



# 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

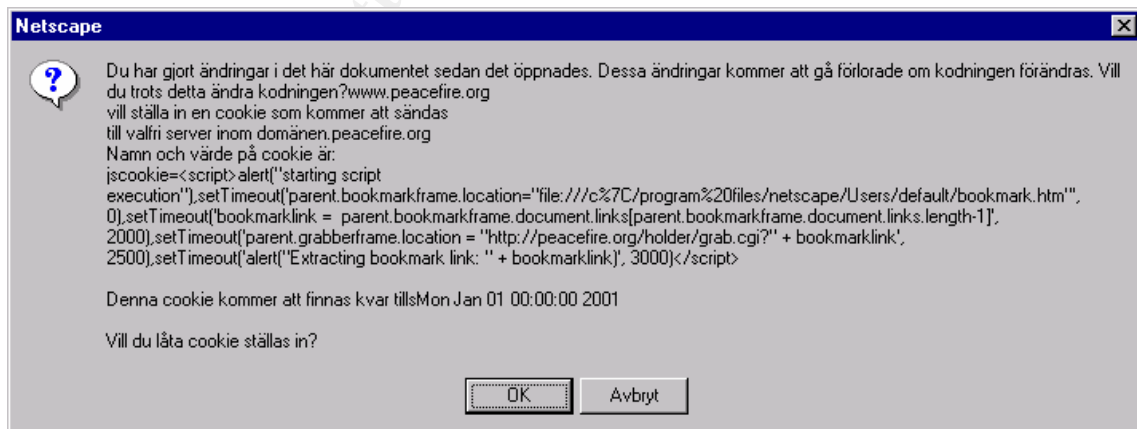
```
HTTP: Line 1: GET /hrticket/pix/blkbar.gif HTTP/1.0
HTTP: Line 2: Referer: http://hrticket.com/
HTTP: Line 3: Connection: Keep -Alive
HTTP: Line 4: User-Agent: Mozilla/4.5 [sv] (WinNT; I)
HTTP: Line 5: Host: hrticket.com
HTTP: Line 6: Accept: image/gif, image/x -xbitmap, image/jpeg, image/pjpeg
HTTP:      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!}**



SANS Vancouver 2018	Vancouver, BC	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	Live Event
Community SANS Nashville SEC401	Nashville, TN	Jun 25, 2018 - Jun 30, 2018	Community SANS
SANS Cyber Defence Canberra 2018	Canberra, Australia	Jun 25, 2018 - Jul 07, 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
SANSFIRE 2018	Washington, DC	Jul 14, 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 Annapolis Junction SEC401	Annapolis Junction, MD	Jul 23, 2018 - Jul 28, 2018	Community SANS
SANS Riyadh July 2018	Riyadh, Kingdom Of Saudi Arabia	Jul 28, 2018 - Aug 02, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PA	Jul 30, 2018 - Aug 04, 2018	Live Event
San Antonio 2018 - SEC401: Security Essentials Bootcamp Style	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	vLive
SANS San Antonio 2018	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, India	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS Boston Summer 2018	Boston, MA	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS August Sydney 2018	Sydney, Australia	Aug 06, 2018 - Aug 25, 2018	Live Event
Mentor Session - SEC401	Ankara, Turkey	Aug 08, 2018 - Oct 03, 2018	Mentor
Northern Virginia- Alexandria 2018 - SEC401: Security Essentials Bootcamp Style	Alexandria, VA	Aug 13, 2018 - Aug 18, 2018	vLive
SANS Northern Virginia- Alexandria 2018	Alexandria, VA	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS New York City Summer 2018	New York City, NY	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VA	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS Chicago 2018	Chicago, IL	Aug 20, 2018 - Aug 25, 2018	Live Event
Mentor Session AW - SEC401	Raleigh, NC	Aug 22, 2018 - Aug 29, 2018	Mentor
SANS San Francisco Summer 2018	San Francisco, CA	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, Japan	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, Netherlands	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FL	Sep 04, 2018 - Sep 09, 2018	Live Event
SANS Baltimore Fall 2018	Baltimore, MD	Sep 08, 2018 - Sep 15, 2018	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201809,	Sep 11, 2018 - Oct 18, 2018	vLive
SANS Munich September 2018	Munich, Germany	Sep 16, 2018 - Sep 22, 2018	Live Event