# Sec Bug #79099 OOB read in php_strip_tags_ex

**Submitted:** 2020-01-11 07:02 UTC **Modified:** 2020-01-21 07:15 UTC
**From:** wxhusst at gmail dot com **Assigned:** stas (profile)
**Status:** Closed **Package:** Filesystem function related
**PHP Version:** 7.2.26 **OS:** *
**Private report:** No **CVE-ID:** 2020-7059



**[2020-01-11 07:02 UTC] wxhusst at gmail dot com**

```
Description:
------------
sorry. I think this bug is difficult.
I want to reduce the code of explian,  But it can't crash.

Maybe you could know why

first export USE_ZEND_ALLOC=0

then php -f file.php

=================================================================
==6268==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000005d8f at pc 0x000002b3333a bp 0x7ffe57b54b50
sp 0x7ffe57b54b48
READ of size 1 at 0x602000005d8f thread T0
    #0 0x2b33339 in php_strip_tags_ex /home/raven/fuzz/php-src-php-7.4.1/ext/standard/string.c:5383:8
    #1 0x2b3ed07 in php_strip_tags /home/raven/fuzz/php-src-php-7.4.1/ext/standard/string.c:5146:9
    #2 0x2842a9d in zif_fgetss /home/raven/fuzz/php-src-php-7.4.1/ext/standard/file.c:1137:15
    #3 0x354a4d8 in zend_call_function /home/raven/fuzz/php-src-php-7.4.1/Zend/zend_execute_API.c:824:4
    #4 0x239971a in spl_filesystem_file_call /home/raven/fuzz/php-src-php-7.4.1/ext/spl/spl_directory.c:2102:11
    #5 0x239fcea in zim_spl_SplFileObject_fgetss /home/raven/fuzz/php-src-php-7.4.1/ext/spl/spl_directory.c:2863:2
    #6 0x3fe5c26 in ZEND_DO_FCALL_SPEC_RETVAL_UNUSED_HANDLER /home/raven/fuzz/php-src-php-
7.4.1/Zend/zend_vm_execute.h:1617:4
    #7 0x3c03f76 in execute_ex /home/raven/fuzz/php-src-php-7.4.1/Zend/zend_vm_execute.h:53379:7
    #8 0x3c0513f in zend_execute /home/raven/fuzz/php-src-php-7.4.1/Zend/zend_vm_execute.h:57664:2
    #9 0x36b4324 in zend_execute_scripts /home/raven/fuzz/php-src-php-7.4.1/Zend/zend.c:1663:4
    #10 0x2fa0ab1 in php_execute_script /home/raven/fuzz/php-src-php-7.4.1/main/main.c:2619:14
    #11 0x4626bc7 in do_cli /home/raven/fuzz/php-src-php-7.4.1/sapi/cli/php_cli.c:961:5
    #12 0x4621885 in main /home/raven/fuzz/php-src-php-7.4.1/sapi/cli/php_cli.c:1352:18
    #13 0x7f2d114501e2 in __libc_start_main /build/glibc-4WA41p/glibc-2.30/csu/../csu/libc-start.c:308:16
    #14 0x60297d in _start (/home/raven/fuzz/php-src-php-7.4.1/sapi/cli/php+0x60297d)

0x602000005d8f is located 1 bytes to the left of 16-byte region [0x602000005d90,0x602000005da0)
allocated by thread T0 here:
    #0 0x67a87d in malloc (/home/raven/fuzz/php-src-php-7.4.1/sapi/cli/php+0x67a87d)
    #1 0x33698f4 in __zend_malloc /home/raven/fuzz/php-src-php-7.4.1/Zend/zend_alloc.c:2975:14
    #2 0x3367b4e in _malloc_custom /home/raven/fuzz/php-src-php-7.4.1/Zend/zend_alloc.c:2416:10
    #3 0x3367447 in _emalloc /home/raven/fuzz/php-src-php-7.4.1/Zend/zend_alloc.c:2535:10
    #4 0x336a28d in _estrndup /home/raven/fuzz/php-src-php-7.4.1/Zend/zend_alloc.c:2633:15
    #5 0x2b302cc in php_strip_tags_ex /home/raven/fuzz/php-src-php-7.4.1/ext/standard/string.c:5180:8
    #6 0x2b3ed07 in php_strip_tags /home/raven/fuzz/php-src-php-7.4.1/ext/standard/string.c:5146:9
    #7 0x2842a9d in zif_fgetss /home/raven/fuzz/php-src-php-7.4.1/ext/standard/file.c:1137:15
    #8 0x354a4d8 in zend_call_function /home/raven/fuzz/php-src-php-7.4.1/Zend/zend_execute_API.c:824:4
    #9 0x239971a in spl_filesystem_file_call /home/raven/fuzz/php-src-php-7.4.1/ext/spl/spl_directory.c:2102:11
    #10 0x239fcea in zim_spl_SplFileObject_fgetss /home/raven/fuzz/php-src-php-7.4.1/ext/spl/spl_directory.c:2863:2
    #11 0x3fe5c26 in ZEND_DO_FCALL_SPEC_RETVAL_UNUSED_HANDLER /home/raven/fuzz/php-src-php-
7.4.1/Zend/zend_vm_execute.h:1617:4
    #12 0x3c03f76 in execute_ex /home/raven/fuzz/php-src-php-7.4.1/Zend/zend_vm_execute.h:53379:7
    #13 0x3c0513f in zend_execute /home/raven/fuzz/php-src-php-7.4.1/Zend/zend_vm_execute.h:57664:2
    #14 0x36b4324 in zend_execute_scripts /home/raven/fuzz/php-src-php-7.4.1/Zend/zend.c:1663:4
    #15 0x2fa0ab1 in php_execute_script /home/raven/fuzz/php-src-php-7.4.1/main/main.c:2619:14
    #16 0x4626bc7 in do_cli /home/raven/fuzz/php-src-php-7.4.1/sapi/cli/php_cli.c:961:5
    #17 0x4621885 in main /home/raven/fuzz/php-src-php-7.4.1/sapi/cli/php_cli.c:1352:18
    #18 0x7f2d114501e2 in __libc_start_main /build/glibc-4WA41p/glibc-2.30/csu/../csu/libc-start.c:308:16

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/raven/fuzz/php-src-php-7.4.1/ext/standard/string.c:5383:8 in
php_strip_tags_ex
Shadow bytes around the buggy address:
  0x0c047fff8b60: fa fa 00 06 fa fa 00 04 fa fa 00 02 fa fa 00 00
  0x0c047fff8b70: fa fa 04 fa fa fa 05 fa fa fa 00 02 fa fa 00 03
  0x0c047fff8b80: fa fa 00 07 fa fa 00 01 fa fa 00 00 fa fa fd fa
  0x0c047fff8b90: fa fa 02 fa fa fa 00 03 fa fa 00 03 fa fa 00 03
  0x0c047fff8ba0: fa fa 02 fa fa fa 01 fa fa fa fd fd fa fa fd fa
