

Net-Square Security Advisory:	NS-310107-ORKUT
Date of advisory draft:	08 February, 2006
Release Date:	31 January, 2007
Affected Application:	Orkut.com
Type:	Multiple problems in server-side session handling
Severity:	Medium
Status:	Corrected by Google on 05 January, 2007
Authors:	Pallav Khandhar <pallav at net-square dot com> Saumil Shah <saumil at net-square dot com>
Publication URL:	http://net-square.com/advisory/NS-310107-ORKUT.pdf

OVERVIEW

1. Orkut fails to expire the orkut_state session cookie from the server side even when the user logs off from Orkut upon clicking "Sign-Out" from the application. The cookie is cleared from the client side (browser), but is not cleared from the server side. If re-used, it provides access to the user's Orkut account.
2. Upon logging in again, a new orkut_state session cookie is created, but the old session cookies still stay active on the server side. Therefore, any session cookie can be re-used to gain access to the user's Orkut account.

DETAILED DESCRIPTION

Upon successful authentication to Orkut, Orkut sets a session cookie named orkut_state. The orkut_state cookie is set to expire at the end of the browser session. Upon logging off from Orkut via the "Logout" link, the orkut_state session cookie is cleared from the browser's cookie memory.

However, the orkut_state cookie entry stays active on the server side. If a valid okut_state cookie is re-used, even after logging off, Orkut allows access to that user's mail account. Net-Square has tested that orkut_state session cookies stay active indefinitely. Our testing has shown that it was possible to successfully re-use an orkut_state session cookie for a period of two weeks since its creation.

Secondly, Orkut does not seem to check for duplicate or multiple orkut_state cookies being sent in the same HTTP request. It is possible to send a number of orkut cookies in the same HTTP request and yet gain access to a user's Orkut account, with at least one of the orkut_state cookies belonging to a valid session some time in the past.

The best practices for session handling would involve expiry of all session related cookies and tokens from the server side, as well as an attempt to clear them from the client side. Server side sessions should also be checked for periods of inactivity. If there is no user activity detected for a pre-defined period of time, the application should clear the session cookie and variables.

PROOF OF CONCEPT

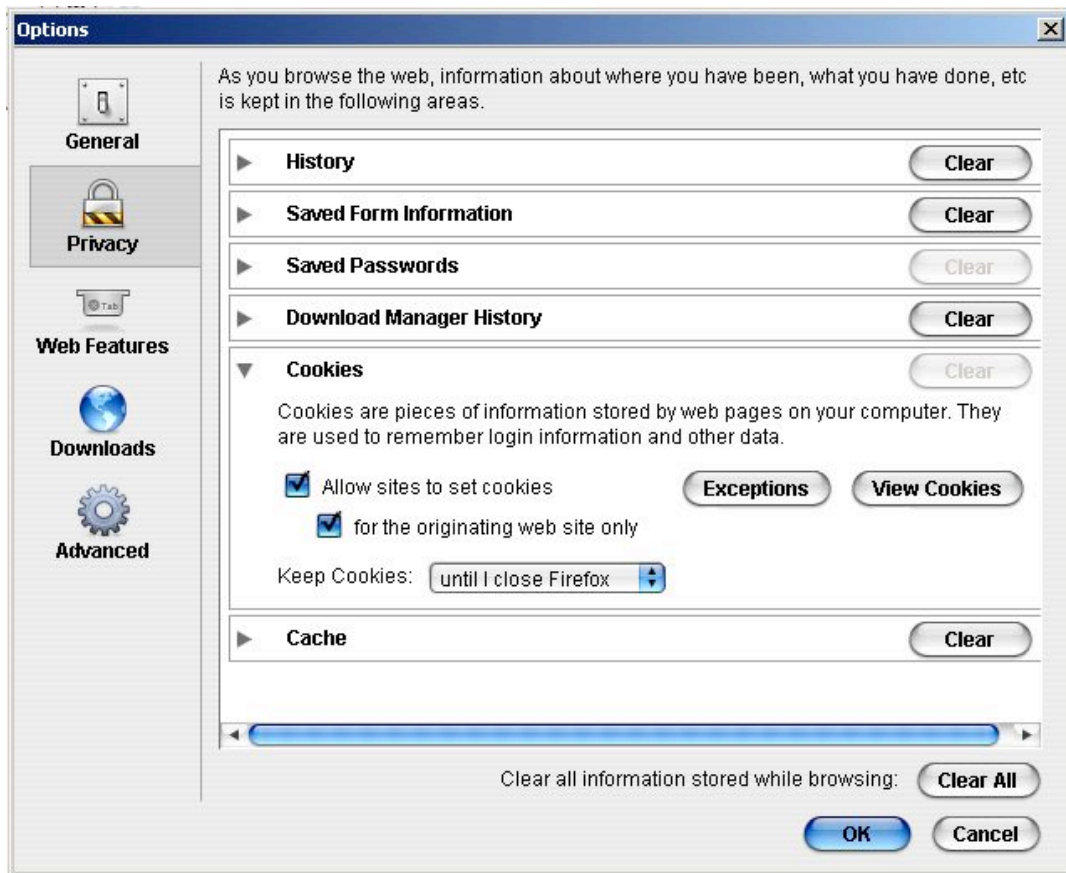
We have used an account "netsquare.test" for demonstrating these vulnerabilities. Testing was performed with Mozilla Firefox 1.5 with the following privacy settings, as shown in figure 1.

