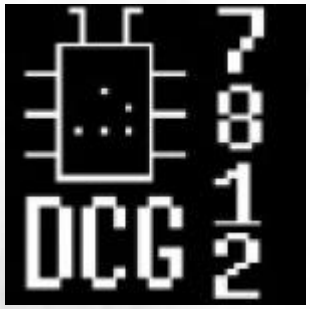
Python Arsenal for Reverse Engineering

Dmitry "D1g1" Evdokimov

DSecRG, Security Researcher

#whoami

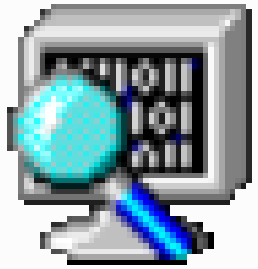
- Security Researcher in DSecRG
  - RE
  - Fuzzing
  - Mobile security
- Organizer: DCG #7812
- Editor in “XAKEP”



ERPScan
Security Scanner for SAP

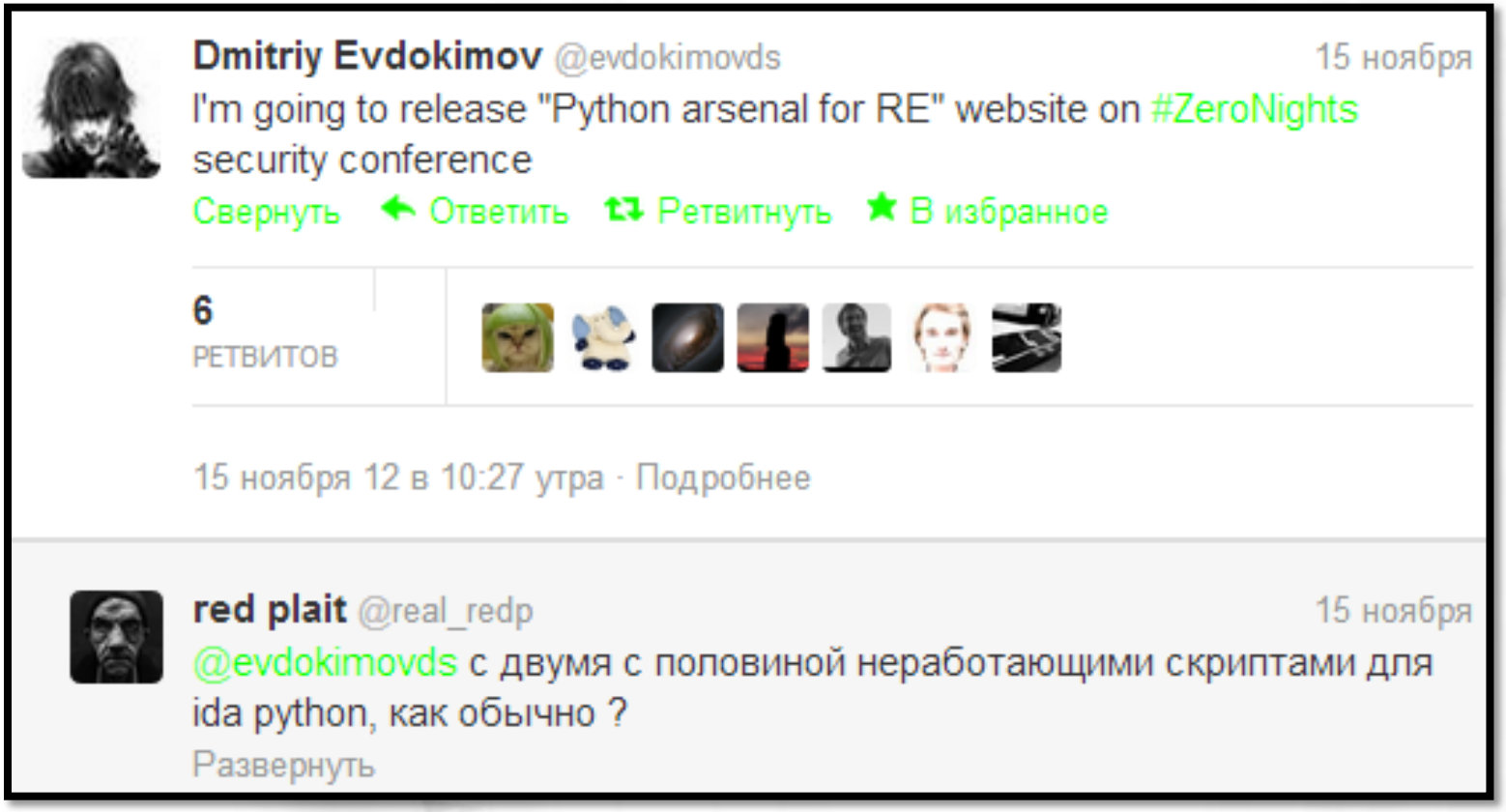
Intro

OllyDbg



GDB
The GNU Project
Debugger

Perl?!



Perl binding for IDA Pro: http://cyrplw.svn.sourceforge.net/viewvc/cyrplw/perl/

http://redplait.blogspot.ru/2011/08/perl-inside-ida-pro.html

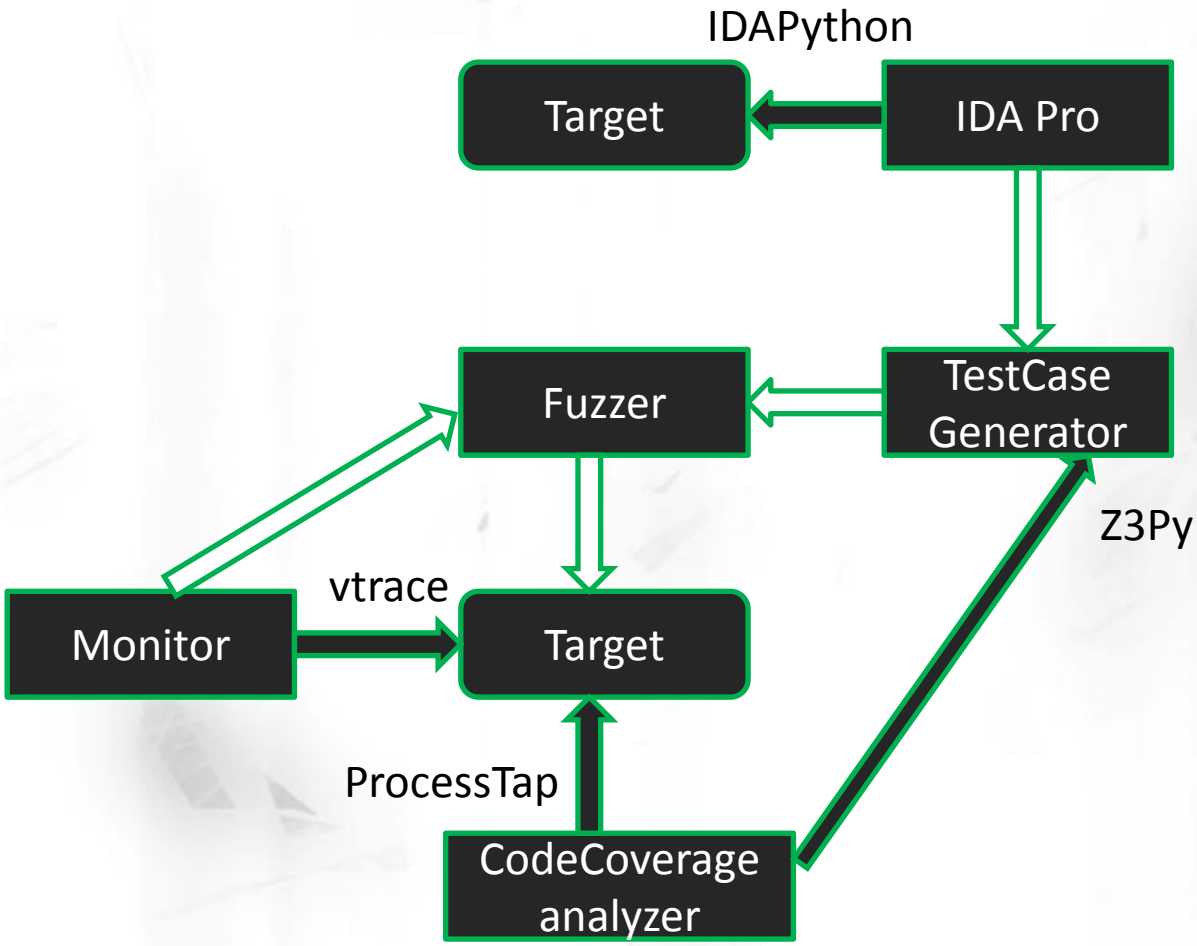
Ruby?

