Securing MetaLib and SFX

Dr. Jason Cooper
Pilkington Library
Loughborough University

Contents

- Introduction
- Known Weaknesses in MetaLib
- Known Weaknesses in SFX
- Securing MetaLib
- Securing SFX
- Reporting Problems

Introduction

- What will this presentation cover?
  - A look at known weaknesses in MetaLib and SFX
  - Securing MetaLib and SFX
  - Reporting security problems
- What won't this presentation cover?
  - General Unix security
  - General network security

Why should we secure our system?

- It is only a matter of time before a machine connected to the internet is targeted
- Once a hacker figures out how to get into a machine they will use that machine to target others more easily
- It can take a long time to rebuild a server that has been messed up by a hacker
- Our servers usually have very fast connections to the internet and large disk space, just what most hackers are looking for

Known Weaknesses in MetaLib Version 2

- Viewing of files (Fixed)
  - Manipulating the URL used to display the help file let anyone view any file visible to the MetaLib user on the server
- Deletion of other users saved searches
  - Adjusting the URL used to delete a saved search it is possible to delete other users saved searches
- Management Interface Exploit
  - After failing to login to the management interface the user is given a phantom session ID (A valid Session ID that is not assigned to any portal)
  - Once the user has a phantom session ID they can manipulate the URL and gain access to the management interface

Known Weaknesses in MetaLib Version 3

- Default Logins / Passwords
  - e.g. The PDS login
- Management Interface Exploit (Fixed)
  - Altered URL from '…./login' to '…./file/main'
- Viewing of files (Fixed)
  - 'http://MetalibServer/V/a?func=file&file_name=../../../../../etc/passwd'

Known Weaknesses in MetaLib Version 3

- tab_management file permissions
  - ‘cat /exlibris/metalib/m3_1/dat01/tab/tab_management’
- Publicly viewable tmp directory (Fixed)
  - Users could access more than just the records they were saving
- Locked resources still accessible (Fixed)

Known Weaknesses in PDS

- Login page over HTTP
- Authentication against CGI scripts over HTTP
  - HTTP is open to being sniffed (Especially as wireless networks are now being used more)

Example of Sniffed HTTP Traffic

POST /pds HTTP/1.1

Host: metalib.lboro.ac.uk

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.0.6) Gecko/20060728 Firefox/1.5.0.6

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: 30

Connection: keep-alive

Content-Type: application/x-www-form-urlencoded

Content-Length: 209

func=login&calling_system=metalib&institute=LOUGHBOROUGH&bor_id=Fred&bor_verification=secret&url=http%3A%2F%2Fhow.lboro.ac.uk%3A80%2FV%2FXXRU1JIK5NA1TSTNM74E6CEH9BRUIA8UHAF1RTPUDQT1BKLK7E-03449%3Ffunc%3Dmeta-1

Example of Sniffed HTTP Traffic

POST /pds HTTP/1.1

Host: metalib.lboro.ac.uk

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.0.6) Gecko/20060728 Firefox/1.5.0.6

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: 30

Connection: keep-alive

Content-Type: application/x-www-form-urlencoded

Content-Length: 209

func=login&calling_system=metalib&institute=LOUGHBOROUGH&bor_id=Fred&bor_verification=secret&url=http%3A%2F%2Fhow.lboro.ac.uk%3A80%2FV%2FXXRU1JIK5NA1TSTNM74E6CEH9BRUIA8UHAF1RTPUDQT1BKLK7E-03449%3Ffunc%3Dmeta-1

Known Weaknesses in SFX

- Default Logins / Passwords
  - E.g. the admin account
  - Each SFX instance has its own set of user accounts so the default passwords will need changing for each instance not just for one

Securing MetaLib and SFX

- Change Default Passwords
  - Do not use weak passwords (e.g. Names or dictionary based words)
  - Include numbers and punctuation in your passwords
  - When changing the password for the PDS user follow the instructions in knowledge base item 6116
  - Don't forget about to change the passwords for all your instances of SFX
- Limit Management Interfaces to Specific IP Range
- Update Regularly (Move from v2 of Metalib to v3)

Securing MetaLib and SFX

- Disable version 2 of MetaLib (ASAP)
- Limit Users Access in the SFX Management Interface to only what they need.
- Use HTTPS for anywhere passwords are being used. (e.g. PDS)

Reporting Problems

- Where to report it and how?
  - Exlibris (Via Pivotal)
- Should I post it to any of the mailing lists?
  - Usually No
- What about if I am not sure if it is a security problem?
  - Report it to Exlibris and let them decide
  - Discuss it with someone you trust in the Metalib / SFX community

Conclusion

- We need to make sure our systems are secure
- Change default passwords
- Keep up to date with the service packs
- Report any security problems you find
- Keep an eye on the apache access logs for URLs you wouldn't expect

Questions?

- Email
  - J.L.Cooper@lboro.ac.uk