Options > Privacy > Cookies

"Allow sites to set cookies" is checked on.

"for the originating web site only" is checked on.

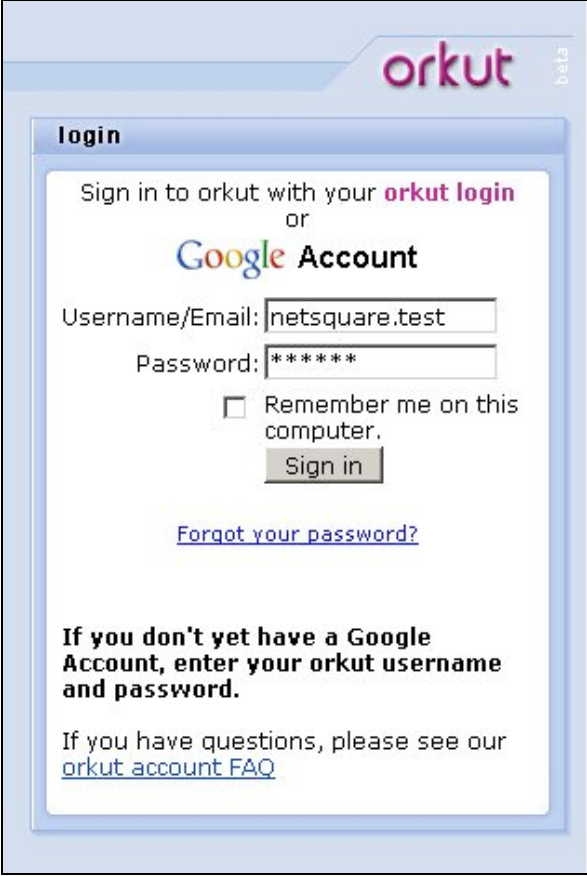
Keep cookies "until I close Firefox".



The above settings ensure that all cookies are cleared every time the browser is shut down.

