

Public Sanitised Notes on QA Mail installation & Testing

Notebook: alan richardson's notebook

Created: 08/05/2015 12:55

Updated: 11/05/2015 16:22

URL: http://qamail.ala.se/show_session?session_key=fO6NNvnk3ZHreG12dCADYFtx

Notes on QA Mail installation

Recommendations & Findings

- * API reports 500 errors - it should protect itself and report 4xx errors rather than exceptions via 5xx - expected error codes for API? (<http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html>), 404 Not Found, 405 Method not Allowed, 406 Not Acceptable or possibly 400 Bad Request
- * Minimal error protection on GUI
- * Project needs to spend time making install easier otherwise it won't be used
- * Could make GUI simpler and less risk of cross platform errors by removing iframe and bringing in text into body from a request - GUI is so simple it doesn't need JS and iframes
- * There is no build automation on the project - Rails has pretty good framework for writing automation - use it
- * Raw message view
 - * Headers shown differently "MIME-Version:" (sent) "Mime-Version:" (qamail)
 - * after reading code suspect this is the postfix app or mail server, not qamail
 - * content differences - qamail shows charset and Content-Transfer-Encoding - again suspect postfix
 - * mail server does not have blanket accept of all email addresses - this is postfix not qamail - does not affect app and protects from hacking - some emails filtered out
 - * Show_mailbox.erb is vulnerable to xss in subject and via body - sanitise output so not render < and >
 - * Tony pointed out the demo server config "<http://qamail.ala.se/>" is incorrect as it has exception reporting enabled see <http://blog.8thcolor.com/en/2014/03/avoid-spilling-your-rails-application-secrets/>
 - * Cookie set 10 years in future - is that right? from calculation in code I expected it to be one year
 - * Blank subjects (Steve pointed this out yesterday, encountered it today during xss), mean can't click on email

Summary Notes

Braindump of tools used:

- * Bitvise SSH client - I find it easier to use than putty
 - * <http://www.bitvise.com/ssh-client>
- * Postman for interaction with API via GUI
- * GUI of the app itself
- * Abstraction layers and Java - sendmail with debug mode
- * Gmail - "Show Original" (for sent and received)
- * Java automation code - SendMail wrapper around Javax Mail, and RestAssured
- * Snagit
- * Psql
- * tail -f import.log
- * mailinator, temp-mail.org as oracles
- * horde - as server side mail client
- * Fiddler
- * Java Test Tool Hub (unreleased)

Hard to test with so many intermediate systems in place i.e. my smtp server, routing servers, mail server, postfix

Sendmail made it hard to test invalid emails.

Abstraction layers need to support 'invalid' testing as well as 'normal' code execution.

https://aithub.com/eviltester/qamail_automation

* Found bug with routing for cc, bcc, to etc. but fixed in most recent version - fix relies on postfix header though so not generic for any install

* Created initial set of tests, but rejected this after code review could see no protection on API for headers or params etc. (all 500 throwing)

Likes:

* GUI - for a session to create new emails and switch between them easily

Interesting that normally when we test email we are checking rendering. Now I'm checking headers and the encoding, etc. Starting to look at the normal emails I'm sent with gmail 'Show original' view

Viable competition:

- * <http://temp-mail.org/>
 - * does show original - close to matching qa mail but formats "Received:" as per google and "MIME-Version:" as per google, also slightly different representation of the content mime (Q: Does temp-mail.org have an api?)
- * <http://mailinator.com>
 - * now has an API, and Pricing plans for Testing (\$29 a month, 1000 emails per day, and private domain email system) - does show original and matches the temp-mail.org pretty closely (mime content and MIME-version)
 - * gmail accounts taking advantage of '+' and '.'

Research:

- * http://en.wikipedia.org/wiki/Disposable_email_address - useful overview and pros and cons
- * http://www.dmoz.org/Computers/Internet/E-mail/Spam/Preventing/Temporary_Addresses/
- * <http://blog.eviltester.com/2011/09/running-out-of-email-addresses-when-you-test.html>

Tuesday 5th May 2015

3 hours

Tried to install app using bitnami machine.

My notes have a big list of permission errors that I was 'sudo' and 'chown' 'ing around.

Eventually had postgres running, and the qmail app running - but hadn't managed to check if system was accessible or picking up mail.

Mathew from Test Partners had spent time installing it and has an amazon instance to use.

The hassle involved in installing this almost makes it a non-starter.

Recommend the project spends time making install easier:

- * creating an out of the box Amazon or Azure machine instance or some chef/docker style installation scripts to make it easy to install and get running.
- * Or have some tutorial videos starting from scratch with a bitnami (or other) off the shelf machine image

If I was in production environment, I'd probably drop the install after an hour and pay for mailinator - I suspect the cost for a year of mailinator would be less than the time of installing QA Mail.

Wednesday 6th May 2015

Started investigating the automation through the API to create more API automation examples.

Investigate JavaXmail

Created example sending code - didn't work.

