Cross site scripting

R.B.S Rathnayake

MS18902662

MSc in IT (Cyber security)

Abstract

The scripting languages like JAVA-script and VB-script are widely used in network application to improve user Experian. scripting languages are light-weight, more powerful procedural language with rudimentary object-oriented capabilities.

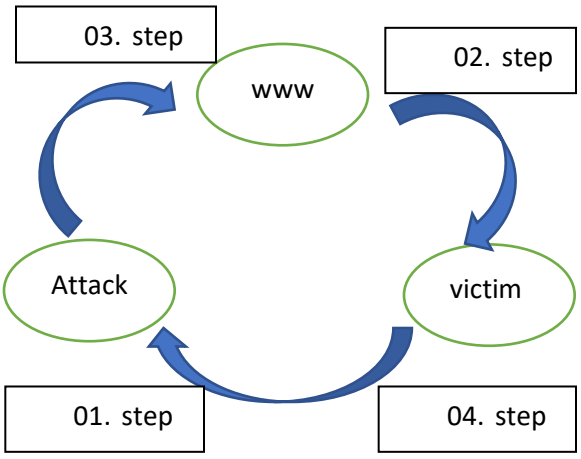
At the same time, scripting language add more vulnerability for cross site scripting (XSS). XSS is more serious computer security threat that allow attacker to get access over sensitive information.

Introduction

Internet and internet application become more important ways to provide day to service for the human-been. To improve user experience most of them are use scripting language like JAVE and VB.NET. However, this trend also makes Cross-Site Scripting attacks one of the most serious threats to Internet. Cross site Scripting (XSS) let and attacker to review over the user privacy, sensitive information. Most often attacker make uses of viruses to propagate this type of attacks. Some famous social networking sites, such as Facebook, Myspace and Twitter, have been suffered XSS attacks. XSS has the features of self-spread and fast spread, and simple implementation as well, so it attracts more and more attention. XSS attacks are often referring as illegal code injection for the web application. When the users browse web page which are suffered with XSS attack, the embedded malicious script will be triggered the way to inject malicious scripts into the web page can be classified into two categories

(1) Persistent XSS attacks (stored XSS)

The persistent XSS [1][2] attacks can be referred stored XSS as well. Following diagram illustrate the behaviors of the stored XSS [3].



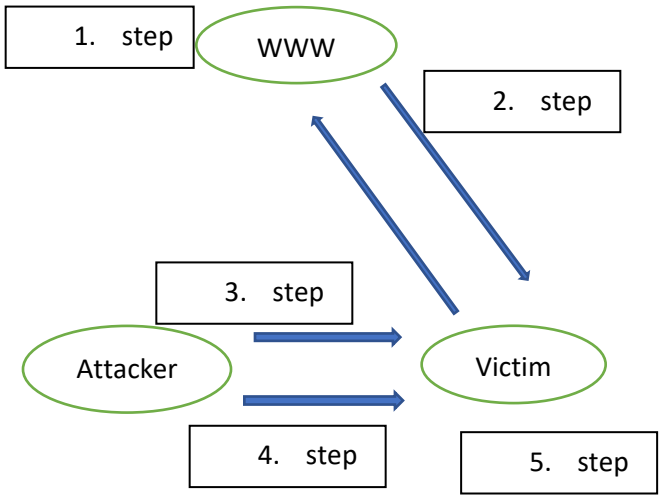
01. Step- attacker find the vulnerable web application
02. Step- inject malicious code into web page

03. Step- victim browser download and execute the code
04. Step- victim information sent to attacker

In this contest attacker find out vulnerable web page and inject malicious script in to that page, more often that will happen as comment on social network, then user browse the particular vulnerable web page malicious code will automatically download and execute it, after that bot machine do what attacker intend to do.

(2) Non-persistent XSS attacks (reflected XSS)

Non-persistent XSS attacks [2] are also referred in the literature as reflected XSS attacks [4].



1. Step- Attacker sent URL for user attraction
2. Step- user click URL
3. Step- Vulnerable web page reflect the code
4. Step- User bowser execute the code
5. Step- User information sent to attacker

It is different form than persistence XSS attack, that inject malicious code into the resources of web application, in reflect XSS the user motivate to click the malicious web application, resource web page directly sent mucinous code to victim machine if the user is flooded to click the link malicious script execute and user information send to the intended attacker.

(3) DOM – based XSS (document object base)

DOM-based XSS is an advanced XSS attack. It is possible if the web application's client-side scripts write data provided by the user to the Document Object Model (DOM). The data is subsequently read from the DOM by the web application and outputted to the browser. If the data is incorrectly handled, an attacker can inject a payload, which will be stored as part of the DOM and executed when the data is read back from the DOM.

Related work

The web-site behavioral mode [2] is a stranded and formal representation of user behavior and web-site structure. This model used to describe legitimate action that web site is permitted to do.

The abstract of the behavior model is as follows at the first it is getting the website source code, then HTML code of all the particular web page of the website is obtained via the execution of website in the website execution simulator then based on the obtained original HTML code for the website, the behavior model is generated

automatically by the automatic modeling method of propose by them as flow.