- Metasm - the Ruby assembly manipulation suite
- Idarub - Ruby plugin for IDAPro
- Ragweed - scriptable Win32/Linux/OSX debugger written in ruby
- frasm - Ruby bindings for distorm64
- LeafRub - x86 ELF Analysis and Debugging
- rbkb - A miscellaneous collection of command-line tools and ruby library helpers related to pen-testing and reversing
- jdi_hook - JRuby based scriptable Java debugger using the JDI interface
- ???

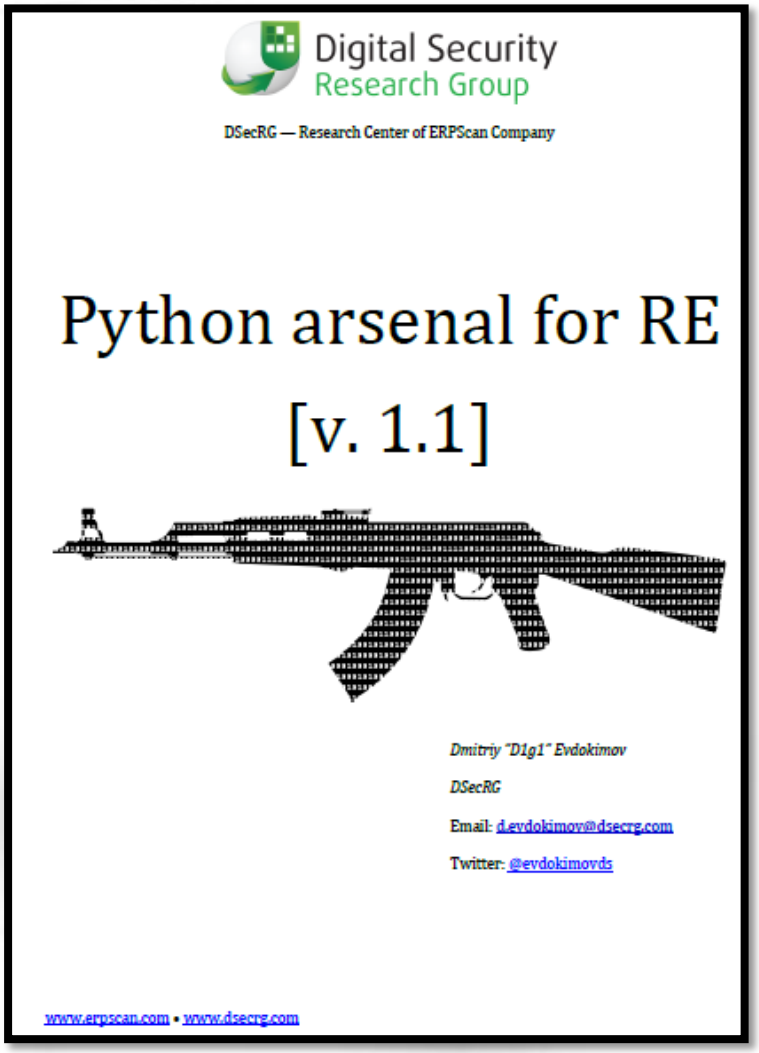
Python!

