International Journal of Trend in Research and Development, Volume 5(2), ISSN: 2394-9333
www.ijtrd.com

Review Paper on Website Attacks -Phishing, SQL Injection & Cross Site Script

[1]K. S. Satpute and [2]H. S. Koparkar,
[1]Department of computer Science and Engineering, Datta Meghe Institute of Engineering, Technology & Research, Wardha, India
[2]Department of Computer Engineering, Acharya Shrimannarayan Polytechnic, Pipri, Wardha, India

Abstract: In the era of digitalization social networking is most popular platform for the user to share or interact with each other's. Because of these interaction most sensitive personal data available to social networking sites. Today's world is very much dependent on the web applications, such as banking, e-trading, e-commerce, etc. because of this privacy protection to user on social networks has become a research issues.

Providing security to these web applications is very important. With hackers aimed to breakthrough this security using various attacks, as a traditional information stealing technique, phishing attacks still work in their way to cause a lot of privacy violation incidents. SQL injection attack is very common attack that manipulates the data passing through web application to the database servers through web servers in such a way that it alters or reveals database contents. While Cross Site Scripting (XSS) attacks focuses more on view of the web application and tries to trick users that leads to security breach. In this paper I am trying to know how these attacks are work to protect the user data.

Keyword: - *Attacks, Social Network, Phishing, SQL injection and Cross Site Scripting.*

I. INTRODUCTION

In the digital world every organization or company such as banking, e-trading, and e-commerce want to reach to its customer quick and easily that why they prefer the web service. The social networking sites are most suitable to attract the customers for their services for that every organization or company create or maintained website. For the use these websites services first user need to register for that. User can share his/her personal information such as name, mobile number, address, account number in case of financial service, etc. the service provider must create database for the future use. Here the major concern is arising for data security. Providing security to these web service is very important, because they are storing the others personal and sensitive data for its own profit or gain.

Some user uses this social media for its own benefits and they are very dangerous to other because the use this social networking sites to still the other information and use for own benefits the different type of attack applies to gain the access or information through this media some of the common type of attack is Phishing, SQL injection and Cross Site Scripting.

II. TYPES OF WEBSITE ATTACKS

A. Phishing

Phishing is a form of social engineering in which some attacker impersonators electronic communications to trap users to provide their confidential information i.e. Steal user data is called Phishing. Such communications are usually through emails that trick users to visit fake web sites that in turn collect users' private information, such as passwords, credit card numbers, and social security numbers. Following Fig 1.1 and Fig 1.2 show some phishing attack example.

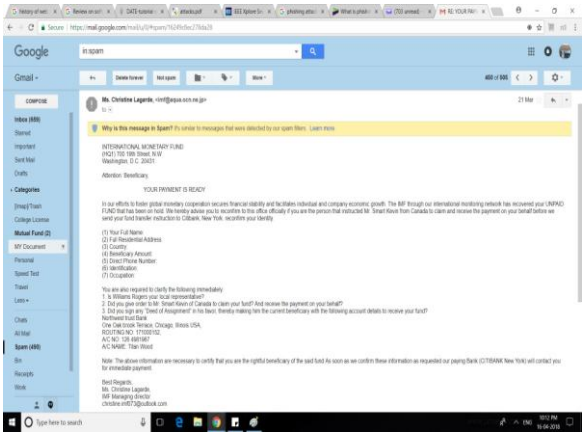


Fig. 1.1 Email to provide the personal and bank information for UNPAID Fund to User account by the Handler of unknown person. The SMS is send to User for Win the 3.7 Cr to claim this amount send the personal information to unknown use email id.

There is various method to collect the user personal information such as:

a) **Design the Fake Website-**here the attacker uses the same domain as original but some extra code is inserted that to access the data. It looks like the real website.
b) **Design Pop-up-** Instead of design a fake web site here the attacker inserts a piece of code that pop-up generates to redirect the data to attack.
c) **Website with validation-** the attacker creates a website when the user input the credential the attacker redirects to original one and gain the access without knowing the user.
d) **Link manipulation-** Misspelled URLs or the use of sub domains are common tricks used by phishers, such as this example URL, https://www.onlinesbi.com.sbi.org /.
e) **Pharming-** Piece of code inserted to computer or server that redirect the user info to attacker.
f) **Phone Phishing-**this is most commonly used attack here attacker send the SMS /Call the user and trick that the user credit card is expire for inconvenience share your

card no to extend the validity. Such types of attacks are coming under the phishing [2].

B. *SQL injection*

Today every person can use web applications for example e-shopping, online bank transactions, reservations etc. for save the time and money. When the user goes through these services all the data and transaction information that is provided in these web sites is recovered and stored in the database. But the database where this information is stored is highly prone to SQL injection attacks. SQL injection attack is where the attacker inserts malicious SQL statements which may possibly give him access to the database or the information stored in the database or harm the web application or the web application users' privacy.

