Cross-site scripting attacks procedure and Prevention Strategies

Xijun Wang[1,a], Weigang Zhang[1]

[1]*Xuchang Vocational and Technical College, Xinxing Road Xuchang City No. 4336, China*

Abstract. Cross-site scripting attacks and defense has been the site of attack and defense is an important issue, this paper, the definition of cross-site scripting attacks, according to the current understanding of the chaos on the cross-site scripting, analyzes the causes and harm cross-site scripting attacks formation of attacks XXS complete process XSS attacks made a comprehensive analysis, and then for the web program includes Mobility there are cross-site scripting filter laxity given from ordinary users browse the web and web application developers two the defense cross-site scripting attacks effective strategy.

1 Introduction

Cross-site scripting attacks and defense has been an important topic of Defense website, along with attack technology advances, many theories about cross-site scripting attacks cannot meet the needs of today's attack and defense, but also because of the awareness of cross-site scripting confusion, resulting in a lot of programs now include dynamic network there are cross-site scripting filter lax problems.

1.1 Definition of cross-site scripting attacks

XSS (Cross-Site Script, abbreviated XSS) [1] refers to the network of human intruders insert some malicious script code to a dynamic web page, when a user opens these pages, the browser will automatically download malicious code embedded in Web pages inside the malicious script code will be interpreted, an attacker can bypass the document Object model (DOM) of security restrictions, to steal Cookies information, change account settings Web application, Web-mailing worm spread a series of malicious actions, so as to achieve illegal special purpose steal user information.

1.2 Harm cross-site scripting attacks

Cross-site scripting attack is a passive attack in many large portals (such as Yahoo, Microsoft, EBay) are on the existence of such loopholes, it is very popular in hacker circles, the danger should not be overlooked.

Intruder exploit XSS vulnerabilities, with the vulnerable Web sites to attack other visit the related website users, steal user browsing session such as user names and passwords (which may be included in the cookie) sensitive information, execute malicious code inserted by the user hanging horse attack. XSS vulnerabilities can also be used by attackers to tamper pages, but in most cases in order to maximize the economic benefits, the attacker does not directly tampering.

XSS attacks can collect user information [2], the intruder by inserting JavaScript in vulnerable Web applications,VBScript, ActiveX or Flash user information such as deception, once succeeded, you can easily obtain a user account illegally, Further modify user settings, false advertising, view the host information.

XSS attacks can also lead to a denial of service attack. An attacker could use a script to run on a recurring, so a simple message box is enough to cause a Dos attack, so that site administrators keep track of.

XSS attacks can also be combined with browser vulnerabilities, modify the system configuration, view system files, or install a backdoor Trojan and execute malicious code.

1.3 Cross-site scripting attack causes

Web server lack of information entered by the user verify the legitimacy or verification is not enough, and the information entered by the user will be returned to the client is the main cross-site scripting vulnerabilities generation [3], there are two points:

Web Server allows users to irrelevant pages in the table or in the edit box and enter the required characters. As edit box requires the user to enter the phone number, which is valid for a smart digital, any other form of symbols are illegal if the programmer did not verify the validity of this, there is a loophole.

Web server to the user's input is stored and returned to the end user on the page display, the designers did not echo the illegal character filtering or re-encoded. If an attacker entered a seemingly normal but hidden content XSS code, such as adding new users on the Web site, to enhance their permissions, end user browser will accept and execute the code, will be on the Web server Web applications and cause unpredictable hazards.

[a] Corresponding author: rwgwz@163.com

2 Cross-site scripting attacks

Belonging to the passive XSS attacks [4]. Or by e-mail when an attacker to construct a cross-site page, use script, <IMG>, <IFRAME> and other ways to lure users to browse this seemingly normal malicious links or visit the page, the trigger for the attack site is http request attacker returns to the user a web page that contains malicious code, engaged in malicious behavior can be achieved posing issued a document capture multiple attacks object permissions. If the embedded script with an additional capability to interact with other legitimate Web server, an attacker can use it to send an unauthorized request, using the data on the legitimate server. The procedure is shown in Fig.

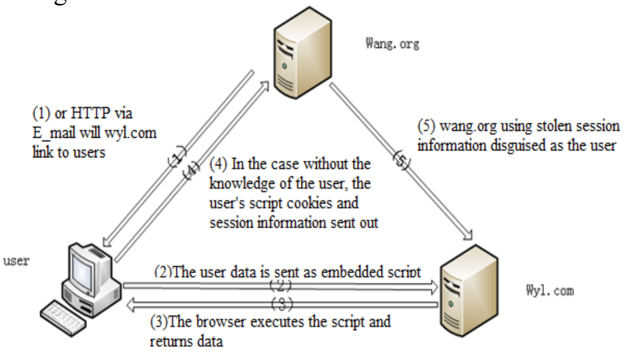
Wang. org
(1) or HTTP via E_mail will wyl.com link to users
(1)
(4)
(4) In the case without the knowledge of the user, the user's script cookies and session information sent out
(5)
(5) wang.org using stolen session information disguised as the user
user
(2)The user data is sent as embedded script
(2)
(3)
(3)The browser executes the script and returns data
Wyl. com

Figure 1. cross-site scripting attacks

In Figure 1, an attacker would first of a seemingly normal HTTP link or by E-mail wyl.com link to the user, the user clicks on the link, the browser will execute script in the user without the knowledge of, and the user cookie and session information is sent to the site wang.org attacker making, then, the attacker will be able to view the private information contained within the cookie and use the information to steal session came disguised as the user with real wyl.com conversation.