Brought in the javax-mail-api dependency, but that doesn't have the implementation, need to bring in the javax-mail dependency from sun.

<http://mvnrepository.com/artifact/com.sun.mail/javax.mail/1.5.3>

- aargh, strange partial machine crash wiped out my code after an hour

- start again, created github repo for code

https://github.com/eviltester/qamail_automation

Try simple mail wrapper <https://github.com/bbottema/simple-java-mail>

Using environment vars for usernames, urls and passwords to allow github commits

Initial url tests through the API

/api/list_mailboxes

Internal Server Error

This is possibly a bug, we don't really want 500 internal server errors propagating from an API

expected error codes for API? (<http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html>)

404 Not Found

405 Method not Allowed

406 Not Acceptable or possibly 400 Bad Request

Basic abstractions and simple automation created.

Personal Notes on abstractions

- * Created a wrapper around sendmail to make it handle my defaults from environments and make it simpler to read from my @Test method code

- * Created an API abstraction around the method calls

- * API Abstraction returns QAMail specific objects to allow easier access to values

- * API Abstraction tracks last response to allow drill down in automation

- * Created a QaMail API abstraction on top of the basic HTTP abstraction to make it easier to read

- * TODO expand the QaMail abstractions to allow things like <mailbox>.empty so that I have contextual methods at the domain level

- * These abstractions allow easy access to simple functionality but don't allow full scope of API testing

e.g.

- * wrong verbs (e.g. POST)

- * null params

- * extra params

- * invalid param values

- * missing params

- * Note: This is common with API abstractions, add to TODO list to investigate a modelling approach to this e.g. the QaMail REST API abstraction delegates to a FlexibleQaMailRestApi that allows misuse of the API, but the QaMailRESTApi enforces the valid constraints. Then we can drop down to the level we need to support testing.

- * NOTE: investigate data generation tools again, and also Agile Designer

Thursday 6th May 2015

10:00 Create initial scope notes

initial scope based on reading docs at <https://bitbucket.org/naushniki/qamail>

- can receive email
- can view email
- check email stored in DB correctly
- check email returned in contents correct for different email formats and types

expected error codes for API? (<http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html>)

404 Not Found

405 Method not Allowed

406 Not Acceptable or possibly 400 Bad Request

API:

- create session
 - verbs other than GET - should return 405
 - params should be ignored or error
 - try with param of existing session_key
- list_mailboxes
 - verbs other than GET - should return 405
 - params other than session_key should be ignored or error
 - try with param of non-existent session_key
 - try with param of multiple session_key (?expected)
- create_mailbox
 - verbs other than GET - should return 405
 - params other than session_key should be ignored or error
 - try with param of non-existent session_key
 - try with param of multiple session_key (?expected)
- show_mailbox_content
 - verbs other than GET - should return 405
 - missing params should be reported as error (requires: session_key, address)
 - try with param of non-existent session_key
 - try with param of non-existent address
 - try with param of existent session_key and existing address but address on different session
 - try with param of non-existent session_key, and address that exists on a session
- show_letter
 - verbs other than GET - should return 405
 - missing params should be reported as error (requires: session_key, address, letter_id)
 - try with param of non-existent session_key (TEST Session_key)
 - try with param of non-existent address for valid session (TEST address)
 - try with param of non-existent letter for valid session and address (TEST LETTERID)
- empty_mailbox
 - verbs other than GET - should return 405
 - missing params should be reported as error (requires: session_key, address, letter_id)
 - try with param of non-existent session_key (TEST Session_key)
 - try with param of non-existent address for valid session (TEST address)

Scenarios:

- email to person

- cc'd to person
- bcc'd to person
- to, cc, bcc - combinations of email addresses in the session
- to, cc, bcc - combinations of email addresses spanning sessions

10:39 Check that existing abstraction layers are good enough at the moment to match manual email creation

send an email to my gmail account

@Test

```
public void firstCheckThatEmailSendingValidByUsingMyNormalEmail(){
    MailSender emailer = MailSender.getInstance();
    emailer.sendEmailTo("<insert gmail address here>", "Alan Richardson", "email title", "body of
email");
}
```

email received and sent as valid text email

Gmail can show the original message sent - compare with that shown in content from QAMail

D:\Users\Alan\Documents\Documents\Compendium
Developments\testing\webinars\blackOpsTesting\qaMail\adhoc\201507_1039_gmailReceivedTestEmail.t
xt

Compare above with QA Mail

D:\Users\Alan\Documents\Documents\Compendium
Developments\testing\webinars\blackOpsTesting\qaMail\adhoc\201507_1039_qamailReceivedTestEmail.
txt

Comparison using WinMerge shows a lot of differences

- * Some of the headers are formatted differently with linebreaks:
 - * "Received:"
 - * "X-AntiAbuse:"
 - * "X-Get-Message-Sender-Via:"
- * Headers shown in different order
- * Unique to Gmail - Some headers missing from the 'raw' report in QAMail
 - * "Deilvered-To:"
 - * "X-Received:"
 - * "Received-SPF"
 - * "Authentication-Results"
- * Headers shown differently "MIME-Version:" (gmail) "Mime-Version:" (qamail)
- * Unique to QAMail
 - * Content-Type: shows charset=UTF-8
 - * because QAMail is doing internal forwarding it has the X-Original-To showing the sent to email address and the Delivered-To: shows the generic qamail email address
- * content differences
 - * qamail shows charset and Content-Transfer-Encoding

