



# 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

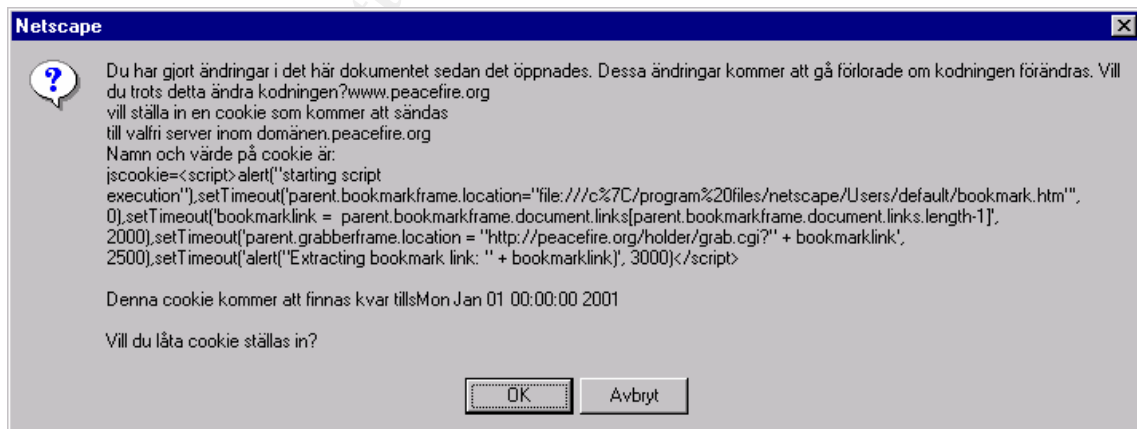
```
HTTP: Line 1: GET /hrticket/pix/blkbar.gif HTTP/1.0
HTTP: Line 2: Referer: http://hrticket.com/
HTTP: Line 3: Connection: Keep -Alive
HTTP: Line 4: User-Agent: Mozilla/4.5 [sv] (WinNT; I)
HTTP: Line 5: Host: hrticket.com
HTTP: Line 6: Accept: image/gif, image/x -xbitmap, image/jpeg, image/pjpeg
HTTP:      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 Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event