



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

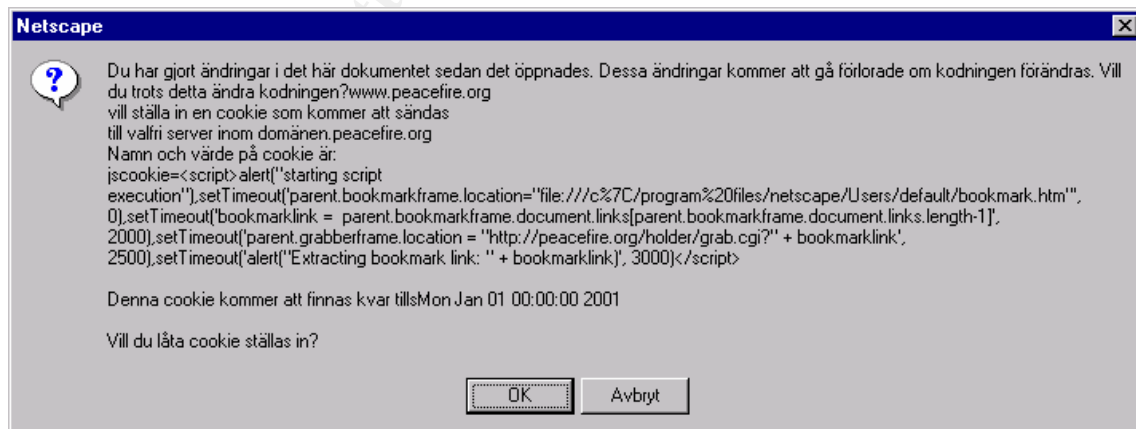
```
HTTP: Line 1: GET /hrticket/pix/blkbar.gif HTTP/1.0
HTTP: Line 2: Referer: http://hrticket.com/
HTTP: Line 3: Connection: Keep -Alive
HTTP: Line 4: User-Agent: Mozilla/4.5 [sv] (WinNT; I)
HTTP: Line 5: Host: hrticket.com
HTTP: Line 6: Accept: image/gif, image/x -xbitmap, image/jpeg, image/pjpeg
HTTP: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

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS Miami 2019	Miami, FL	Jan 21, 2019 - Jan 26, 2019	Live Event
SANS Las Vegas 2019	Las Vegas, NV	Jan 28, 2019 - Feb 02, 2019	Live Event
Mentor Session - SEC401	Richmond, VA	Jan 31, 2019 - Mar 14, 2019	Mentor
SANS Security East 2019	New Orleans, LA	Feb 02, 2019 - Feb 09, 2019	Live Event
Security East 2019 - SEC401: Security Essentials Bootcamp Style	New Orleans, LA	Feb 04, 2019 - Feb 09, 2019	vLive
SANS Anaheim 2019	Anaheim, CA	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Northern VA Spring- Tysons 2019	Vienna, VA	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS New York Metro Winter 2019	Jersey City, NJ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Dallas 2019	Dallas, TX	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Secure Japan 2019	Tokyo, Japan	Feb 18, 2019 - Mar 02, 2019	Live Event
SANS Scottsdale 2019	Scottsdale, AZ	Feb 18, 2019 - Feb 23, 2019	Live Event
Open-Source Intelligence Summit & Training 2019	Alexandria, VA	Feb 25, 2019 - Mar 03, 2019	Live Event
SANS Reno Tahoe 2019	Reno, NV	Feb 25, 2019 - Mar 02, 2019	Live Event
Mentor Session @Work - SEC401	Raleigh, NC	Feb 27, 2019 - Mar 06, 2019	Mentor
SANS Baltimore Spring 2019	Baltimore, MD	Mar 02, 2019 - Mar 09, 2019	Live Event
Baltimore Spring 2019 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Mar 04, 2019 - Mar 09, 2019	vLive
SANS Secure India 2019	Bangalore, India	Mar 04, 2019 - Mar 09, 2019	Live Event
Community SANS Indianapolis SEC401	Indianapolis, IN	Mar 04, 2019 - Mar 09, 2019	Community SANS
SANS Secure Singapore 2019	Singapore, Singapore	Mar 11, 2019 - Mar 23, 2019	Live Event
SANS San Francisco Spring 2019	San Francisco, CA	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS London March 2019	London, United Kingdom	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS St. Louis 2019	St. Louis, MO	Mar 11, 2019 - Mar 16, 2019	Live Event
Mentor Session - SEC401	Fredericksburg, VA	Mar 12, 2019 - May 14, 2019	Mentor
SANS Munich March 2019	Munich, Germany	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Secure Canberra 2019	Canberra, Australia	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Norfolk 2019	Norfolk, VA	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201903,	Mar 19, 2019 - Apr 25, 2019	vLive
SANS 2019	Orlando, FL	Apr 01, 2019 - Apr 08, 2019	Live Event
SANS 2019 - SEC401: Security Essentials Bootcamp Style	Orlando, FL	Apr 01, 2019 - Apr 06, 2019	vLive
Community SANS Raleigh SEC401	Raleigh, NC	Apr 01, 2019 - Apr 06, 2019	Community SANS
SANS London April 2019	London, United Kingdom	Apr 08, 2019 - Apr 13, 2019	Live Event