Against the Tell Friend Email Security Vulnerability

Ali Hameed Yassir

College of Computer Science and Information Technology, Sumer University, Thi-Qar, Iraq.

Author's contribution

The sole author designed, analyzed and interpreted and prepared the manuscript.

Article Information

DOI: 10.9734/AJRCOS/2018/v1i324745

Editor(s):

(1) M. Ilayaraja, Assistant Professor, Department of Computer Science and Information Technology, Kalasalingam University, Krishnankoil, India.

Reviewer(s):

(1) Manish Mahajan, CGC College of Engineering, India.
(2) Dandy Pramana Hostiadi, Stimik Stikom Bali, Indonesia.
(3) Robiah Binti Yusof, Universiti Teknikal Malaysia Melaka, Malaysia.
(4) Jose Ramon Coz Fernandez, University Complutense of Madrid, Spain.
(5) G. A. Sathish Kumar, Sri Venkateswara College of Engineering, SriPerumbudur, India.

Complete Peer review History: http://prh.sdiarticle3.com/review-history/25956

ABSTRACT

Today an E-mail service is one principal tool in our daily work and life. We cannot dispense Email services. Spammers continue to develop their techniques to flood our inbox daily. On the other hand, websites are created to be in different types of different goals like news, sports, environments, staticalists, governments, etc. Websites may be in its environments, static sites, programs, or databases, and very often a combination of the three integrating relational databases as a back-end. Websites require intensive care in configuration and programming to assure a security factor, confidentiality, and trustworthiness of the published information. Most websites have many scripts that give visitors elastic options to share some subject's links URL with their friends one of that by using a tell a friend form. One of most well-known attacks over the internet is done by SQL-injection, though SQL-injections back to exploits, weak validation of textual input that is used to build tell friend scripts which cause dangerous attacks threat email user’s privacy through cheating attacks. In this paper, the author aims to analyse a tell friend exploit and proposes a solution to stop this exploit.


Keywords: Email security; tell friend exploit; information security; SQL-injections.

*Corresponding author: E-mail: alihameed_48@yahoo.com;
1. INTRODUCTION

Like other services through the internet, e-mail has been created based on the server-client mechanism; Email has the simplest architecture [1].

To explain techniques for sending an e-mail from sender to receiver, both sender and receiver represent a user agent; a user agent is a software package (program) that composes, reads, replies to and forward messages. It also handles mailboxes [2].

After the connection was established between sender and receiver over TCP/IP suites, now sender is ready to compose an email depends on user agents capabilities, like use a command line or GUI window that has input text box to write one character each time as in Command line as was the to write all message one time at one time as is now in GUI development applications [3,4].

After assigning the destination address in an e-mail header which represents an email address of the receiver, e-mail is pushed from its source (sender) by SMTP at first stage, then it is popped by either POP or IMAP to its destination (Receiver). As shown in Fig. 1.

As the simplest description of e-mail architecture and mechanisms, Web site’s pages also are designed simply and basically from an HTML tags with many scripts types like VB scripts, Java scripts, and PHP scripts, which let websites designers add many elements into their pages codes to increase interaction between web pages and the users from one side or among other web services from other sides [5]. One of these elements is telling friend scripts, tell a friend scripts to let website visitors share links to some preferred subjects with their friend by e-mail. These scripts can be inserted inside web page codes to pop up a new window when visitor click on the tell friend’s hyperlink icon or tell friend’s hyperlink title when they want to share some things. The new window has been popped up has its URL for a visited page, this window has a form many text boxes, combo boxes and others for filling in it by a visitor information like sender’s name, sender’s email and the destination information like friend’s name,

Fig. 1. Email mechanism
friend's e-mail and some time with a short message [6].

![Tell A Friend Form](image)

**Fig. 2. Tell friend mail form**

As shown in Fig. 2, after the sender fills this form, the sender can click the send command to submit the filled form to the server that hosts the preferred page using HTTP transactions, then server process incoming data from the client (sender) then forwards an e-mail using an SMTP to the destination's friend email box [7]. When an email is delivered to the destination mailbox, then the receiver (destination) can read the email that is sent to him from the Server by his friend (RFC 2822).