Step 1: Login to Orkut

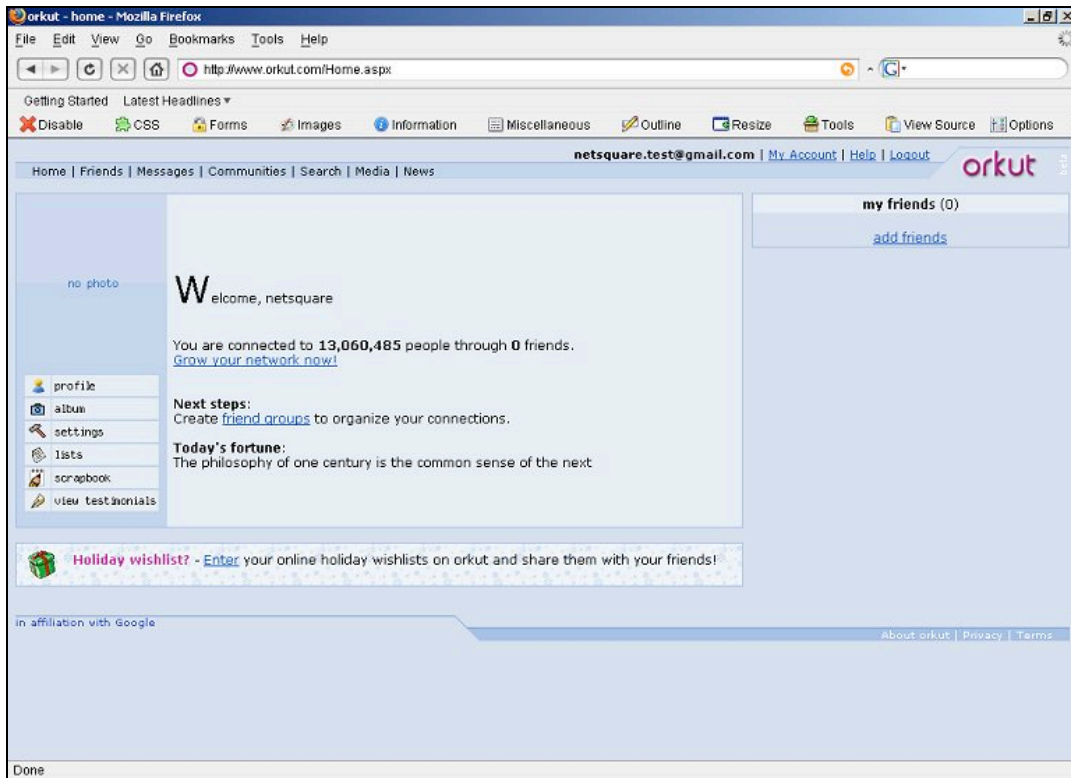
Open the URL <http://www.orkut.com/> and enter your username and password.



The screenshot shows the Orkut login page. At the top right, the Orkut logo is displayed in purple, with the word "beta" written vertically next to it. Below the logo, the word "login" is written in a blue box. The main content area is white and contains the following text: "Sign in to orkut with your **orkut login** or **Google Account**". Below this, there are two input fields: "Username/Email:" with the value "netsquare.test" and "Password:" with the value "*****". A checkbox labeled "Remember me on this computer." is present below the password field. A "Sign in" button is located below the checkbox. A link for "Forgot your password?" is positioned below the "Sign in" button. At the bottom of the form, there is a bold instruction: "If you don't yet have a Google Account, enter your orkut username and password." and a link for "orkut account FAQ".

After a couple of redirections, the browser will be pointing to the main Orkut login page at:

