Global Information Assurance Certification Paper

Cookies and Exploits

Jasmir Beciragic

Sweden

Summary

There are many questions and discussions about cookies. What are cookies? Are there any security risks with cookies? Cookies and security. Cookies and privacy.

I have investigated two cookie exploi ts and will express the common characteristics of the investigated exploits.

HTTP Cookie Protocol

According to [1], HTTP cookies are mechanism for maintaining state between clients and origin servers. A cookie is a very small text file placed on your ha rd drive by a Web Page server [2]. The complete specification of the HTTP Cookie protocol is in RFC 2109 [3] and a simple communication between web -browser and web-server shows the next example:

1. web-browser -> web-server (get request without cookie)

```
HTTP: Line  1:  GET / HTTP/1.0
HTTP: Line  2:  Referer: http://dir.altavista.com/Top/News/Newspapers
HTTP: Line  3:  Connection: Keep -Alive
HTTP: Line  4:  User -Agent: Mozilla/4.5 [sv] (WinNT; I)
HTTP: Line  5:  Host: hrticket.co m
HTTP: Line  6:  Accept: image/gif, image/x  -xbitmap, image/jpeg, image/pjpeg,
HTTP:           image/png, */*
HTTP: Line  7:  Accept -Encoding: gzip
HTTP: Line  8:  Accept -Language: sv
HTTP: Line  9:  Accept -Charset: iso-8859-1,*,utf-8
```

2. web-server -> web-browser (set-cookie)

```
HTTP: Line  1:  HTTP/1.1 200 OK
HTTP: Line  2:  Server: Netscape -Enterprise/3.5.1G
HTTP: Line  3:  Date: Tue, 25 Jul 2000 11:52:33 GMT
HTTP: Line  4:  Set-cookie: NGUserID=cdb43e6e -6705-964525953-1; expires=Wedn
HTTP:           esday, 30 -Dec-2037 16:00:00 GMT; path=/
HTTP: Line  5:  Content -type: text/html
```

3. web-browser -> web-server (get requests with cookie)

```
HTTP: Line  1:  GET /hrticket/pix/sidebar3.gif HTTP/1.  0
HTTP: Line  2:  Referer: http://hrticket.com/
HTTP: Line  3:  Connection: Keep -Alive
HTTP: Line  4:  User -Agent: Mozilla/4.5 [sv] (WinNT; I)
```

HTTP: Line 5: Host: hrticket.com
HTTP: Line 6: Accept: image/gif, image/x -xbitmap, image/jpeg, image/pjpeg
HTTP: image/png
HTTP: Line 7: Accept -Encoding: gzip
HTTP: Line 8: Accept -Language: sv
HTTP: Line 9: Accept -Charset: iso-8859-1,*,utf-8
HTTP: Line 10: Cookie: NGUserID=cdb43e6e -6705-964525953-1

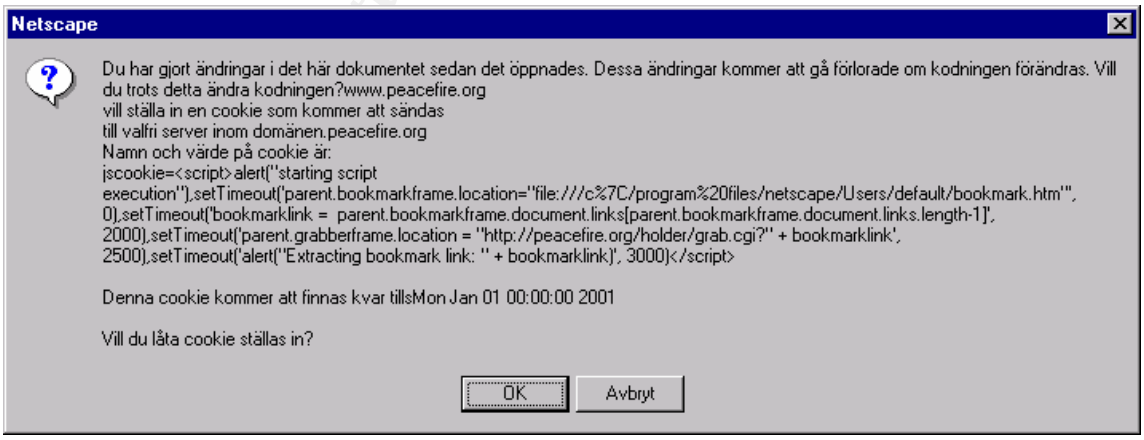
or next

HTTP: Line 1: GET /hrticket/pix/blkbar.gif HTTP/1.0
HTTP: Line 2: Referer: http://hrticket.com/
HTTP: Line 3: Connection: Keep -Alive
HTTP: Line 4: User -Agent: Mozilla/4.5 [sv] (WinNT; I)
HTTP: Line 5: Host: hrticket.com
HTTP: Line 6: Accept: image/gif, image/x -xbitmap, image/jpeg, image/pjpeg
HTTP: image/png
HTTP: Line 7: Accept -Encoding: gzip
HTTP: Line 8: Accept -Language: sv
HTTP: Line 9: Accept -Charset: iso-8859-1,*,utf-8
HTTP: Line 10: Cookie: NGUserID=cdb43e6e -6705-964525953-1

Exploits

I have picked out two cookie exploits:
- JavaScript-in-cookies - Netscape Communicator 4.x [4],
- Open Cookie Jar - Internet Explorer [5].