[X]Need a way of interrogating the actual sent message to see what is included in the original to improve the comparison analysis

[X]investigate other email sites for temporary and anonymous email see what they offer

[X]http://en.wikipedia.org/wiki/Disposable_email_address - useful overview and pros and cons

[X]http://www.dmoz.org/Computers/Internet/E-mail/Spam/Preventing/Temporary_Addresses/ -

list of services

[X]- <https://www.guerrillamail.com> - does not show raw original email

[X]+ <http://temp-mail.org/> - does show original - close to matching qa mail but formats

"Received:" as per google and "MIME-Version:" as per google, also slightly different representation of the content mime (Q: Does temp-mail.org have an api?)

[X]- 10minutemail.com - offline when I tried it

[X]+ mailinator.com - now has an API, and Pricing plans for Testing (\$29 a month, 1000 emails per day, and private domain email system) - does show original and matches the temp-mail.org pretty closely (mime content and MIME-version)

[X]- getairmail.com (big ad supported) didn't seem to receive the email

[X]- throwAwayMail.com - does not show raw original email

[X]o trashMail.com (offers pro version for \$12.99 a year), has an API, need to register, is really a forwarding account rather than a mail box

[X]mailcatch.com - either slow to pick up mail or did not arrive

[X]by switching on debug in the sendmail api I could see the smtp session and the original mail that was sent `mailer.setDebug(true);`

Headers actually sent are:

Date:

From:

To:

Message-ID:

Subject:

MIME-Version:

then the content

Comparing with the Actual mail sent I can see that:

qaMail lowercases the MIME-Version: header name

and adds additional info to all the mime Part sections

charset=UTF-8

Content-Transfer-Encoding: 7bit

So it doesn't really display the 'raw' message.

The SMTP server I use will have added some of the other fields, but since the other email systems didn't show the header info differently or the extra mime info, I assume that qamail did this - or the installed mail system on our side -

[X]confirm by using the demo system on the qamail site

http://qamail.ala.se/show_session?session_key=LyzXaGnOZu8Ih6JrdoecgyeW

63moeuk@qamail.ala.se

This has the same format as the one we are using for testing so I think the comments on formatting message on the 'raw' email are valid

[x]Comments to pass on:

[x]Raw message view does not show the 'sent' message in a raw format

[x]Headers shown differently "MIME-Version:" (sent) "Mime-Version:" (qamail)

[x]content differences - qamail shows charset and Content-Transfer-Encoding

12:19 Confirmed that sending email method I'm using is good enough to test the qamail system

[x]use abstraction layers for testing & identify what can't do with current abstraction

- different verbs

- incorrect param spelling
- missing params
- extra params
- null params

[X]figure out how to look at the database

[X]emailed Mathew to find username and database name for psql

[X]look at code to answer questions - can we delete a session? etc. 12:35

[X]quick review of

<https://bitbucket.org/naushniki/qamail/src/34e4f15d6ca0d8a185ebf327497a12ecb51591d2/qamail.rb?at=default>

[X]quick review of api

<https://bitbucket.org/naushniki/qamail/src/34e4f15d6ca0d8a185ebf327497a12ecb51591d2/api.rb?at=default>

suggests that we can trigger 500 errors on may requests e.g. empty mailbox with non existant values

12:42 - yup - session key that does not exist triggers 500

/api/list_mailboxes?session_key=bodddddd

- this is throughout the qamail.rb - there are checks for some params which issue 404 e.g.

show_letter with missing letter via the GUI

- not a lot of point testing with different verbs as everything is coded as a 'get' (assuming associated post etc. as I'm not familiar with rails)

[X]no additional functionality suggested by code - can't delete unless vulnerable to Rails SQL injections

break 13:10

17:10 try some multiple email sending

create session 1, 2 3

```
<?xml version="1.0" encoding="UTF-8"?>
<session>
  <session_key>LjbwFaxfzrxtdbT32PqUmyXk</session_key>
  <mailbox>
    <address>1fw5qua@obscuredthedomainviafindandreplace.com</address>
  </mailbox>
</session>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<session>
  <session_key>RoJUhyEdCJy3jT51CP63YDQ2</session_key>
  <mailbox>
    <address>ycqxx9f@obscuredthedomainviafindandreplace.com</address>
  </mailbox>
</session>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<session>
  <session_key>vqGu5PkvTMEu7Wc8A9cPq153</session_key>
  <mailbox>
    <address>8rms32y@obscuredthedomainviafindandreplace.com</address>
  </mailbox>
</session>
```