SQL injection, also known as SQLI, Multi-tiered web application typically has three tiers- the web, Application and Database. The web tier interacts with the application layer which, interface with database, application with limited business logic, the database tier contains the database and Database Management System (DBMS). The database nothing but a relations or tables and each relation has no of Row and columns. For example, the college website displays the result of semester's student need to access this result with the help of correct credentials i.e. user id and Password. The college has the webserver to store this information in advance when the get the admission. Student need to enter the correct user id and password to access the result. The student enters the login id and password and click to submit button. The parameter is pass in the body of HTTP POST/GET request such as www.abccollege.org?s_ID=123 & Pass=123. The server application restores the form parameter and generate the SQL query such as select s_ID, Result from Student_Info where s_ID=123 and Pass='123' the result is shown to student as the correct id and password. Some application builds the SQL Queries using string concatenation and then submit the query to the DBMS. select s_ID, Result from Student_Info where s_ID=123 and Pass='123' or 'a'='a' here where clause is true even if first two are false the OR ensure that clause evaluate to true.

The user entering part of an SQL commands as an input parameter, thus changing the semantics of the original query such attack is refer to as SQL Injection attack. The attacker can insert the condition which would always evaluate to true. E.g. 'or '1'= '1' - -, 'or 1=1; - - drop table logintable; - -, [1][3].

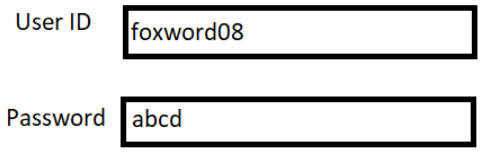


Fig. 2.1: User Login Page

Here the user login with correct user id and Password. For the SQL Injection.

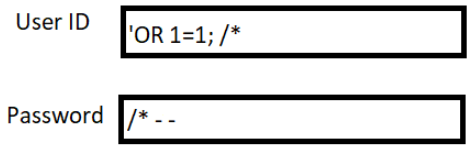
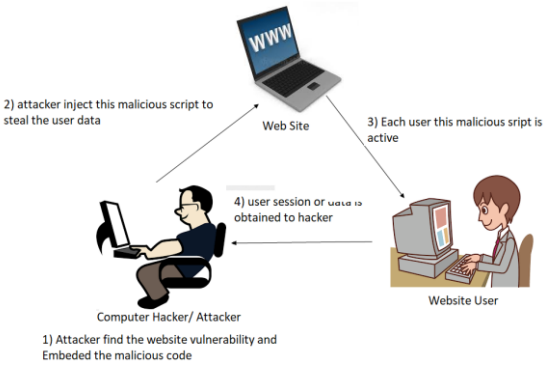


fig 2.2 SQL Injection for Login

C. *Cross Site Scripting*

Cross site scripting (XSS) target the client-side scripting like HTML contents of the web page. This attack can affect ActiveX and Java Scripts. In XSS attacker tries to inject the HTML view with some scripts that runs on client side causing damage to users. The malicious code is created by the cleaver design of an attacker, not the developer.

Social networking sites are used to target this attack by the attacker send the code embedded with the script <script> malicious code</script>. For example, the user wants to login in social networking site page the attacker sends the link that embedded the XSS Script. <script> alert ('You have been hacked!') </script>whenever the script is run the alert message is come "You have been hacked" the user displays this message on screen. By using such malicious code attacker get the information without knowing the user [1] [5].



CONCLUSION

In this paper explain how the Phishing, SQL injection and XSS attack is work through social networking sites. The user need to take precaution when he/she use the social network or, otherwise he/she is victim by attacker to Phishing, SQL injection and XSS attacks

References

[1] Bernard Menezes, "Network Security and Cryptography", Cengage Learning, 2011, Page 250-275.
[2] Jian Mao, Wenqian Tian, Pei Li, Tao Wei, Zhenkai Liang "Phishing-Alarm: Robust and Efficient Phishing Detection via Page Component Similarity", IEEE Access, September 19, 2017.
[3] Karis D'silva, Vanajakshi J, Manjunath KN, Srikanth Prabhu, "An Effective Method for Preventing SQL Injection Attack and Session Hijacking", 2nd IEEE International Conference on Recent Trends in Electronics Information & Communication Technology (RTEICT), May 19-20, 2017, India.
[4] Shaimaa Khalifa Mahmoud, Marco Alfonse, Mohamed Ismail Roushdy, Abdel-Badeeh M. Salem, "A comparative analysis of Cross Site Scripting (XSS) detecting and defensive techniques", Eighth International Conference on Intelligent Computing and Information Systems (ICICIS), IEEE Conference,2017 page 36-42.
[5] Ding Lan; Wu ShuTing; Ye Xing; Zhang Wei "Analysis and prevention for cross-site scripting attack based on encoding", IEEE 4th International Conference on Electronics Information and Emergency Communication,2013 page 102-105.