BeaEnginePython
bochs-python-instrumentation
Buggery
Ctypes
Deviare
dislib
diStorm
FrASM
IDAPython
ImmLIB
libdisassemble
lldb
llvmpy
Macholib
Miasm
OllyPython
PDBparse
PEEL
pefile
PIDA
PinPy
ProcessTap
pyasm
PyBox
PyCodin
pydasm
Pydb
PyDBG
PyDbgEng
pydbgr
PyDevTools
pydot
pydusa
PyEA
PyELF
Pyelftools
PyEMU
pyew
pygdb
pyHIEW
pykd
Pylibemu
pylibscizzle
pyMem
pymsasid
pyREtic
PySTP
python-adb
python-haystack
python-ptrace
PythonGdb
pytracer
radapy
ramooflax
uhooker
Vivisect
vtrace
WinAppDbg
Z3-python
Z3Py
…

Example


IDAPython
Target
IDA Pro
Fuzzer
TestCase Generator
Z3Py
vtrace
Monitor
Target
ProcessTap
CodeCoverage analyzer

The first idea

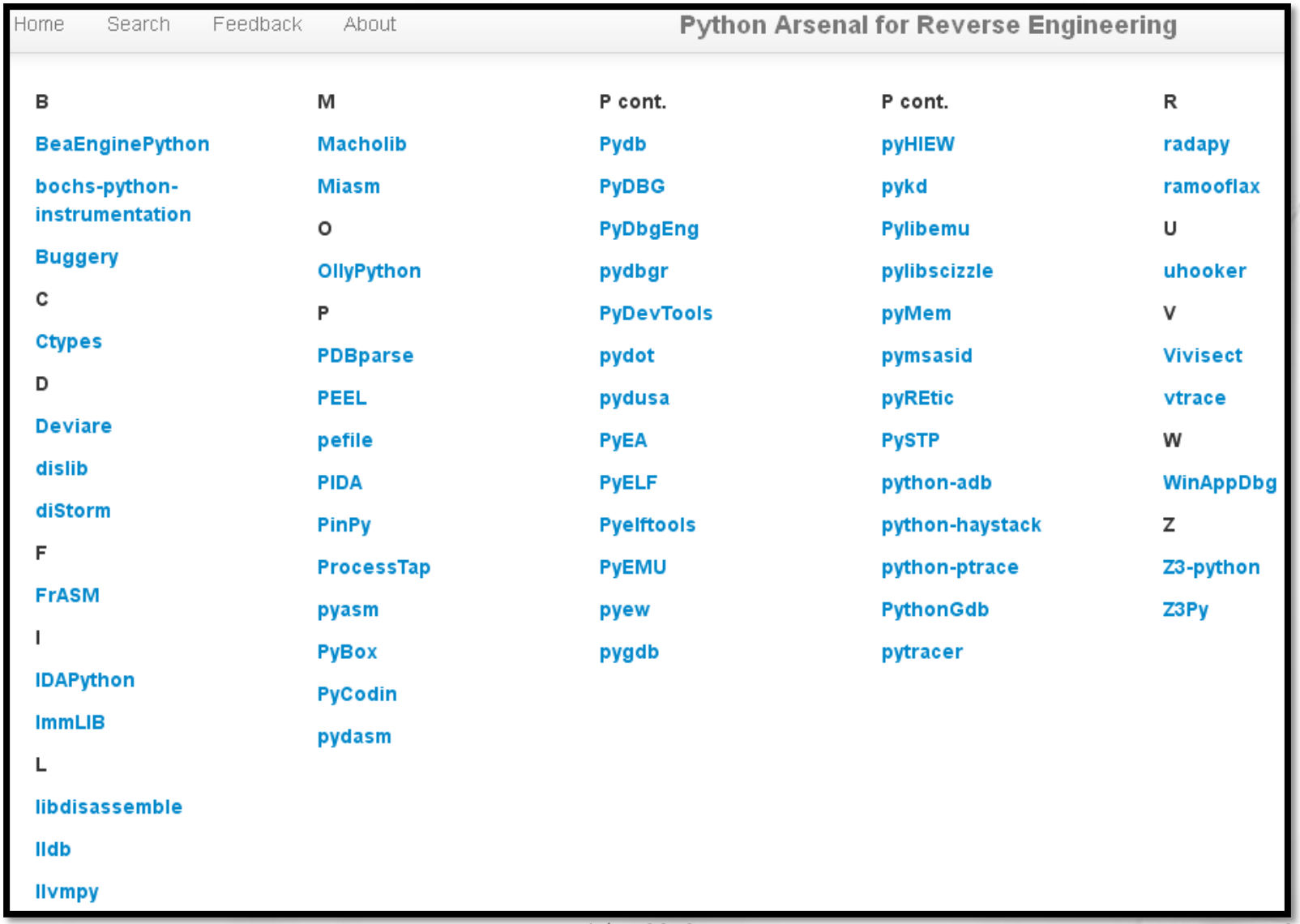


Web portal

http://pythonarsenal.dsecrg.ru/

http://pythonarsenal.erpscan.com/

Site:Main


Home
Search
Feedback
About
Python Arsenal for Reverse Engineering
B
BeaEnginePython
bochs-python-instrumentation
Buggery
C
Ctypes
D
Deviare
dislib
diStorm
F
FrASM
I
IDAPython
ImmLIB
L
libdisassemble
lldb
llvmpy
M
Macholib
Miasm
O
OllyPython
P
PDBparse
PEEL
pefile
PIDA
PinPy
ProcessTap
pyasm
PyBox
PyCodin
pydasm
P cont.
Pydb
PyDBG
PyDbgEng
pydbgr
PyDevTools
pydot
pydusa
PyEA
PyELF
Pyelftools
PyEMU
pyew
pygdb
P cont.
pyHIEW
pykd
Pylibemu
pylibscizzle
pyMem
pymsasid
pyREtic
PySTP
python-adb
python-haystack
python-ptrace
PythonGdb
pytracer
R
radapy
ramooflax
U
uhooker
V
Vivisect
vtrace
W
WinAppDbg
Z
Z3-python
Z3Py

