Analysis Cookies Spoofing Attack and Defense Strategies

Dong-Hui Li
Henan College of Fiscal and Financial, Zhengzhou, Henan, China
llman788@163.com

Keywords: Cookies, Deception, Attack, Prevention Policy.

Abstract. Cookies deception is to steal, modify, forgery Cookies Web content to cheat the system and get the appropriate permission or authority to operate accordingly an attack, this article describes the definition of deception Cookies, usage and work process analysis of the Cookies Cookies deception deception theory and method of stealing, cheating typical attacks against Cookies steps to simulate the identity of the attacker against a simple message of the system implementation process Cookies deception, and then on this basis, given the build a broad sense, from the scripting system to prevent cheating Cookies policy.

Introduction
And other conventional network technologies inadvertently create security risks as a Web server in the presence of a minor part, Cookies in the early stage of development, as an improved user experience, improve network speed using appears and currently been countless Cookies as a malicious attacker in a smart link exists, particularly in the case of Web attacks become mainstream attacks, Cookies burst into a huge security risk, so many seemingly impregnable Web applications have been ruined.

Cookies attacker spoofing attack in many cases do not need effort to inject test directly through Cookies spoofing can be obtained otherwise require a great effort to get the injection administrative privileges.

Cookies Overview

The Definition of Cookies
Cookies are data for some websites in order to identify the user identity, carried Session tracking and stored on the user’s local terminal, the data are usually encrypted. Cookies relatively small amount of information about the 255 characters, when a user is browsing a site, it is stored in the client’s random access memory RAM [1], after exiting the browser, it is stored in the user’s hard drive, only 4KB hard disk space, in general, when a user’s browser session ends, the system will terminate all Cookies.

Cookies in the form of a text file stored in the directory browser, Cookies most of the information is common, every keystroke information and addresses of visited sites, such as when browsing a site, etc., but many Web sites use Cookies to store for personal data registered password, user name, credit card number, etc., when the next time the user back to the server, the server can read this information back from the browser.

Cookies Use
Cookies application in the network by its very nature, the server can use Cookies contain any information to filter the information and regular maintenance, in order to determine the status of the HTTP transmission.
Cookies users mainly reflected in the following aspects:

(1) The most typical application is to determine whether the user has registered visit the website, the user may be prompted whether to enter the next time this site is reserved for user information in order to simplify the login procedure.

(2) Another important application is the “shopping cart” like the process, users will generally choose different goods in different pages a period of time with a site, this information is written Cookies, so that when the user last payment extract information.

(3) The third purpose is to deal with personal web site, which is one of the most effective Cookies users. On some Providing personalized service’s website, if the user has set their favorite configuration, and storage of Cookies, each time a user logs on to the site, the browser first checks whether the user has Cookies pre-defined, and if so, Cookies and users will be sent with a request for a web page to the server, it returns the user to define their own pages and other relevant information.

**Cookies Work Process**

Cookies usually by HTTPHeader returned from the server to the browser [2]. First, the server-side use in response Set-Cookies header to create a Cookies, then the browser in its request by Cookies Cookies header includes this has been created, and returns it to the server, thereby completing the browser authentication.

After you create a browser Cookies, for each request for the site, and will be included in the Header in the Cookies, but to seek other websites which are not sent along, and the browser will always send this guide Cookies expired until.

**Cookies Hazards**

There are two sides to everything, Cookies for user convenience, it is stored on a particular site user accounts and passwords, to some extent has been a serious crisis in the user’s privacy and safety when it is stolen unscrupulous users it can cause harm unimaginable.

**Cookies Spoofing Attack**

**Cookies Deceive Principle**

Cookies deception, that is, only the user authentication Cookies do scripting system, an attacker by modifying the contents of Cookies way to get the appropriate user permissions, and after a successful landing for further attacks.

