expecting for the same, it would be better to stay back and don't proceed further.

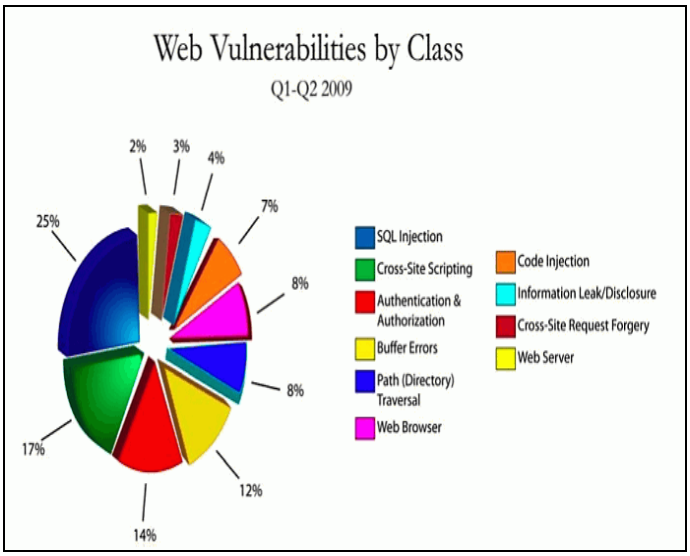

Figure 1 - Web Vulnerabilities

Many web services today allow their users to reset the password. Generally you need to provide your username and answers to some security questions. Sometimes these questions are very simple like : "Where did you go to primary school?", "What is your date of birth?', "What is your mother's maiden name ?" etc .These information can be extracted from your social media integration very easily. This stealing will allow an attacker to answer the simple security question correctly and then reset the account. Once the account is compromised it might be used to generate other useful information or to wrongly spamming with connected friends.

Figure 2-Million Users information on Social Media

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 9.274||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 12, Issue 2, April 2024 ||

Since millions of users are currently active over internet through various social media channels it is quite high time that their information can be easily stolen by a hacker due to even a minor security flaw in web service integrations.

IV. PROBLEMS IN SINGLE SIGN ON

In this era of social networking and software-as-a-service (SaaS), Web-Based single sign-on (SSO) facilities are now provided by many commercial websites to secure and provide many web resources in a SSO. The seasoned research work in formal verification process has been over but only few of the scientists have analyzed and reported the threats exposed by poor security quality of SSO policies which are commercially deployed in the real time websites. This type of analysis always faced with technical challenges such as including lack of access to well established code and protocols, also the complexity by the rich browser elements.

Single Sign on (SSO) is used extensively today in major e commerce domain for improved user experience. In a recent survey, a majority of web users prefer SSO to be offered by websites to have an immediate access to the web resources of different applications. Single Sign on (SSO) is a way of using resources of multiple websites having autonomous end to end software systems. With this facility a user is prompted to do one time log in and he gains the access to all the systems and web resources, saving the time to be authenticated against every website. This type of security is managed by using Lightweight Directory Access Protocol (LDAP) & stored LDAP databases on servers. Saving Cookie is the yet another way to manage single sign on feature if the websites are on the same domain.