create emails in session 1, session 2, session 3

http://obscuredthedomainviafindandreplace.com/api/create_mailbox?session_key=LjbwFaxfzrxtdbT32PqUmyXk

```
<?xml version="1.0" encoding="UTF-8"?>
<mailbox>
  <address>lkbj0tt@obscuredthedomainviafindandreplace.com</address>
</mailbox>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<mailbox>
  <address>acwccjo@obscuredthedomainviafindandreplace.com</address>
</mailbox>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<mailbox>
  <address>vkq74v7@obscuredthedomainviafindandreplace.com</address>
</mailbox>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<mailbox>
  <address>emrlh45@obscuredthedomainviafindandreplace.com</address>
</mailbox>
```

http://obscuredthedomainviafindandreplace.com/api/create_mailbox?session_key=RoJUhyEdCJy3jT51CP63YDQ2

```
<?xml version="1.0" encoding="UTF-8"?>
<mailbox>
  <address>3sa3gni@obscuredthedomainviafindandreplace.com</address>
</mailbox>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<mailbox>
  <address>kykegfk@obscuredthedomainviafindandreplace.com</address>
</mailbox>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<mailbox>
  <address>r16m5v8@obscuredthedomainviafindandreplace.com</address>
</mailbox>
```

http://obscuredthedomainviafindandreplace.com/api/create_mailbox?session_key=vqGu5PkvTMEu7Wc8A9cPq153

```
<?xml version="1.0" encoding="UTF-8"?>
<mailbox>
  <address>mydrnvd@obscuredthedomainviafindandreplace.com</address>
</mailbox>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<mailbox>
  <address>bhgdbqr@obscuredthedomainviafindandreplace.com</address>
</mailbox>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<mailbox>
  <address>ul3ppea@obscuredthedomainviafindandreplace.com</address>
</mailbox>
```

LIST Mailboxes to check

http://obscuredthedomainviafindandreplace.com/api/list_mailboxes?
session_key=LjbwFaxfzrxtdbT32PqUmyXk

```
<?xml version="1.0" encoding="UTF-8"?>
<session>
  <session_key>LjbwFaxfzrxtdbT32PqUmyXk</session_key>
  <mailbox>
    <address>1fw5qua@obscuredthedomainviafindandreplace.com</address>
  </mailbox>
  <mailbox>
    <address>lkbj0tt@obscuredthedomainviafindandreplace.com</address>
  </mailbox>
  <mailbox>
    <address>acwccjo@obscuredthedomainviafindandreplace.com</address>
  </mailbox>
  <mailbox>
    <address>vkq74v7@obscuredthedomainviafindandreplace.com</address>
  </mailbox>
  <mailbox>
    <address>emrlh45@obscuredthedomainviafindandreplace.com</address>
  </mailbox>
</session>
```

http://obscuredthedomainviafindandreplace.com/api/list_mailboxes?
session_key=vqGu5PkvTMEu7Wc8A9cPq153

```
<?xml version="1.0" encoding="UTF-8"?>
<session>
  <session_key>vqGu5PkvTMEu7Wc8A9cPq153</session_key>
  <mailbox>
    <address>8rms32y@obscuredthedomainviafindandreplace.com</address>
  </mailbox>
  <mailbox>
    <address>mydrnvd@obscuredthedomainviafindandreplace.com</address>
  </mailbox>
  <mailbox>
    <address>bhgdbqr@obscuredthedomainviafindandreplace.com</address>
  </mailbox>
  <mailbox>
    <address>ul3ppea@obscuredthedomainviafindandreplace.com</address>
  </mailbox>
</session>
```

http://obscuredthedomainviafindandreplace.com/api/list_mailboxes?
session_key=RoJUhyEdCJy3jT51CP63YDQ2

```
<?xml version="1.0" encoding="UTF-8"?>
<session>
  <session_key>RoJUhyEdCJy3jT51CP63YDQ2</session_key>
  <mailbox>
    <address>ycqx9f@obscuredthedomainviafindandreplace.com</address>
  </mailbox>
  <mailbox>
    <address>3sa3gni@obscuredthedomainviafindandreplace.com</address>
  </mailbox>
  <mailbox>
    <address>kykegfk@obscuredthedomainviafindandreplace.com</address>
  </mailbox>
  <mailbox>
```

```
<address>r16m5v8@obscuredthedomainviafindandreplace.com</address>
</mailbox>
</session>
```

Send email to single person as 'to' 6 times
ycqxx9f@obscuredthedomainviafindandreplace.com

Not convinced that google sent email with same 'to' 6 times - suspect it went down to one
TODO: try this with automation

empty

```
http://obscuredthedomainviafindandreplace.com/api/empty_mailbox?
session_key=RoJUhyEdCJy3jT51CP63YDQ2&address=ycqxx9f@obscuredthedomainviafindandreplace.co
m
```

BUG: send email to, cc, bcc all within same session

```
RoJUhyEdCJy3jT51CP63YDQ2
to: ycqxx9f@obscuredthedomainviafindandreplace.com
cc: 3sa3gni@obscuredthedomainviafindandreplace.com
bcc: kykegfk@obscuredthedomainviafindandreplace.com
```

