Analysis of Cookies Deception and Defending Measures

SHUXIN XU and WEIGANG ZHANG

ABSTRACT
Cookies spoofing is a kind of web-based attack method commonly used by hackers. In this paper, the purpose and working process of Cookies cheating are expatiated. Then, the principle of Cookies cheating, the methods of harms and stealing are analyzed. Then, a simple message to the system to cheat the integrity of the process, and finally gives a broad sense from the Cookies to deceive the script system strategy.

INTRODUCTION
In the beginning of the cookies, as a Web server exists in a subtle, like other conventional network technology inadvertently have a security risk, as a user experience to improve and increase the speed of use of the network appears, but the current Cookies are countless Attackers as a malicious attack in a smart link exists, especially in the Web attacks become mainstream attacks, Cookies outbreak of a huge security risk, so that many seemingly impregnable Web application systems have been drowned in the disaster.

COOKIES OVERVIEW

Definition of Cookies
Cookies refers to some sites in order to identify the user identity, Session tracking and stored in the user's local terminal on the data, these data are usually encrypted. The information of the Cookies is small, about 255 characters, when a user is browsing a site, it stored in the client's random access memory RAM \cite{1}, exit the browser, it is stored in the user's hard drive, Only 4KB hard disk space, usually, when the user ends the browser session, the system will terminate all Cookies.

Cookies are stored in the browser directory in the form of text files. Most of the information in cookies is common, such as each keystroke when browsing a site and the address of the site visited. However, many Web sites use cookies to store the server can read back this information from the browser when the user next comes back to the

ShuXin Xu, Xuchang Vocational Technical College, NO.4336 East Xinxing Road Xuchang City, 461000, China
WeiGang Zhang, Xuchang Vocational Technical College, NO.4336 East Xinxing Road Xuchang City, 461000, China
server for private data such as the registered password, the user name, the credit card number, and so on.

**Use of Cookies**

Cookies application mainly in the following areas:

1. The most typical application is to determine whether the registered user has logged on the site, the user may be prompted whether the next entry into this site is to retain user information in order to simplify the login step.
2. Another important application is the "shopping cart", the user usually in a period of time select different products in the same website different pages, these information will be written Cookies, so that users in the final payment Extract information.
3. The third purpose is to personalize the site, which is one of the most effective users of Cookies. On some Web sites that offer personalized services, if the user has set up his favorite configuration and has cookies stored, the browser will first check if the user has predefined cookies each time the user logs in. If so, Cookies are sent to the server along with the user's request for the page, returning the user-defined page and other relevant information.

**The work process of the Cookies**

Cookies are generally returned to the browser from the server side via HTTPHeader. First, the server uses the Set-Cookies header in the response to create a cookie, and the browser in its request through the Cookies header contains the Cookies have been created, and it will return to the server to complete the browser authentication.

After a browser creates a cookie, the cookie is included in the header for each request made to the site, but for other Web sites which are not sent with, and has been sent by the browser, guide the Cookies expire.

**The hazards of the Cookies**

Everything thing has two sides, Cookies in the convenience of the user at the same time, its specific site stored in a user account and password, to a certain extent, has been a serious crisis of user privacy and security, when they are stolen by illegal users, Can cause unimaginable harm.

**COOKIES ATTACK**

**Cookies Spoofing Principle**

Cookies deceive, is only in the user to do Cookies authentication script system, the attacker by modifying the contents of the Cookies to get the appropriate user permissions, and after a successful landing for further attacks.

Traditional programmers think that although Cookies records the user's account number, password and other information, MD5 is encrypted in the network transmission process, even if the attacker cannot see the specific information, so that is
In fact, the attacker, the interception of Cookies does not need to know the meaning of encrypted characters, as long as the server authentication program loopholes, the attacker only to intercept the Cookies submitted to the server and verified, you can easily posing as legitimate users Login to the site.

Traditional programmers more commonly used security vulnerabilities in the script system login process to determine the code:

```c
Response.cookies(prefix)("logpwd")=logpwd
Response.cookies(prefix)("logtype")=logtype
Response.cookies(prefix)("logcook")=cook if cook>0 then
  Response.cookies(prefix).Expires=date+cook
end if
```

The above code structure is clear, judging process is complete, appears to be very safe, but because there is no judgement on the authenticity of the Cookies, there is a security vulnerability. In the above code, because the server is read directly, and Cookies information is secure by default, and real, and thus ignored the Cookies can be modified locally and forgery, making Cookies simply allow an attacker spoofing an easy invasion.

**The hazard of Cookies spoofing**

Cookies for vulnerabilities, according to the degree of damage caused by the attack, the attacker's attack is divided into two levels of primary and advanced.

Beginning Cookies Spoofing attacks modify the expiration time of Cookies to achieve permanent login, unlimited use of certain restrictions. In some huge websites or private forums, in order to save the limited network resources such as traffic and space, users will be restricted to use some network services (such as uploading space and uploading number of registered users) with relatively large consumption of network resources. These restrictions are basically achieved through the Cookies, for such a script system, a mature attacker by modifying the local Cookies information, to spoof the server, to achieve permanent login and unlimited use of network resources purposes.

Advanced Cookies spoofing attacks is currently popular Cookies deception. For some programmers to write script code the user accounts, passwords, permissions, privacy of information stored in the Cookies, the attacker can steal Cookies for administrators, forum moderators and other advanced users, then worked out the password to successfully obtain permission, or don't even crack passwords, Cookies directly through the script is not perfect flaw, direct access to administrator privileges.