3 Cross-site scripting attacks step

A successful cross-site scripting attacks there are two necessary conditions: first, the need cross-site scripting vulnerability web applications; Second, the user needs to click on a link or visit a page [5]. Specific attack process is as follows.

3.1 Found XSS vulnerabilities

At present, people browse the pages are all based on HTML (HTML) created, XSS attack is through to the HTML script code artificially inject malicious scripts, the script is specified HTML tags: <script > </ script>, in the absence of filtering character case, just keep complete and error-free script tag can trigger XSS.

User to display an image in the page, you need to use <img>tag,such as<imgsrc= http://127.0.0.1/wyl_xss.gif">, this time through the browser's task is to explain the img tag to access the src attribute URL address assignment and display pictures, but browser src attribute value assigned does not validate correctly, which resulted in an opportunity for the attacker is known, javascript have a pseudo-URL protocol that allows users to use "javascript:" plus any form of javascript code when the browser loaded this URL, automatically execute the javascript code to form a classic XSS case:<Img src = "javascript: alert ('XSS');">

3.2 Injection of malicious code

Find pages containing XSS vulnerability, the attacker can start trying to write and inject malicious code. The purpose is to inject malicious code when the cheater is visited pages containing this malicious code, attackers can achieve the purpose.

Get cookie typical code:javascript:window.location=' http: //www.xcitc.edu.cn/cgi-bin/cookie.cgi?'+ document. cookie. In which, window.location role is to make the page automatically jump to another page; the role is to read document.cookie cookie, users browse the page, the user's cookie will be read and passed as a parameter to http://www.xcitc.edu.cn/cgi-bin/cookie.cgi,after displaying the contents of the cookie. These malicious code, will be issued a visitor's information to a remote attacker Cookie hands, or to enhance the user's permission to upload arbitrary files and other malicious actions.

If a site for receiving user input pages of <,>, ', "special characters filtering, we need to use coded form into the browser's default .IE uses UNICODE coding, coding scripts can & # ASCII way to write the XSS transcoding support decimal and hexadecimal form, and is assigned value for the property, codes are as follows:javascript: window.location = & # x31http:? //www.xcitc.edu.cn/cgi-bin/cookie.cgi & # x31 + document.cookie

3.3 To deceive the user access

When the attacker malicious code into a web page, the next thing to do is to trick target users to access the malicious page, "indirectly" by the target user to complete the attacker's purpose.

4 Cross-site scripting attacks defense

XSS attack main goal is not the Web server itself, but the logged-on user websites for XSS attack defense, the need for defense from ordinary users browse the web and WEB application developers in two ways.

4.1 Ordinary person browsing the web

Click the link to pay special attention to the site, e-mail or instant messaging software, rice open suspicious links, especially when they appear to contain a HTML script code but cannot be easily opened.

For the XSS vulnerability, no kind of web browser has obvious security benefits, in order to get more security, you can install some browser plug-ins, users should try to access the regular large-scale portal, to avoid access may be a problem site.

There is no absolute safe and effective in the world, the average user should try to avoid visiting suspicious websites, such as the provision of information and hacking tools to crack software, indecent photographs of the site free of charge. These types of sites tend to take advantage of the current browser vulnerabilities to compromise the operating system.

4.2 Web application designer

Should concentrate on submission to all users a reliable input validation. These include submission URL, query keywords, post data, allowing only the use of legitimate characters only accept within a predetermined length range, the characters in the appropriate format, blocking, filtering, or ignore any other things.

Using the session tag (session tokens), the verification code technology to protect users of all confidential information, to avoid being robot automatically be executed or perform other illegal websites.

When developing a web application must support users to submit HTML script code, avoid application security by devastating decline, we must use the relevant technology protected when developing web sites, such as received HTML script code to confirm the contents are properly formatted, contains only minimized, secure tag (absolutely no JavaScript), to remove all references to remote content (especially CSS style sheets and JavaScript) and the like.

To make use of filtering and limiting the input method of XXS attack prevention [6], for all dynamic pages input and output should be encoded, so the maximum to avoid cross-site scripting attacks.

Has been completed for the site, you can filter all the special characters input from the web page by adding a dynamic IIS components. This component can usually intercept the Request goal from ASP pages, the table, cookie, request content strings and procedures for testing, which can effectively prevent cross-site scripting attacks.

5 Conclusion

Cross-site scripting attacks, while a passive attack, but because there are many sites on this loophole, likely to cause leaks and illegal data server to steal, the danger is very large, as long as ordinary users browse the web carefully, WEB applications developers tight design, this attack is difficult to achieve.

References

1. Wang Z.C.,Tonghua Teachers College, 08, P36-37(2012)
2. Cheng J.Q. Zhang Y.Q., Computer Engineering, 06, P49-51(2010)
3. Liu J., Zhang X.Z., Computer Development & Applications, 10, P28-30 (2011)
4. Sun W.Y., Zhang Y.R., Neijiang Science and Technology, 05, P33-34(2010)
5. Li J.M., Guo Y.L., network security and hacker attack and defense, P412-413(Electronic Industry Press,2010)
6. Deng W.W., information network security, 09, P23-25(2007)