BUG: - received email 3 times in ycqxx9f@obscuredthedomainviafindandreplace.com

```
http://obscuredthedomainviafindandreplace.com/api/show_mailbox_content?
session_key=RoJUhyEdCJy3jT51CP63YDQ2&address=ycqxx9f@obscuredthedomainviafindandreplace.co
m
```

```
<?xml version="1.0" encoding="UTF-8"?>
<mailbox>
  <address>ycqxx9f@obscuredthedomainviafindandreplace.com</address>
  <letter>
    <id>57</id>
    <subject>to ycqxx9f, with cc and bcc in same session</subject>
    <from>notmyemail@notmydomain.co.uk</from>
    <date>2015-05-07 16:41:24 UTC</date>
  </letter>
  <letter>
    <id>58</id>
    <subject>to ycqxx9f, with cc and bcc in same session</subject>
    <from>notmyemail@notmydomain.co.uk</from>
    <date>2015-05-07 16:41:24 UTC</date>
  </letter>
  <letter>
    <id>59</id>
    <subject>to ycqxx9f, with cc and bcc in same session</subject>
    <from>notmyemail@notmydomain.co.uk</from>
    <date>2015-05-07 16:41:24 UTC</date>
  </letter>
</mailbox>
```

Did not receive in cc

```
http://obscuredthedomainviafindandreplace.com/api/show_mailbox_content?
session_key=RoJUhyEdCJy3jT51CP63YDQ2&address=3sa3gni@obscuredthedomainviafindandreplace.co
m
```

```
<?xml version="1.0" encoding="UTF-8"?>
<mailbox>
```

```
<address>3sa3gni@obscuredthedomainviafindandreplace.com</address>
</mailbox>
```

Did not receive in bcc

```
http://obscuredthedomainviafindandreplace.com/api/show_mailbox_content?
session_key=RoJUhyEdCJy3jT51CP63YDQ2&address=kykegfk@obscuredthedomainviafindandreplace.co
m
```

```
<?xml version="1.0" encoding="UTF-8"?>
<mailbox>
  <address>kykegfk@obscuredthedomainviafindandreplace.com</address>
</mailbox>
```

erase session to clean up ycqx9f

```
http://obscuredthedomainviafindandreplace.com/api/empty_mailbox?
session_key=RoJUhyEdCJy3jT51CP63YDQ2&address=ycqx9f@obscuredthedomainviafindandreplace.co
m
```

check

```
http://obscuredthedomainviafindandreplace.com/api/show_mailbox_content?
session_key=RoJUhyEdCJy3jT51CP63YDQ2&address=ycqx9f@obscuredthedomainviafindandreplace.co
m
```

checked

Bugged: send email to, cc, bcc all within different sessions (all go to 'to')

```
<session_key>LjbwFaxfzrxtdbT32PqUmyXk</session_key>
  <address>1fw5qua@obscuredthedomainviafindandreplace.com</address>
```

```
<session_key>vqGu5PkvTMEu7Wc8A9cPq153</session_key>
<mailbox>
  <address>8rms32y@obscuredthedomainviafindandreplace.com</address>
```

```
<session_key>RoJUhyEdCJy3jT51CP63YDQ2</session_key>
<mailbox>
  <address>ycqx9f@obscuredthedomainviafindandreplace.com</address>
```

to: 1fw5qua@obscuredthedomainviafindandreplace.com

cc: 8rms32y@obscuredthedomainviafindandreplace.com

bcc: ycqx9f@obscuredthedomainviafindandreplace.com

```
http://obscuredthedomainviafindandreplace.com/api/show_mailbox_content?
session_key=LjbwFaxfzrxtdbT32PqUmyXk&address=1fw5qua@obscuredthedomainviafindandreplace.co
m
```

```
<?xml version="1.0" encoding="UTF-8"?>
<mailbox>
  <address>1fw5qua@obscuredthedomainviafindandreplace.com</address>
  <letter>
    <id>60</id>
    <subject>different sessions</subject>
    <from>notmyemail@notmydomain.co.uk</from>
    <date>2015-05-07 16:48:45 UTC</date>
  </letter>
  <letter>
    <id>61</id>
    <subject>different sessions</subject>
    <from>notmyemail@notmydomain.co.uk</from>
    <date>2015-05-07 16:48:45 UTC</date>
  </letter>
```

```
<letter>
  <id>62</id>
  <subject>different sessions</subject>
  <from>notmyemail@notmydomain.co.uk</from>
  <date>2015-05-07 16:48:45 UTC</date>
</letter>
</mailbox>
```

http://obscuredthedomainviafindandreplace.com/api/show_mailbox_content?session_key=vqGu5PkvTMEu7Wc8A9cPq153&address=8rms32y@obscuredthedomainviafindandreplace.com

```
<?xml version="1.0" encoding="UTF-8"?>
<mailbox>
  <address>8rms32y@obscuredthedomainviafindandreplace.com</address>
</mailbox>
```

http://obscuredthedomainviafindandreplace.com/api/show_mailbox_content?session_key=RoJUHyEdCJy3jT51CP63YDQ2&address=ycqxx9f@obscuredthedomainviafindandreplace.com

```
<?xml version="1.0" encoding="UTF-8"?>
<mailbox>
  <address>ycqxx9f@obscuredthedomainviafindandreplace.com</address>
</mailbox>
```

