Interpreters Under Pressure

a.k.a. fuzzing languages for lulz

Andrzej Dyjak, WarCon 2017

Intro
(whoami etc)

Outline

- Revelation
- Initial experiment
- Initial results
- More experiments
- More results
- Future Work
- References
- Q&A

Revelation

What if I… 🤔

Initial experiment

Where’s my duct tape? 👨‍🔬

Initial results

Wait, what? 😳

Why did I switch to *dead languages?
Should’ve go with mainstream ones…

* Although I’ve heard greek is still alive 💪

More experiments

Even more duct tape! 🤘

More results

	PHP	HHVM	Ruby	Python
	(php-7.1.1-asan)	(hhvm-3.15.6-dev)	(mri-2.4.0-asan)	(cpython-2.7.13-asan)
EXPLOITABLE	**58**	**35**	**74**	**2**
PROBABLY_EXPLOITABLE	**8**	**0**	**0**	**2**
PROBABLY_NOT_EXPLOITABLE	**8**	**0**	**2**	**4**
UNKNOWN	**12**	**5**	**5**	**3**

*Classification done with gdb !exploitable 😎

Future Work

Be smart.
Don’t be dumb.
😎

References

Standing on the shoulders of giants. 🙌

- https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/holler
- https://sean.heelan.io/2016/04/26/fuzzing-language-interpreters-using-regression-tests/
- https://vimeo.com/181078970
- https://docs.google.com/presentation/d/1vvl34hw0pAyFeNo-oqJnMUg8zsKIVNj0NHOKxdW-UEs/edit?pref=2&pli=1#slide=id.p
- https://infiltratecon.com/downloads/sean_heelan_2014_slides.pdf
- https://github.com/SeanHeelan/Malamute
- https://sean.heelan.io/2012/07/10/better-interpreter-fuzzing-with-clang/
- https://github.com/SeanHeelan/InterParser
- https://blog.exodusintel.com/2017/01/03/gramfuzz/
- https://users.own-hero.net/~decoder/holler-mthesis-2011.pdf
- https://people.csail.mit.edu/akiezun/pldi-kiezun.pdf
- https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/tr-2007-154.pdf
- https://theory.stanford.edu/~aiken/publications/new/InputGrammars.pdf
- https://github.com/silviocesare/Fuzzer
- https://www.usenix.org/legacy/event/lisa06/tech/slides/kaminsky.pdf
- https://www.usenix.org/legacy/event/woot08/tech/full_papers/viide/viide.pdf

- https://www.slideshare.net/logicaltrust/torturing-the-php-interpreter
- https://www.slideshare.net/logicaltrust/201105-owasp-fuzzing-interpretera-php
- http://php-security.org/2010/05/11/mops-submission-05-the-minerva-php-fuzzer/index.html
- https://www.evonide.com/how-we-broke-php-hacked-pornhub-and-earned-20000-dollar/
- https://www.evonide.com/fuzzing-unserialize/
- https://www.evonide.com/breaking-phps-garbage-collection-and-unserialize/
- https://github.com/80vul/phpcodz
- http://www.agarri.fr/en/publications.html
- https://medium.com/@dgryski/fuzzing-perl-xs-modules-with-afl-4bfc2335dd90
- http://www.geeknik.net/71nvhf1fp
- http://blogs.perl.org/users/rurban/2011/11/adventures-with-clang-and-asan.html
- http://blogs.perl.org/users/rurban/2012/03/address-sanitizer-round-2.html
- http://tomforb.es/segfaulting-python-with-afl-fuzz

Q/A

Did I answer your question? 😎

Peace Out ✌️

https://dyjak.me
Twitter: **@andrzejdyjak**
Github: **@dyjakan**