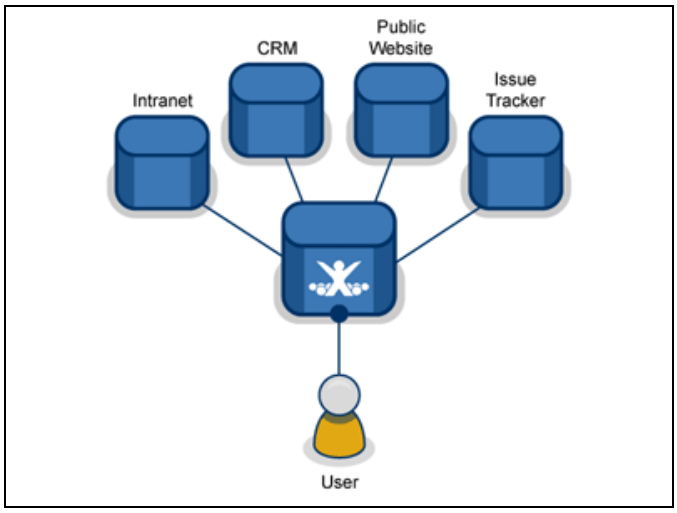

Figure 3-Single Sign On Feature

On the other hand, single sign-off is the reverse feature which terminates user access to multiple systems if a user simply signs out. A better way of using single sign on feature should be that it internally stores encrypted authentication credentials to access different systems apart from managing initial authentication and authorization. There are some other available shared authentication mechanisms that include security feature of OpenID, OAuth, OpenID Connect, and FB Connect, which requires the users to log on using their credentials whenever they want to access a different system or an application. Since in the single sign on mechanism the user is logged in initially with his credentials for accessing multiple resources, his credentials might get hacked for misused due to security threat. Therefore, SSO feature is required to be improved so that it protects the user credentials, & should be , and should be merged to the well built authentication mechanisms, for example one time password token, smart cards etc.

SSO usually makes the Authentication Systems highly critical because sometimes its availability may result in inaccessibility of all the systems which are leveraging the single sign on mechanism. Additionally single sign on may be configured with Session Failover Safeties (SFS) in order to maintain the system operation fluently.

V. STEPS TAKEN BY COMPANIES TO REDUCE SECURITY VULNERABILITIES

As per the research studies it has been revealed that the companies are revising their security model which takes into account the sharing of information and tweets across social networks. There are risks in the use of and social media channels which may be integrated with web services having one or more security flaws those are often not well recognized. The companies are educating its customers to keep them alert to what may happen and the precautions

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 9.274||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 12, Issue 2, April 2024 ||

which can be taken thereof. They are even guiding the people to let them believe that the Internet is not a private place. Some big giants like Google, Amazon are informing the users about the advantages and of the risks of social networking sites. Generally the young users are more vulnerable and they should take care of the information being shared online with great cautiously. A legislation owned by law of the land needs be designed again to protect personal information online, and also to define and then to protect data ownership rights and behaviors in a web-based environment.

Figure 4: THE SOCIAL MEDIA REACH

Companies have identified some dangerous risks that should be taken care of. They have started with providing some guidelines about usage of social media. A disclaimer policy needs to be accepted by the users to adhere to acceptable use policies while browsing social media through company account credentials. Apart from that social media access via single sign on has been blocked partially with the help of proxy servers and next generation firewalls. A technical solution should be provided by developers to capture messages, mails and chat repositories of social media, especially those which are tightly integrated into social networking sites.

VI. CONCLUSION

Today's world thinks that the use of social media is a vital task. But they don't understand a security risk behind it like the effects of social media, i.e. what can happen, how much damage it can cause. Integration of social media with web services has been put on a toss for many times due to security flaws in the channel which can attract an attacker. While social media integration is indeed a beneficial adds-on to your site which can generate more traffic and aiding in search engine optimization as well). However an excessive amount of social media widgets will leave your site in a messy state and will make users annoyed. The user's information retrieving by web services involved in the integration may be easily stolen by hackers for their personal use.

REFERENCES

[1]Elisa Bertino, Security for Web Services and Service-Oriented Architectures, Springer, 2010.
[2]Jodi Mardesich, A widespread security flaw allows hackers to steal information from people using social media logins, May 4, 2014.
Social Login information by Wikipedia.
[3] Outlook.com information by Wikipedia.
[4]Jodi Mardesich,How FB connect & other social logins can expose you to hackers, May 4,2014.
[5]Candid Wuest, The risks of social networking, Symantec Security response
[6]RuiWang, Signing me onto your accounts through FB and Google, A traffic guided security study of commercially deployed SSO web services.
[7]Robert Shullich, Risk Assessment of social media, Dec 5, 2011.
[8]Priidu Tammeorg, Social Media Integration to a Web Service. The Case of Vifi.ee,2011