Bugged: Can I send from gmail without 'to', it appears so, but nothing received

cc: 8rms32y@obscuredthedomainviafindandreplace.com
bcc: ycqxx9f@obscuredthedomainviafindandreplace.com

nothing received in either
http://obscuredthedomainviafindandreplace.com/api/show_mailbox_content?session_key=RoJUHyEdCJy3jT51CP63YDQ2&address=ycqxx9f@obscuredthedomainviafindandreplace.com
http://obscuredthedomainviafindandreplace.com/api/show_mailbox_content?session_key=vqGu5PkvTMEu7Wc8A9cPq153&address=8rms32y@obscuredthedomainviafindandreplace.com

Can I send it to my normal address and cc, bcc the qamail system?

received by me
but not by the system

qa mail cannot seem to handle being cc'd or bcc'd

[X]confirm in the demo system (not a bug in their system *fixed*)

http://qamail.ala.se/show_session?session_key=LyzXaGnOZu8Ih6JrdoecgyeW

63moeuk@qamail.ala.se
8500314@qamail.ala.se

to: me
cc: 63moeuk@qamail.ala.se
bcc: 8500314@qamail.ala.se

received: cc and bcc in the test system
http://qamail.ala.se/show_session?session_key=LyzXaGnOZu8Ih6JrdoecgyeW

what is different between systems?

investigate....

different versions

Email to BlackOpsTeam:

we are testing against an older version of the qmail application than the test system on their site.

I found a bug in the system where it wasn't handling cc, or bcc routing of messages. But that seems to have been fixed 5 days ago...

<https://bitbucket.org/naushniki/qmail/commits/2e36e9e558f4ffb7e31036c23e596ad8d221cd6a>

... so isn't present on the test version that they have running.

Friday 8th May 2015

Start by collating notes

Aaaaargh - my log files and notes folder has been lost

- present in windows search, not on disk

dropping testing - investigate and try and fix machine - assume yesterday's logs of different message types have been lost

Investigation: Suspect sync and backup apps are colliding and locking files/folders etc. - but why deleted? some sort of caching? (but files were not picked up in hourly cloud sync due to clash with expanded scope from other backup). changed cloud sync scope to try and prevent this.

Aaaargh.

Braindump of tools used:

- * Bitvise SSH client - I find it easier to use than putty
- * <http://www.bitvise.com/ssh-client>
- * Postman for interaction with API via GUI
- * GUI of the app itself
- * Abstraction layers and Java - sendmail with debug mode

Likes:

GUI - for a session to create new emails and switch between them easily

Interesting that normally when we test email we are checking rendering. Now I'm checking headers and the encoding, etc. Starting to look at the normal emails I'm sent with gmail 'Show original' view

16:00 reinstate the API changes that I made - i.e. allow api sending at Session and at Mailbox

DONE: allow creation of session with known session key

Monday 11/5/2015

Look in database using bitvise

sudo su postgres

psql

help

\h

\q to quit

\connect db_name

\dt

tables -

letters

mailboxes

schema_migrations

sessions

/d+ letters

Column	Type	Modifiers
	Storage	Stats target Description
id	integer	not null default nextval('letters_id_seq'::regclass) plain
mailbox_id	integer	
	plain	
raw	text	
	extended	
written_at	timestamp without time zone	
	plain	
from	character varying	
	extended	
subject	character varying	
	extended	

Indexes:

"letters_pkey" PRIMARY KEY, btree (id)

"index_letters_on_mailbox_id" btree (mailbox_id)

Has OIDs: no

/d+ mailboxes

Table "public.mailboxes"		
Column	Type	Modifiers
	Storage	Stats target Description
id	integer	not null default nextval('mailboxes_id_seq'::regclass) plain
address	character varying	
	extended	
session_id	character varying	
	extended	

Indexes:

"mailboxes_pkey" PRIMARY KEY, btree (id)

"index_mailboxes_on_address" btree (address)

Has OIDs: no

Table "public.sessions"		
Column	Type	Modifiers
	Storage	Stats target Description
id	integer	not null default nextval('sessions_id_seq'::r

```
egclass) | plain |
session_key | character varying |
          | extended |
```

Indexes:

```
"sessions_pkey" PRIMARY KEY, btree (id)
"index_sessions_on_session_key" btree (session_key)
```