<https://www.orkut.com/Home.aspx...>

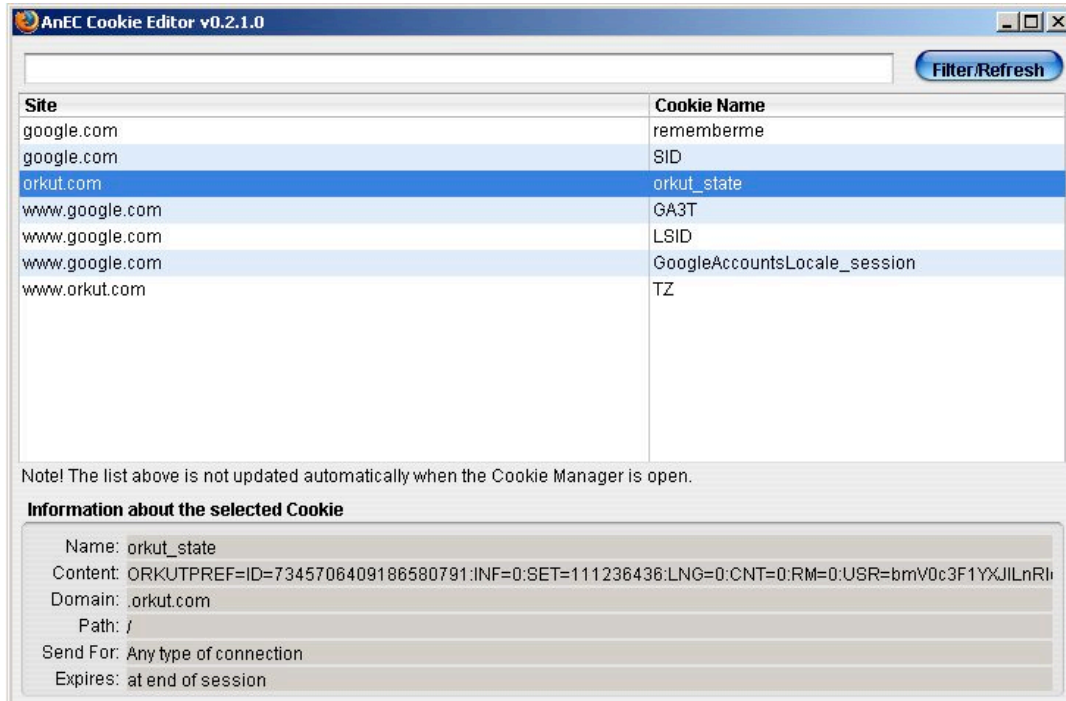


Step 2: Inspect cookies

After logging in, if we view the cookies currently set in our browser, we find the following two cookies set for "*.orkut.com":

```
orkut_state  
TZ
```

The figure below shows the cookies set in our browser:



The orkut_state cookie is a session cookie, which is set to expire whenever the browser terminates.

In our test, the orkut_state cookie observed was:

```
orkut_state=ORKUTPREF=ID=7345706409186580791:INF=0:SET=111236436:LNG=0:CNT=0:RM=0:USR=bmV0c3F1YXJlLnRlc3RAZ21haWwuY29t:PHS=:TS=1139464962:LCL=en-US:NET=1:GC=DQAAAHIAAACHt2C7G2yE_QHHwhtq6IrwHbxX3HM_dc08ebUYI_kAdVMIswoVtp02jEehQoei3EiUvVUJQBWRhNQQBxaRt2MASDd0T55CXFLc1e13800XzjYi_OP-MufQrdZ5GG8QjecK2o9qJT6ggvWT0pk9zG4rSUQV45xFlBnDgwOrZAx4A:S=JBeeckM0uyLMUSrsoOYYx8XTmo=;;  
Path=/
```

Save this cookie for future use.

The request header (after clearing the login form) going to <https://www.orkut.com/RedirLogin.aspx> is as follows:

```
GET /RedirLogin.aspx?msg=0&page=http%3A%2F%2Fwww.orkut.com%2F&auth=DQAAAHMAAAC8HAZGjvWyLbfRURHF_8Hi8XpPuWOOQ3_ltYAdbtK2pXuHlyjddSrGu7PqQ3KXdL-zFtTEmb-xT-zKsZS3tgTfIRI7zkQSihw_-s6y_8JM_HEtZyrYNHNEd7RLts1NXUFifLMJG-eAbyH1TlkFbSUIaR-OsB52kcmoPra82TcxKQ HTTP/1.1  
Host: www.orkut.com  
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.7.9) Gecko/20050711 Firefox/1.0.5  
Accept: text/xml,application/xml,application/xhtml+xml,text/html;
```

