



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"Security Essentials Bootcamp Style (Security 401)"  
at <http://www.giac.org/registration/gsec>

---

## 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 exploits 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 hard 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 -bitmap, 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

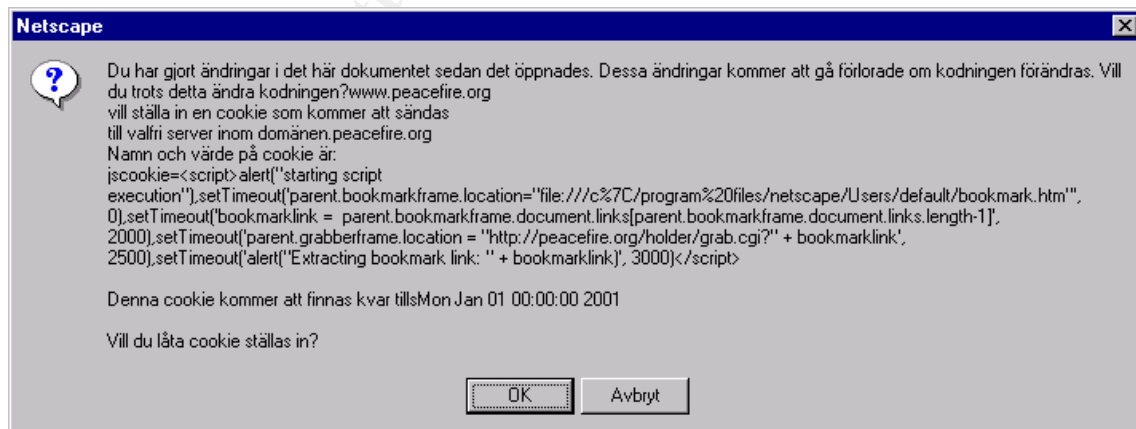
```
HTTP: Line 1: GET /hrticket/pix/blkbar.gif HTTP/1.0
HTTP: Line 2: Referer: http://hrticket.com/
HTTP: Line 3: Connection: Keep -Alive
HTTP: Line 4: User-Agent: Mozilla/4.5 [sv] (WinNT; I)
HTTP: Line 5: Host: hrticket.com
HTTP: Line 6: Accept: image/gif, image/x -xbitmap, image/jpeg, image/pjpeg
HTTP:      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, application/vnd.ms-powerpoint, image/gif, image/x-bitmap, image/jpeg, image/png, \*/\*  
 HTTP: Line 3: Referer: http://www.securityspace.com%2fexploit%2fexploit\_1c.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/](http://www.securityspace.com/exploit/exploit_1c.html/)

# Upcoming Training

Click Here to  
**{Get CERTIFIED!}**



Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401*	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Oct 03, 2017 - Nov 14, 2017	Mentor
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
Community SANS Omaha SEC401	Omaha, NE	Oct 23, 2017 - Oct 28, 2017	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Colorado Springs SEC401**	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401*	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event