Has OIDs: no

```
select column_name, data_type, character_maximum_length from INFORMATION_SCHEMA.COLUMNS
where table_name = 'letters';
```

```
db_name=# select column_name, data_type, character_maximum_length from INFORMATI
ON_SCHEMA.COLUMNS where table_name = 'letters';
```

```
column_name | data_type | character_maximum_length
-----+-----+-----
id | integer |
mailbox_id | integer |
raw | text |
written_at | timestamp without time zone |
from | character varying |
subject | character varying |
(6 rows)
```

```
select column_name, data_type, character_maximum_length from INFORMATION_SCHEMA.COLUMNS
where table_name = 'mailboxes';
```

```
db_name=# select column_name, data_type, character_maximum_length from INFORMATI
ON_SCHEMA.COLUMNS where table_name = 'mailboxes';
```

```
column_name | data_type | character_maximum_length
-----+-----+-----
id | integer |
address | character varying |
session_id | character varying |
(3 rows)
```

```
select column_name, data_type, character_maximum_length from INFORMATION_SCHEMA.COLUMNS
where table_name = 'sessions';
```

```
db_name=# select column_name, data_type, character_maximum_length from INFORMATI
ON_SCHEMA.COLUMNS where table_name = 'sessions';
```

```
column_name | data_type | character_maximum_length
-----+-----+-----
id | integer |
session_key | character varying |
(2 rows)
```

I couldn't figure out how to 'inject' into the rails queries
'%20--' etc.

<http://rails-sqli.org/>

"Mime-version" is stored in the raw

examine code for things to test - as most of this is select * and display

there is 'real' code in letter_import.rb

cd ./usr/share/qamail/letter_import.rb

cd log

tail -f import.log

if I send without a 'to' what happens?

```
I, [2015-05-11T09:51:20.040591 #12323] INFO -- : Found new letter file: 1431337
879.Vca01I62a47M916315.ip-172-31-7-45
I, [2015-05-11T09:51:20.053190 #12323] INFO -- : Mailbox not found in the datab
ase: . This letter was not imported. Deleting file.
```

fix uses the X-Original-to added by postfix - perhaps the Mime-version and meme encoding text is done by postfix and is actually a bug with postfix.org?

Try on demo app

http://qamail.ala.se/show_session?session_key=fO6NNynk3ZHreG12dCADYFtx

jgndvxd@qamail.ala.se

###Can we use letter_import.rb to inject sql?

Could this be an easier way of injecting sql commands? Since the Mailbox table is accessed in the letter_import.rb

tried to send to [1234'\)--@domain.com](mailto:1234')--@domain.com)

and received

```
SMTP error from remote mail server after RCPT TO: <"1234')--@domain.com">:
550 5.1.1 <1234')--@domain.com>: Recipient address rejected:
User unknown in local recipient table
```

If it is configured to pass on every email then this should not happen, so this is triggering an 'error' in the mail routing app

Simple mail Java API made it impossible for me to send invalid emails easily - would need a different library or lower level abstraction to help me automate these conditions. This is a generic issue to watch out for with automation libraries.

try different addresses

```
1234
1234'
1234)
```

http://en.wikipedia.org/wiki/Email_address#Local_part

local part does allow ' and) and --

```
"1234'"@
```

Try on demo see if that makes a difference

Nope - unknown in local recipient table

```
"()<>[:;@\\!#$%&'*+/,=?^_`{| ~.a"@
```

Using a valid email addresss like the above from
(http://en.wikipedia.org/wiki/Email_address#Local_part)

is returned as

```
SMTP error from remote mail server after RCPT TO: <"()<>[:;@\\!#$%&'*/+=?^_`{}|
~.a"@domain.com>:
501 5.1.3 Bad recipient address syntax
```

a3a5a7a10a13a16a19a22a25a28a31a34a37a40a43a46a49a52a55a58a61a64a@

a3a5a7a10a13a16a19a22a25a28a31a34a37a40a43a46a49a52a55a58a61a64ab@

- 65 chars in local is accepted - this is actually an invalid email since local is supposed to be limited to 64 chars, how far can we push this?

total email == 254 max

@aaaa.com == 9 chars

254-9 = 245

a3a5a7a10a13a16a19a22a25a28a31a34a37a40a43a46a49a52a55a58a61a64a67a70a73a76a79a82a85a88a91a94a97a101a105a109a113a117a121a125a129a133a137a141a145a149a153a157a161a165a169a173a177a181a185a189a193a197a201a205a209a213a217a221a225a229a233a237a241a245a

2a4a6a8a11a14a17a20a23a26a29a32a35a38a41a44a47a50a53a56a59a62a65a68a71a74a77a80a83a86a89a92a95a98a102a106a110a114a118a122a126a130a134a138a142a146a150a154a158a162a166a170a174a178a182a186a190a194a198a202a206a210a214a218a222a226a230a234a238a242a246a

a3a5a7a9a12a15a18a21a24a27a30a33a36a39a42a45a48a51a54a57a60a63a66a69a72a75a78a81a84a87a90a93a96a100a104a108a112a116a120a124a128a132a136a140a144a148a152a156a160a164a168a172a176a180a184a188a192a196a200a204a208a212a216a220a224a228a232a236a240a244a248a252a256a@