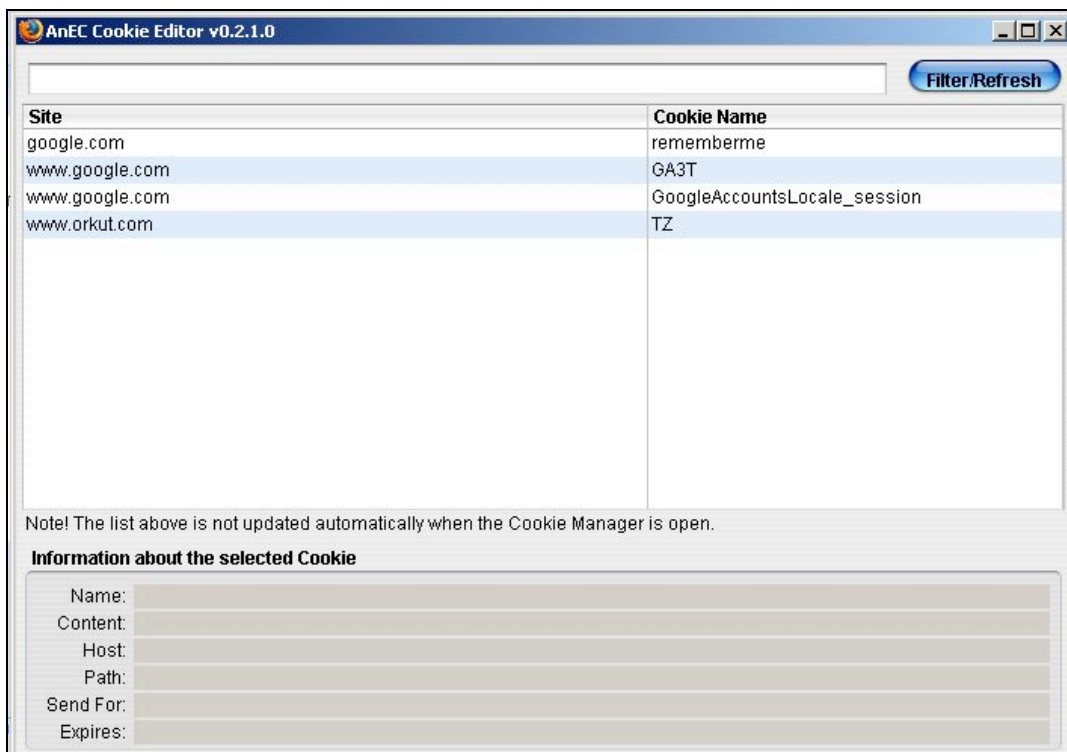
```
q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: https://www.google.com/accounts/ServiceLoginBoxAuth
Cookie: TZ=-330
```

The response header received is as follows:

```
HTTP/1.x 200 OK
Cache-Control: no-cache, must-revalidate, no-cache="Set-Cookie",
private
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Pragma: no-cache
Set-Cookie: orkut_state=ORKUTPREF=ID=7345706409186580791:INF=0:SET=
111236436:LNG=0:CNT=0:RM=0:USR=bmV0c3F1YXJlLnRlc3RAZ21ha
WwuY29t:PHS=:TS=1139181125:LCL=en-US:GC=DQAAAHEAAAA5RS
pNO2tOLt02zgeCKe6lhUC07ImLiK0DJuTde09zlAbsKkyPswUy84g
NFJOX7MdNPDETKsrCG0NBP-ss_03dFmHqDHfakQ5wBYuZFN048Je5
thF4uVjWZwLqkwu2RsbTEs1qMDGVFsIqUfS-ayYl381KlnDwyd7xAwh
3ZU1YA:S=GGrXWvaaUGxawkChpKuFLs/I25Q=:; Domain=.orkut.
com; Path=/; HttpOnly
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding: gzip
Date: Mon, 06 Feb 2006 06:12:06 GMT
Server: GFE/1.3
```