=>0x0c047fff8bb0: fa[fa]00 00 fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8bc0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8bd0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8be0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8bf0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8c00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
```

```
==6268==ABORTING

Test script:
---------------
<?php

// $ref_bool = true;
// $ref_int = 0;
// $ref_string = "a";
// $ref_array = array(0);
// $ref_object = new StdClass();
// $ref_resource = fopen("/dev/null", "r");

function templateFunction($templateParameter) {
        return 0;
}

function templateGenerator() {
        yield 0;
}

class TemplateClass {
        var $templateProperty;
        const TEMPLATE_CONSTANT = 0;
        function templateMethod() {
                return 0;
        }
}

$p = new Phar("/tmp/fuzz.phar");
$p["fuzz.txt"] = "fuzz";

$vars = array(
        "stdClass"                      => new stdClass(),
        "Exception"                     => new Exception(),
        "ErrorException"                => new ErrorException(),
        "Error"                         => new Error(),
        "CompileError"                  => new CompileError(),
        "ParseError"                    => new ParseError(),
        "TypeError"                     => new TypeError(),
        "ArgumentCountError"            => new ArgumentCountError(),
        "ArithmeticError"               => new ArithmeticError(),
        "DivisionByZeroError"           => new DivisionByZeroError(),
//      "Closure"                       => new Closure(),
//      "Generator"                     => new Generator(),
        "ClosedGeneratorException"      => new ClosedGeneratorException(),
        "DateTime"                      => new DateTime(),
        "DateTimeImmutable"             => new DateTimeImmutable(),
        "DateTimeZone"                  => new DateTimeZone("America/Chicago"),
        "DateInterval"                  => new DateInterval("P2Y4DT6H8M"),
        "DatePeriod"                    => new DatePeriod("R4/2012-07-01T00:00:00Z/P7D"),
        "LibXMLError"                   => new LibXMLError(),
        "DOMException"                  => new DOMException(),
        "DOMStringList"                 => new DOMStringList(),
        "DOMNameList"                   => new DOMNameList(),
        "DOMImplementationList"         => new DOMImplementationList(),
        "DOMImplementationSource"       => new DOMImplementationSource(),
        "DOMImplementation"             => new DOMImplementation(),
        "DOMNode"                       => new DOMNode(),
        "DOMNameSpaceNode"              => new DOMNameSpaceNode(),
        "DOMDocumentFragment"           => new DOMDocumentFragment(),
        "DOMDocument"                   => new DOMDocument(),
        "DOMNodeList"                   => new DOMNodeList(),
        "DOMNamedNodeMap"               => new DOMNamedNodeMap(),
        "DOMCharacterData"              => new DOMCharacterData(),
        "DOMAttr"                       => new DOMAttr("artr"),
        "DOMElement"                    => new DOMElement("root"),
        "DOMText"                       => new DOMText(),
        "DOMComment"                    => new DOMComment(),
        "DOMTypeinfo"                   => new DOMTypeinfo(),
        "DOMUserDataHandler"            => new DOMUserDataHandler(),
        "DOMDomError"                   => new DOMDomError(),
        "DOMErrorHandler"               => new DOMErrorHandler(),
        "DOMLocator"                    => new DOMLocator(),
        "DOMConfiguration"              => new DOMConfiguration(),
        "DOMCdataSection"               => new DOMCdataSection("root value"),
        "DOMDocumentType"               => new DOMDocumentType(),
        "DOMNotation"                   => new DOMNotation(),
        "DOMEntity"                     => new DOMEntity(),
        "DOMEntityReference"            => new DOMEntityReference("nbsp"),
        "DOMProcessingInstruction"      => new DOMProcessingInstruction("php"),
        "DOMStringExtend"               => new DOMStringExtend(),
        "DOMXPath"                      => new DOMXPath(new DOMDocument()),
        "finfo"                         => new finfo(),
//      "HashContext"                   => new HashContext(),
        "JsonException"                 => new JsonException(),
        "LogicException"                => new LogicException(),
        "BadFunctionCallException"      => new BadFunctionCallException(),
        "BadMethodCallException"        => new BadMethodCallException(),
        "DomainException"               => new DomainException(),
        "InvalidArgumentException"      => new InvalidArgumentException(),
        "LengthException"               => new LengthException(),
        "OutOfRangeException"           => new OutOfRangeException(),
        "RuntimeException"              => new RuntimeException(),