JavaScript-in-cookies works by setting a cookie whose value contains JavaScript code. Below is a warning of the Netscape Communicator, for the JavaScript -in-cookies.



Open Cookie Jar uses a specially constructed URL. The following is a sniffer trace of the Open Cookie Jar, with "Your DoubleClick ad -banner id=dd43f713" [6].

HTTP: Line 1: POST /exploit/exploit_1f.html HTTP/1.1

```
HTTP: Line  2:  Accept: application/vnd.ms  -excel, application/msword, applic
HTTP:           ation/vnd.ms -powerpoint, image/gi f, image/x -xbitmap, image/j
HTTP:           peg, image/pjpeg, */*
HTTP: Line  3:  Referer: http://www.securityspace.com%2fexploit%2fexploit_1e
HTTP:           .html%3fa=.doubleclick.net/
HTTP: Line  4:  Content -Type: application/x -www-form-urlencoded
HTTP: Line  5:  Accept -Encoding: gzip, deflate
HTTP: Line  6:  User -Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows NT)
HTTP: Line  7:  Host: www.securityspace.com
HTTP: Line  8:  Content -Length: 47
HTTP: Line  9:  Connection: Keep -Alive
HTTP: Line 10:
HTTP: Line 11:  cookie=1&source=doubleclick.net&c=id%3Ddd43f713
```

The common characteristics of the cookie exploits are:

Exploit	How it works	Impact	Restrictions
JavaScript-in-cookies	The exploit works by setting a cookie whose value contains JavaScript code.	Web site can read HTML files on a user's hard drive.	The hostile site must know the path name of the Communicator installation directory and the user's profile name (such as "default").
Open Cookie Jar	The exploit use a specially constructed URL.	Web site can read Internet Explorer cookies set from any domain.	No.

Conclusion

First, I describe the HTTP Cookie Protocol and then show the common characteristics of the cookie exploits.

The cookie exploits use HTTP Cookie Protocol. There are patches for both cookie exploits. It is not problem with cookie, there is a problem with security holes in the web browsers.

References:

[1] Luotonen, Ari. “Web Proxy Servers.” Prentice Hall.
[2] URL: http://www.microsoft.com/info/cookies.htm.
[3] Kristol, D., Montulli, L., “ HTTP State Management Mechanism.” February 1997.
[4] URL: http://peacefire.org/security/jscookies/
[5] URL: http://www.peacefire.org/security/iecookies/
[6] URL: http://www.securityspace.com/exploit/exploit_1c.html/

Last Updated: April 22nd, 2018

Upcoming Training

SANS Seattle Spring 2018	Seattle, WA	Apr 23, 2018 - Apr 28, 2018	Live Event
Mentor Session - AW SEC401	Detroit, MI	May 01, 2018 - May 17, 2018	Mentor
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VA	May 20, 2018 - May 25, 2018	Live Event
SANS Atlanta 2018	Atlanta, GA	May 29, 2018 - Jun 03, 2018	Live Event
Community SANS Bethesda SEC401	Bethesda, MD	Jun 04, 2018 - Jun 09, 2018	Community SANS
Community SANS New York SEC401	New York, NY	Jun 04, 2018 - Jun 09, 2018	Community SANS
SANS London June 2018	London, United Kingdom	Jun 04, 2018 - Jun 12, 2018	Live Event
SANS Rocky Mountain 2018	Denver, CO	Jun 04, 2018 - Jun 09, 2018	Live Event
Community SANS Madison SEC401	Madison, WI	Jun 18, 2018 - Jun 23, 2018	Community SANS
SANS Crystal City 2018	Arlington, VA	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Cyber Defence Japan 2018	Tokyo, Japan	Jun 18, 2018 - Jun 30, 2018	Live Event
SANS Oslo June 2018	Oslo, Norway	Jun 18, 2018 - Jun 23, 2018	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 18, 2018 - Jun 23, 2018	Community SANS
Minneapolis 2018 - SEC401: Security Essentials Bootcamp Style	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	vLive
Community SANS Nashville SEC401	Nashville, TN	Jun 25, 2018 - Jun 30, 2018	Community SANS
SANS Minneapolis 2018	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Cyber Defence Canberra 2018	Canberra, Australia	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS Vancouver 2018	Vancouver, BC	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, United Kingdom	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, Singapore	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Charlotte 2018	Charlotte, NC	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DC	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Malaysia 2018	Kuala Lumpur, Malaysia	Jul 16, 2018 - Jul 21, 2018	Live Event
SANSFIRE 2018 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 16, 2018 - Jul 21, 2018	vLive
Mentor Session - SEC401	Jacksonville, FL	Jul 17, 2018 - Aug 28, 2018	Mentor
Community SANS Bethesda SEC401	Bethesda, MD	Jul 23, 2018 - Jul 28, 2018	Community SANS
SANS Pittsburgh 2018	Pittsburgh, PA	Jul 30, 2018 - Aug 04, 2018	Live Event
SANS Boston Summer 2018	Boston, MA	Aug 06, 2018 - Aug 11, 2018	Live Event
San Antonio 2018 - SEC401: Security Essentials Bootcamp Style	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	vLive
SANS August Sydney 2018	Sydney, Australia	Aug 06, 2018 - Aug 25, 2018	Live Event