The traditional programmer that although Cookies records the user’s account, password and other information, but the network transmission is encrypted via MD5, even if the attacker can not get to see specific information, it is considered to be safe [3]. In fact, for the attacker to intercept Cookies do not need to know the meaning of encrypted characters, as long as the server authentication program vulnerabilities, an attacker simply cut to obtain Cookies submitted to the server and verified, you can easily impersonate legitimate users Login site.

Traditional programmers commonly used security vulnerabilities scripting system login process to determine the code:

```plaintext
If userlogin = false then dl = ‘Login failed’ mess = mess & “return to re-fill” else
Response.cookies (prefix) ( “logname”) = logname
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
```
Although the above code structure clear, comprehensive judging process, it seems very safe, but because there is no judgment on the authenticity of Cookies, there is a security vulnerability. In the above code, because the server is directly read, and the default Cookies information is secure and true, to the neglect of the local Cookies can be modified and forged, an attacker very easily simply by spoofing Cookies invasion.

**Cookies Deception Hazards**

Cookies for vulnerabilities, according to the degree of harm caused by the attack, attackers divided into junior and senior two levels.

The primary purpose of Cookies Cookies spoofing attacks by modifying the expiration time, in order to achieve permanent login, unlimited use of certain limiting function [4]. On some huge web platform or private forum, in order to save traffic, space limited network resources, go through the procedure to limit users to certain network resources consumed relatively large network services (such as registered users to upload and upload space number, etc.) these restrictions are basically achieved through Cookies, scripts for such systems, sophisticated attackers Cookies by modifying the local information, to deceive the server, log on to achieve a permanent and unlimited use of network resources.

Advanced Cookies spoofing is currently popular Cookies deception. Some programmers when writing the script for the code user accounts, passwords, permissions and other private information stored in the Cookies in the phenomenon, an attacker can use to steal administrator, forum moderators and other advanced users Cookies, and then break out the way passwords successfully obtained permission, or do not even crack the code directly verified by imperfect defect Cookies script, access to administrator privileges directly.

**Steal Cookies Manner**

Cookies are stealing through deception to achieve, implement generally have the following aspects.

1. Through script code
   Scripts for different systems, there are different script code, but the basic principle is similar. Perl version steal Cookies basic code is as follows:
   ```perl
   $Borrowed_info = $ENV{'QUERY_STRING'};
   $Borrowed_info =~ s/%([a-fA-F0-9][a-fA-F0-9])/{hex($1)}/eg;
   Open(EVIL_COOKIE_LOG, ">> evil_cookie_log") or print "content-type:
Text/html

something went wrong"
;
Print EVIL_COOKIE_LOG "$borrowed_info
";
Print "Content-type: text/html"

Close(EVIL_COOKIE_LOG);
```

2. Use flash
   The use of flash can be achieved at higher ambient steal Cookies. Flash in the getURL () function can automatically open the specified web page, the user can use this feature to steal Cookies contain information directed to a Web site. When a forum or blog allows the use of HTML code or flash label, the attacker can use the code above technique to collect Cookies, and put it in a forum or blog, and then to take a post appealing theme, write interesting content, access through a large number of users will soon be able to collect the Cookies, to achieve the purpose of theft, when the administrators, moderators and other advanced users of these fiery posts were concerned, it was stolen Cookies also to obtain the appropriate permissions.
(3) Use of social engineering

Social engineering to its essence, it is a fraud, when a site’s security and defense technology is relatively high, relatively good safety awareness administrator when an attacker to invade the site, often using social engineering approach will contain a small special code exquisite flash animation transferred to the administrator, the administrator once to open the animation, flash in the code will quietly link the Internet, open a naked eye simply can not find the page, thus steal the administrator’s Cookies.

Cookies Deception Steps and Achieve

Typical Deception Step

Attacker first to a normal user to access the site, register on the website they know a valid user account password, of course, its authority is relatively low [5]. After successful registration, an attacker using the user log in, and see if the system will automatically save and generate Cookies, which is the second portion of Cookies need to find a local store files. Cookies find his post, some of the normal information attacker script storm drain system, and find the right high user name. Attackers get their own Cookies, the commonly used tools such as IECookiesView, modify the local Cookies information using code verification lax defect resubmit modified Cookies information, the Cookies deception to obtain administrator or other highly privileged users related rights.