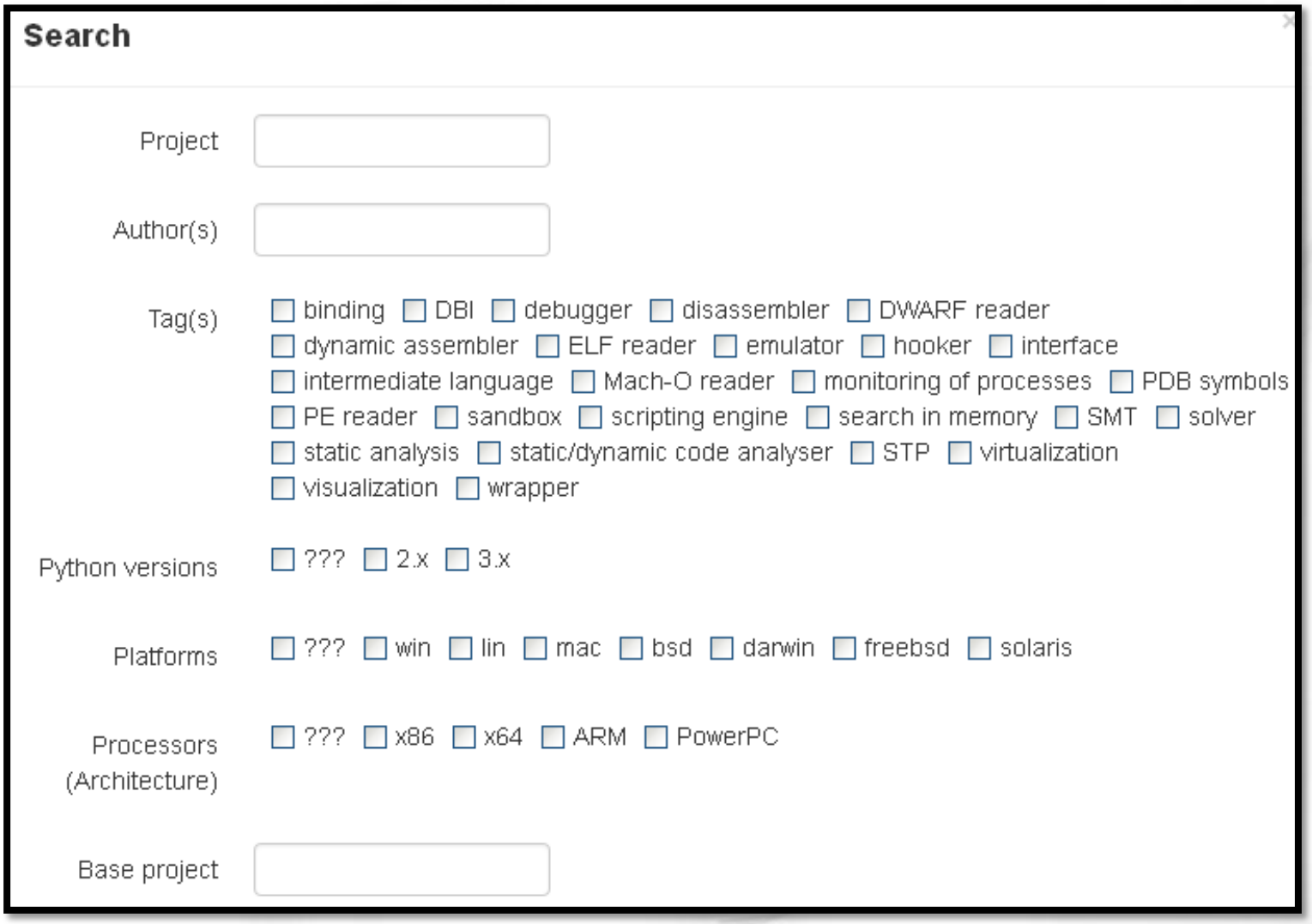
Library:Description

bochs-python-instrumentation

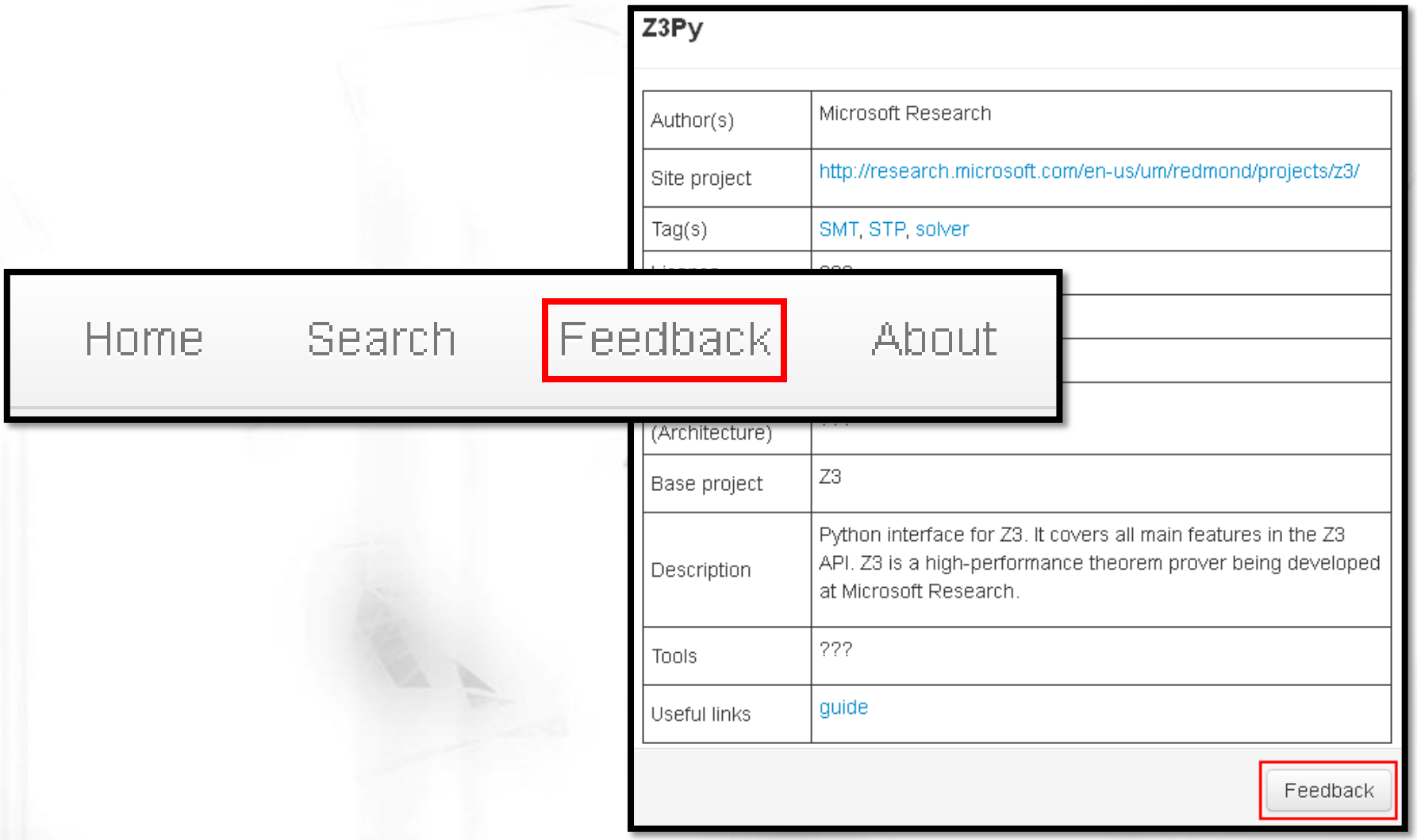
Author(s)	Ero Carrera (@erocarrera)
Site project	https://github.com/zynamics/bochs-python-instrumentation
Tag(s)	debugger, emulator
License	???
Python versions	2.5
Platforms	win/lin
Processors (Architecture)	x86/x64
Base project	Bochs (2.4.5 and 2.4.6)
Description	This patch for Bochs provides a Python interpreter instead of Bochs' own debugger, yet still providing the debugger functionality. It also allows to interact with the instrumentation interface on-demand, by dynamically associating Python methods to handle instrumentation events.
Tools	???

Feedback

Site:Search


Search
Project
Author(s)
Tag(s)
binding DBI debugger disassembler DWARF reader
dynamic assembler ELF reader emulator hooker interface
intermediate language Mach-O reader monitoring of processes PDB symbols
PE reader sandbox scripting engine search in memory SMT solver
static analysis static/dynamic code analyser STP virtualization
visualization wrapper
Python versions
??? 2.x 3.x
Platforms
??? win lin mac bsd darwin freebsd solaris
Processors (Architecture)
??? x86 x64 ARM PowerPC
Base project

Site:Feedback



Conclusion

- Gratz!
  - Anton Astafiev

- Future work
  - Update/implementation/fix
  - Development
    - News
    - Statistics/graph/chart

Contact

Twitter: @evdokimovds

E-mail: d.evdokimov@dsecrg.com