        "OutOfBoundsException"          => new OutOfBoundsException(),
        "OverflowException"             => new OverflowException(),
        "RangeException"                => new RangeException(),
        "UnderflowException"            => new UnderflowException(),
        "UnexpectedValueException"      => new UnexpectedValueException(),
/*
        "RecursiveIteratorIterator"     => new RecursiveIteratorIterator(),
        "IteratorIterator"              => new IteratorIterator(),
        "FilterIterator"                => new FilterIterator(),
        "RecursiveFilterIterator"       => new RecursiveFilterIterator(),
        "CallbackFilterIterator"        => new CallbackFilterIterator(),
        "RecursiveCallbackFilterIterator" => new RecursiveCallbackFilterIterator(),
        "ParentIterator"                => new ParentIterator(),
```

```
        "LimitIterator"                 => new LimitIterator(),
        "CachingIterator"               => new CachingIterator(),
        "RecursiveCachingIterator"      => new RecursiveCachingIterator(),
        "NoRewindIterator"              => new NoRewindIterator(),
        "AppendIterator"                => new AppendIterator(),
        "InfiniteIterator"              => new InfiniteIterator(),
        "RegexIterator"                 => new RegexIterator(),
        "RecursiveRegexIterator"        => new RecursiveRegexIterator(),
        "EmptyIterator"                 => new EmptyIterator(),
        "RecursiveTreeIterator"         => new RecursiveTreeIterator(),
        "ArrayObject"                   => new ArrayObject(),
        "ArrayIterator"                 => new ArrayIterator(),
        "RecursiveArrayIterator"        => new RecursiveArrayIterator(),
        "SplFileInfo"                   => new SplFileInfo(),
        "DirectoryIterator"             => new DirectoryIterator(),
        "FilesystemIterator"            => new FilesystemIterator(),
        "RecursiveDirectoryIterator"    => new RecursiveDirectoryIterator(),
        "GlobIterator"                  => new GlobIterator(),
*/
        "SplFileObject"                 => new SplFileObject(__FILE__),
        "SplTempFileObject"             => new SplTempFileObject(),
        "SplDoublyLinkedList"           => new SplDoublyLinkedList(),
        "SplQueue"                      => new SplQueue(),
        "SplStack"                      => new SplStack(),
//      "SplHeap"                       => new SplHeap(),
        "SplMinHeap"                    => new SplMinHeap(),
        "SplMaxHeap"                    => new SplMaxHeap(),
        "SplPriorityQueue"              => new SplPriorityQueue(),
        "SplFixedArray"                 => new SplFixedArray(),
        "SplObjectStorage"              => new SplObjectStorage(),
        "MultipleIterator"              => new MultipleIterator(),
/*
        "PDOException"                  => new PDOException(),
        "PDO"                           => new PDO(),
        "PDOStatement"                  => new PDOStatement(),
        "PDORow"                        => new PDORow(),
*/
        "SessionHandler"                => new SessionHandler(),
        "ReflectionException"           => new ReflectionException(),
        "Reflection"                    => new Reflection(),
//      "ReflectionFunctionAbstract"    => new ReflectionFunctionAbstract(),
        "ReflectionFunction"            => new ReflectionFunction("templateFunction"),
        "ReflectionGenerator"           => new ReflectionGenerator(templateGenerator()),
        "ReflectionParameter"           => new ReflectionParameter("templateFunction", "templateParameter"),
        "ReflectionType"                => (new ReflectionClass("ZipArchive"))->getMethod("getCommentName")-
>getReturnType(),
        "ReflectionNamedType"           => new ReflectionNamedType(),
        "ReflectionMethod"              => new ReflectionMethod("TemplateClass", "templateMethod"),
        "ReflectionClass"               => new ReflectionClass("TemplateClass"),
        "ReflectionObject"              => new ReflectionObject(new TemplateClass()),
        "ReflectionProperty"            => new ReflectionProperty("TemplateClass", "templateProperty"),
        "ReflectionClassConstant"       => new ReflectionClassConstant("TemplateClass", "TEMPLATE_CONSTANT"),
        "ReflectionExtension"           => new ReflectionExtension("Reflection"),

);


try { try { $vars["SplFileObject"]->fgetss(str_repeat(chr(6), 17) + str_repeat(chr(226), 65)); } catch (Exception $e)
{ } } catch(Error $e) { }

try { try { $vars["SplFileObject"]->fseek(3, 5); } catch (Exception $e) { } } catch(Error $e) { }

try { try { $vars["SplFileObject"]->fgetss(implode(array_map(function($c) {return "\\x" . str_pad(dechex($c), 2,
"0");}, range(0, 255)))); } catch (Exception $e) { } } catch(Error $e) { }

?>

Expected result:
----------------
normal

Actual result:
--------------
crash
```