Typical steps sum up, Cookies deception is:
1. Find the code stored Cookies spoofing vulnerability.
2. To obtain a low-privileged users instant Cookies local information.
3. The use of scripting system to normal function, access to the administrator or other high-privilege user account information.
4. Construction, illegal Cookies submit information, to cheat the system to obtain highly privileged purposes.

Use Cookies Spoofing Message of This System Implementation

Currently, many business sites like placing a light style after the product page message this program to facilitate the potential customers are interested in immediate returns information. As the function of such a simple message of this code is not very standardized, there are many loopholes, so the use of Cookies spoofing message of this system is a common practice of the attacker.

Typical steps in accordance with the attack, the attacker first register a regular user, registration is successful, turn off all the pages, then use just registered account password, and save login information in order to generate this site Cookies files locally.

The attacker then download and install IECookiesView tools to find just save the message system corresponding local IECookiesView information in the list, edit the information, the contents of the values in the value “useridname” to an administrator, and then save Cookies changes and close web page and then open the page, the page will appear to the right of the options “management center”, which gained administrator privileges.

Of course, after obtaining administrator privileges, an attacker who often need to upload your own Webshell, in order to achieve the purpose of further control scripting system.

This method is only suitable system only judge Cookies username to give permission message of this program, most of the message of the need to construct a specific program content and breakthrough Cookies multiple authentication before they can successfully deceive.

Cookies Spoofing Defense

In essence, the root causes of Cookies deception is generated script, the script is the program development programmers presence of various security risks that led to these attacks, the most fundamental method of defense is to start from the programmer, however, due to the lack of
planning script level code standards, defense technology behind the attack techniques and people tend to make mistakes and other factors, can not be completely Cookies spoofing attack defense can only be avoided in the larger context.

Cookies for the principle of deception and implementation steps, need to build a system to prevent the script from Cookies spoofing a broad sense, design ideas as follows:

(1) Cookies are not stored sensitive information. This is an idealized idea, and its essence is to abandon Cookies, but obviously a security breach platform design ideas, not because Cookies possible spoofing attack and abolish its convenience.

(2) Strict protection of databases does not leak. Not just to protect the database leaked Cookies defense technology security measures that need attention, as well as other security measures that must be the focus of attention.

(3) Using a single multi-function special accounts del routine maintenance, NA, less the highest privilege account. The design ideas alone prevent Cookies deception, it is more practical, smart and effective prevention methods, suitable for deep understanding of scripting, the script can not modify system administrators and code layer reinforcement.

(4) Strict script blocking system may be submitted steal Cookies code. In order to achieve normal user interactive features, general scripting system has posted, comments, discussions, comments and other features that allow users to submit or upload some of your own code, programs, such code is likely to steal code Cookies Therefore, for security reasons, the administrator to conduct rigorous review of the code, or use a filter plug-filtering software to filter some illegal information submitted by the user.

(5) Two-factor authentication using Session and Cookies

   Session and Cookies purpose is different, Cookies stored in the client, an attacker can easily obtain or copied to other computers, and Session stored in the server side, when the end user’s interaction with the website, Session life cycle is then terminated from this level, say, Session security than Cookies higher. On administrator or site operators, and the pressure in the server security considerations, the perfect solution is to use a combination of both.

Conclusion

Cookies by deception to steal, modify, counterfeit Web content Cookies to deceive the system, and get the appropriate authority or the appropriate permissions to carry out an attack mode operation, since there are some defects can not be changed, to bring you in improving network usage rate at the same time, many also exploited by attackers to steal user’s confidential information, therefore, to build a defense Cookies spoofing and script injection system in a broad sense, you can avoid being attacked Cookies certain extent.

References