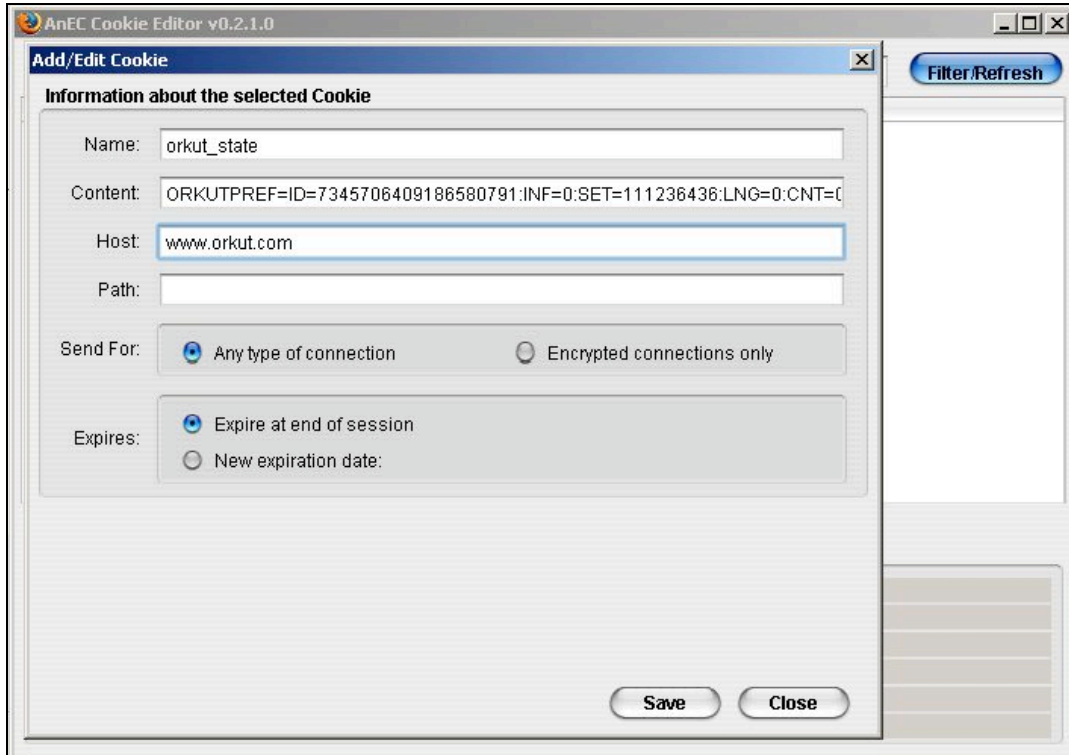
Step 3: Log out of Orkut

Use the "Logout" link to log out of Orkut. The session cookies will be cleared from the browser's memory. The following screenshot shows there are no session cookies remaining in the browser's memory.