The general presentation, the website behavior model M that can be presented as the form of quadruple M (s0, A, St, Ss), in here s0 Ss. s0 is the initial state of the website behavior model, St represent all the non-steady state of the behavior model, Ss is representation of all the steady state of the website behavior model, and A represent all the Behaviors of the website behavior model. i.e. there is a A, si, sj St Ss, so that a (si) = sj.

There are many advance studies, investigations and researches have done in the last few years about detecting and preventing XSS issues associated with network application. Along with this research many solutions of XSS vulnerability has invented by researchers but unfortunately XSS threat still happens in both web sites and web applications. Web pages still face various cross site scripting attacks and the most significant is session hijacking, hackers steal the cookie data of victim's user and they may use the same sessions. Tools and instruments are designed to protect the web application security; it characterizes the arrangement that helps developers for building up a secure web application and web site. It says XSS is a result of despicable filtering of user input and proposed cautious expulsion of undesirable scripts or HTML tags that can be executed on the web pages [5].

In this paper provide significant cross site scripting risk. the first is to place to apply a context dependent output encoding. In this case web application need to encode HTML specific characters. In the above table contain HTML opening and closing tag.

Table 1 [6].

TABLE III. COMMON CHARACTERS REPLACING TO DEFEAT XSS

Replace	With
<	&lt
>	&gt
(	&#40
)	&#41
#	&#35

XSS threats can be avoided by validating and checking data that are provided by users to ensure consistence with the required format for web applications, there are four suggested mechanisms for user input validation [7], [8].

- Replacement is a way to search for dangerous user inputs then substitutes those dangerous codes with correct and true characters.
- Removal is a way also to find dangerous inputs but opposed to replacement by removing them.
- Escaping way changes (or marks) key characters of the data to avoid it from being interpreted in a dangerous code.
- Restriction way checks the user inputs to limited non malicious.

OWASP's guide to secure development gives three rules for dealing with user data [9].

• Accept only known valid data

• Reject recognized harmful data

• Clean harmful data

Also in recently use anther method is tool base method [10].

Conclusion

Most people and organization are using web base service for this customer convenience and which are required many information for the user and stored in the web site. These features allow attacker to launch XSS attack and access sensitive information of the user. Many review presenting deferent ways to prevent those type of attack. Mainly secure code development, input validation, web behavioral model and tools base approach. It discussed about various tools for examining the XSS vulnerability and summarizes the preventive measures against XSS.

Acknowledgment

I would like to thank Sri Lanka institute of information technology and Research for providing us the environment to carry out the research work successfully.

References

[1] M. Elkhodr, J. K. Patel, M. Mahdavi, and E. Gide, "Prevention of Cross-Site Scripting Attacks in Web Applications," *Adv. Intell. Syst. Comput.*, vol. 1150 AISC, no. March 2014, pp. 1077–1086, 2020, doi: 10.1007/978-3-030-44038-1_100.

[2] Y. Sun and D. He, "Model checking for the defense against cross-site scripting attacks," *Proc. - 2012 Int. Conf. Comput. Sci. Serv. Syst. CSSS 2012*, pp. 2161–2164, 2012, doi: 10.1109/CSSS.2012.537.

[3] "Stored XSS (Cross-site Scripting) | CISSPAnswers - YouTube." https://www.youtube.com/watch?v=ABwS2MIxFPQ&t=301s (accessed May 15, 2021).

[4] "Reflected XSS (Cross-site Scripting) | CISSPAnswers - YouTube." https://www.youtube.com/watch?v=yJSnggHSH1U&t=188s (accessed May 15, 2021).

[5] T. A. Taha and M. Karabatak, "A proposed approach for preventing cross-site scripting," *6th Int. Symp. Digit. Forensic Secur. ISDFS 2018 - Proceeding*, vol. 2018-Janua, pp. 1–4, 2018, doi: 10.1109/ISDFS.2018.8355356.

[6] A. Singh and S. Sathappan, "A Survey on XSS web-attack and Defense Mechanisms," vol. 4, no. 3, pp. 1160–1164, 2014.

[7] H. Zeng, "Research on developing an attack and defense lab environment for cross site scripting education in higher vocational colleges," *Proc. - 2013 Int. Conf. Comput. Inf. Sci. ICCIS 2013*, pp. 1971–1974, 2013, doi: 10.1109/ICCIS.2013.515.

[8] V. Anupam and A. Mayer, "Secure web scripting," *IEEE Internet Comput.*, vol. 2, no. 6, pp. 46–55, 1998, doi: 10.1109/4236.735986.

[9] Lachlan McGill, "Information Security Reading Room Defense In Depth

[10] P. Anand and J. Ryoo, “Security Patterns As Architectural Solution - Mitigating Cross-Site Scripting Attacks in Web Applications,” *Proc. - 2017 Int. Conf. Softw. Secur. Assur. ICSSA 2017*, pp. 25–31, 2018, doi: 10.1109/ICSSA.2017.30.