## Patches

Add a Patch

## Pull Requests

Add a Pull Request

## History

All | Comments | Changes | Git/SVN commits | Related reports

**[2020-01-14 11:41 UTC] cmb@php.net**

```
-Summary: SUMMARY: AddressSanitizer: heap-buffer-overflow /home/raven/fuzz/php-src-php-7.
+Summary: OOB read in php_strip_tags_ex
-Status: Open
+Status: Verified
-Package: Unknown/Other Function
+Package: Filesystem function related
-PHP Version: 7.4.1
+PHP Version: 7.2.26
-Assigned To:
+Assigned To: stas
```

**[2020-01-14 11:41 UTC] cmb@php.net**

```
Thanks for reporting!  A simpler reproducer:

<?php
$stream = fopen('php://memory', 'w+');
fputs($stream, "<?\n\"\n");
```

```
rewind($stream);
var_dump(fgetss($stream));
var_dump(fgetss($stream));
?>
```

There are two more similar issues.  Suggested patch for PHP-7.2:
<https://gist.github.com/cmb69/eff31156c4a14cf0887f1347b0439eff>.

Merging into PHP-7.3 will conflict because the strip tags parser
has been refactored.  Resolving these conflicts manually shouldn't
be hard, though.

Stas, can you please handle this ticket?

**[2020-01-14 11:41 UTC] cmb@php.net**

```
-Operating System: linux
+Operating System: *
```

**[2020-01-21 05:28 UTC] stas@php.net**

```
-CVE-ID:
+CVE-ID: 2020-7059
```

**[2020-01-21 07:16 UTC] stas@php.net**

Automatic comment on behalf of stas
Revision: http://git.php.net/?p=php-src.git;a=commit;h=0f79b1bf301f455967676b5129240140c5c45b09
Log: Fix #79099: OOB read in php_strip_tags_ex

**[2020-01-21 07:16 UTC] stas@php.net**

```
-Status: Verified
+Status: Closed
```