**The ways to steal Cookies**

Cookies are to steal through deception to achieve, generally have the following aspects:

1. Through the script code
   For different scripting systems, there are different script code, but the basic principles are similar. Perl version of the basic code to steal Cookies are as follows:
   ```perl
   $borrowed_info=$ENV{‘QUERY_STRING’};
   $borrowed_info=~S/%([a-fA-F0-9][a-fA-F0-9])/pack(‘c’,hex($1))/eg;
   ```
Open(EVIL_COOKIE_LOG,">>evil_cookie_log") or print “content-type: Text/html\n
 something went wrong\n”;
Print EVIL_COOKIE_LOG “$borrowed_info\n”;  
Print “Content-type: text/html\n\n”;  
Close(EVIL_COOKIE_LOG);

(2) Using flash
Using flash can be achieved in a more advanced environment to steal Cookies. Flash in the getURL () function can automatically open the specified Web page, use this feature can lead users to a site that contains information to steal Cookies. When a forum or blog allows the use of HTML code or flash tags, the attacker can use the technology to collect Cookies code, put it in the forum or blog, and then to the post to take an attractive theme, write interesting of the content, through a large number of visits will soon be able to collect the user's Cookies, to steal the purpose, when the administrator, moderator and other advanced users of these hot posts concerned, the Cookies also stolen, The corresponding permissions.

(3) Using social engineering
When a site's security technology is relatively high, the administrator's security awareness is better, the attacker in order to invade the site, often using the social engineering approach to a small special code that contains a small special code of the flash animation sent to the administrator, once the administrator to open the animation, flash in the code to quietly link to the Internet, open a naked eye can not find the page, to steal the administrator Cookies.

COOKIES DECEPTION STEPS AND IMPLEMENTATION

Typical spoofing steps

First the attacker use a normal user to visit the site, the site registered a password that they know the legitimate user account, of course, its authority is relatively low\[5\]. After successful registration, the attacker to use the normal user login, and see whether the system automatically save and generate Cookies, which is the second need to find the local Cookies storage file. In finding their own Cookies, the attacker through the script system leak some of the normal information, to find high-power user name. After obtaining their own cookies, attackers usually use tools such as IEcookiessView to modify local cookie information, re-submit the modified cookies, cheat the cookies, obtain the administrator or other high-privileged users of the relevant authority.

To sum up, Cookies deception typical steps are:

(1) Locate the code that contains the Cookies spoofing vulnerability.
(2) Access to local users of low-power real-time Cookies information.
(3) The use of the normal function of the script system, access to administrator or other high-privileged user account information.
(4) Structure, submit illegal Cookies information, to achieve the purpose of obtaining high-privileged system to deceive.

Using Cookies spoofing message of the system to achieve

At present, many business websites like product pages and placing a light style of message this program to facilitate interested potential customers to return the
information, so using Cookies spoofing mail system is a technique commonly used by an attacker.

In accordance with the typical attack steps, the attacker first registered a regular user, registration is successful, close all pages, and then just use the account password login, and save the login information in order to locally generate the site Cookies file.

Then the attacker to download and install the IecookiesView tool, in the list to find just saved the message corresponding to the local IecookiesView information, edit the information, the values of the contents of the "useridname" to the administrator, then save the Cookies modify, Web page and then open the page, appeared on the right side of the page "management center" option, that is, access to administrator privileges.

Of course, access to administrator privileges, the attacker often need to upload their own Webshell, in order to achieve further control script system.

**COOKIES DEFRAUDING DEFENSES**

Cookies for the deception of the principles and implementation steps, the need to build a broad sense from the Cookies to deceive the script system, the design ideas are as follows:

(1) Strict protection of the database is not disclosed. Protection of the database is not only not leaked Cookies defense technology in the need to pay attention to security measures, but also other security measures must pay attention to the focus.

(2) The use of a single multi-functional Dell account for routine maintenance, not applicable, less use of the highest authority account. This design idea is to prevent Cookies deception, is a more practical, smart and effective method of prevention for the script to understand the programming is not deep, cannot modify the script system and code layer reinforcement of the administrator.

(3) Strictly block the script system may be submitted to steal Cookies code. In order to achieve normal user interaction functions, the general script system has posted, comments, discussions, comments and other functions, these features allow users to submit or upload some of their own code, procedures, such code may be stealing Cookies code, So, for security reasons, the administrator of the code to be strictly reviewed, or use the filter plug-in, filtering software to filter out some of the illegal information submitted by the user.

(4) Use both Session and Cookies to verify

Cookies are stored on the client side. Attackers can easily acquire or copy them to other computers, while sessions are stored on the server. When the interaction between the user and the Web site ends, the session's life cycle ends. From this level, session of the security than Cookies to be high. On the administrator or site operators, in the server stress and security considerations, the most perfect program is the combination of the two.

**CONCLUSION**

Cookies cheat is through steal, and modified, and forged Cookies of content to cheat Web system, and get corresponding permission or for corresponding permission operation of a attack way, due to exists some cannot change of defects, in with to everyone improve network using speed of while, also was countless attack who using steal user of confidential information, so, from widely meaning Shang building a
prevention Cookies cheat and injected of script system, Cookies attacks can be avoided to a certain extent.

REFERENCES