### 2. EMAIL TRACKING

Many technologies such as Email tracking that is used by individuals, email marketers, spammers, and phishers, to verify that emails are actually read by recipients, that email addresses are valid, and that the content of emails has made it past spam filters. Other technologies used to secure email during transmission [8].

Spam Email may have an attachment of different media file or it has only a link with a labelled data that are phishing the user to follow the mined link which may redirect the user to a trap. The worst incoming Emails that appear to the user as it comes from trusted one, but they have bad news in different subjects Personally, military, Economics,...... Etc. The most dangerous types of emails are those that redirect the user’s web navigation to sites that causes hacking or exploits the computer, software or the information [9,10].

### 3. TELL FRIEND EMAIL EXPLOIT

The exploitation of E-mails is one of the various exploitations types in which the attacker to fake addresses, data or both, hence it is important to spotlight on one of the ways that the attackers using by injecting the link of some Web pages then generate the page that allows the attacker to fill information in its form as he wants. Attackers follow a specific procedure in an easy steps. The Email vulnerability exploits procedure in an easy way is the SQL- Injection that injected instead of the reference id value of any URL of any website page [11,12,13].

As an example, let us assume that there is a bank website and there is a news page. When the sender clicks the icon button of tell friend to send a specific news to a specific receiver, the news window will pop up with the link to the news, then sender process the link by SQL - Injection through change the id reference of the news page that attached through the link instead the original URL.

If the news page has a reference URL= http://www.example.com/news?id=123abc

There is two method of attacker to inject his Value as SQL- injection.

#### 3.1 First Method

The attacker change the Url Reference id for the original page URL. Then the attacker using tell friend service form as he wants (filling with a fake data). As an example, if the original URL, for example website has a page news URL as follow http://www.example.com/news?id=123abc

Then an attacker can change the original URL reference id from id=123abc into id=0 Or id =1 http://www.example.com/news?id=0

So when the attacker click a tell friend button the popup page tell a friend page will appear has URL like http://www.example.com/journal?tellfriend&id=0

Then the attacker can fill the tell a friend form as he wants.

#### 3.2 Second Method

The attacker follows the original URL for the specific page, then he clicks the tell a friend
button, then when the popup page window form appears, the attacker change the id reference for the popup window. As an example, if the original URL, for example website has a page news URL as follow:

http://www.example.com/news?id=123abc

Then attacker can let original URL and directly click a tell friend button then the popup page tell friend page will appear has URL like

http://www.example.com/journal?tellfriend&id=123abc

Then the attacker change the tell friend URL reference id from id=123abc into id=0 or id =1

http://www.example.com/journal?tellfriend&id=0

Then the attacker can fill the tell a friend form as he wants (filling with a fake data).

4. TEST AND EXPERIMENTS

The author tested a huge number of websites were infected and suffer from security vulnerabilities of this type. The author cannot refer directly to specific websites because this violates the privacy of those websites, but the author able to enhance the field of information security through the detection of this vulnerability of security and calls to fix these security problems. By using any web browser the attacker can inject the link of telling friend tool. See Fig. 3 a simple flow diagram represents the analysis of the attack.

Fig. 3. A simple flow diagram represents the analysis of the attack
5. CONCLUSION

In this paper the author revealed one of the methods that is used by the attackers to submit a fake E-mail through using of the service called a tell a friend, the author refers that most of the website pages containing a service that sends and shares the news to a friend infected by this vulnerability and allow the attackers to exploit this problem. The author urges the use of methods to verify the security of websites and enhance the quality of services through designing. The author recommends the use of modern techniques that limit the use of mechanisms to tell a friend in a way that allows exploitation. As an example the use of modern secure sharing tools like using the services of addthis tools. (https://www.addthis.com).

6. FUTURE WORK

Future work concerns deeper analysis of particular mechanisms using the theory of computation models to describe this problem than to find a more reliable method for providing safe sharing tools.

COMPETING INTERESTS

Author has declared that no competing interests exist.

REFERENCES

12. Chandrashekhar Sharma, Jain SC. Analysis and Classification of SQL injection vulnerabilities and Attacks on Web Applications. IEEE International Conference on Advances in Engineering and Technology Research (ICAETR); 2014.

© 2018 Yassir; This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Peer-review history:
The peer review history for this paper can be accessed here: http://prh.sdiarticle3.com/review-history/25956