256 sent but not received - may have been halted at an intermediate point

Was not received - did not receive a return email, may not have been sent by my mail server - hard to test with so many intermediate systems in place i.e. my smtp server, routing servers, mail server, postfix

a3a5a7a9a12a15a18a21a24a27a30a33a36a39a42a45a48a51a54a57a60a63a66a69a72a75a78a81a84a87a90a93a96a99a103a107a111a115a119a123a127a131a135a139a143a147a151a155a159a163a167a171a175a179a183a187a191a195a199a203a207a211a215a219a223a227a231a235a239a243a247a

above sent - but not received - because 256 is too long (it should not really have been sent by my mail server)

create source scan notes

<https://bitbucket.org/naushniki/qamail>

Source scan - can't figure out how to pass in data which might cause the letter_import.rb to fail

qamail.rb
cookie set for 365 day expiry (Checked and this is not what happens - mentioned in notes as possible bug)
could test 404 validation
some have no 404 validation e.g. show session
could check redirect validation
could check conditions in each of the sections

review show_mailbox.erb - could subject be used for xss ?

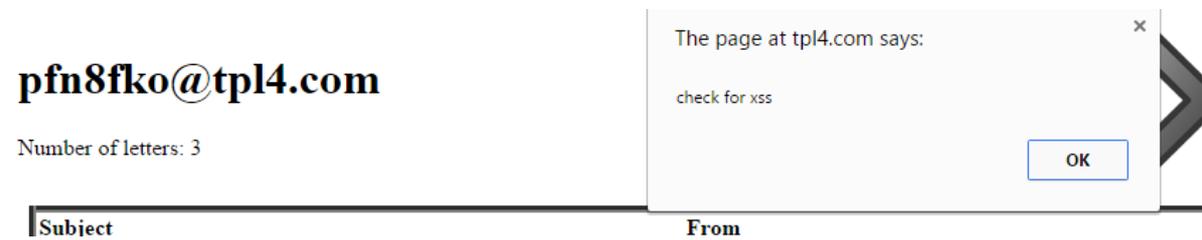
check if show_mailbox.erb can be used for xss

pfn8fko@tpl4.com

```
<script>alert(document.cookie);</script>  
pfn8fko@tpl4.com
```

Vulnerable to xss in title and in body

```
title <script>alert("check for xss");</script>
```

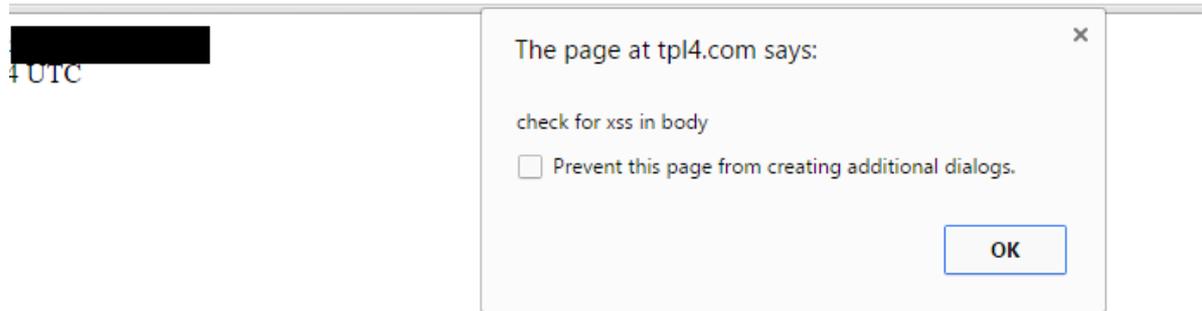


body of message

```
<script>alert("check for xss in body");</script>
```

```
<script>alert("check for xss in body");</script>
```

```
/show_letter?id=101&session_key=sv3Ss4BzivJyNSArMECtscl2&address=pfn8fko@tpl4.com
```



eviltester.com/siteimages/evil_laugh_cleaned_transparent_h300.png

```

```

See http://adomainnamehere.com/show_session?session_key=sv3Ss4BzivJyNSArMECtscl2

Investigate cookie creation

Only created when visit '/' and no cookie set

Cookie set to 08 - 05 - 2025

expected it to be 10th May 2016 - based on using <http://joshnuss.github.io/mruby-web-irb/> and <http://joshnuss.github.io/mruby-web-irb/>

not sure what the expectation around cookie is supposed to be

pfn8fko@tpl4.com

Number of letters: 3



<p>Subject</p>  <p><code></code> injection</p> <p>Blank Subject</p> <p><code><script></code> <code>> injection</code></p> <p>is this bold</p> <p><code>is this bold</code></p>	<p>From: [REDACTED]</p> <p>Date: 2015-05-11 11:01:10 UTC</p> <p>From: [REDACTED]</p> <p>Date: 2015-05-11 11:01:10 UTC</p> <p>Subject: [REDACTED]</p> <p>Show raw message</p> <p>test embedded image</p>  <p>image from subject</p> <p>Image in body of text</p> 
--	--