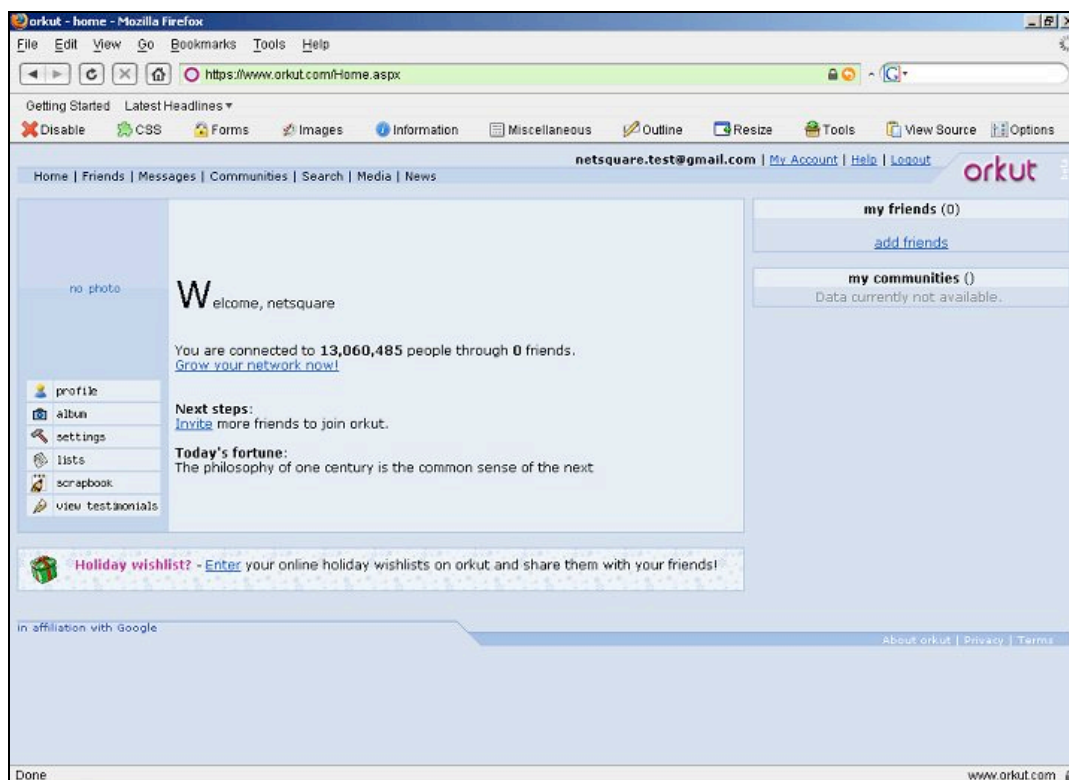
Step 4: Set the orkut_state cookie back in the browser's cookie store

Use the Firefox Add n Edit Cookies extension to insert the saved orkut_state cookie back into the browser's cookie store. The following screenshot demonstrates this:



Step 5: Browse to <https://www.orkut.com/>

Once the cookie is set, as described above, point the browser to <http://www.orkut.com/>. After a few HTTP redirects, it will land you into the user's mail account.



IMPACT

Session cookies such as the `orkut_state` should be cleared at both the client side as well as the server side upon termination of the authenticated session. Orkut fails to clear the `orkut_state` cookie from the server side. It was observed that `orkut_state` session cookies stay active for two weeks after they are created. If at any point during a user's Orkut session, the `orkut_state` cookie has been intercepted or recovered, an attacker can gain unauthorized access to the Orkut account long after the user signs off. Even if the user logs in again with a new `orkut_state` cookie, the old ones never expire, and the replay attack still works.

It has been observed by Net-Square that sending HTTP requests with multiple `orkut_state` cookies also works, and lets the attacker gain unauthorized access to a victim's Orkut account.

Changing the password has no effect either, since an `orkut_state` session cookie once set after proper authentication stays working.

WORKAROUNDS/FIXES

~~At this point in time, there are no workarounds that a user can use to protect his or her session. Net-Square advises Orkut users not to use their Orkut accounts from untrusted computers or networks.~~

Google has fixed this problem on their side. Session cookies are now set to expire within 24 hours from the server side, as opposed to two weeks. Net-Square was checking this vulnerability almost every week. The vulnerability seems to have been fixed around 05 January, 2007.

VULNERABILITY REPORTING AND STATUS

Date of discovery: 01 February 2006

Date of reporting to Google: 10 February 2006

Follow-up emails: 22 February 2006, 20 June 2006, 10 December 2006

Vulnerability fix from Google: January 2007

CREDITS

AnEC Cookie Editor - <http://addneditcookies.mozdev.org/>

CONTACT

Net-Square Solutions Pvt. Ltd.
1 Sanjivbaug, Paldi, Ahmedabad 380007, India
Tel: +91 79 2663 7090
Fax: +91 79 2663 8051
<http://net-square.com/>

DISCLAIMER

The information contained in this advisory is the copyright (c) 2006 of Net-Square Solutions Pvt. Ltd. and believed to be accurate at the time of authoring, but no representation or warranty is given, express or implied, as to its accuracy or completeness. Neither the author nor the publisher accepts any liability whatsoever for any direct, indirect or consequential loss or damage arising in any way from any use of or reliance placed on, this information for any purpose.