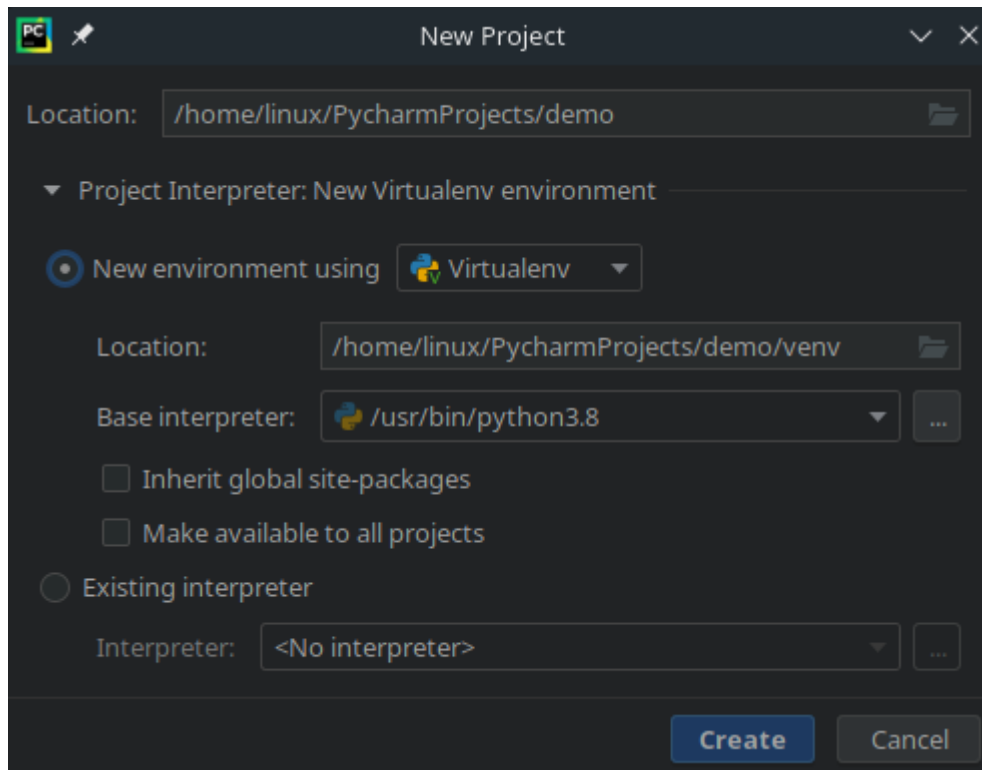


Chapter 1: Working with Python Scripting



```
params_global_argparse
params_global_argparse.py x
1 import argparse
2
3
4 class Parameters:
5     """Global parameters"""
6
7     def __init__(self, **kwargs):
8         self.param1 = kwargs.get("param1")
9         self.param2 = kwargs.get("param2")
10
11
12 def view_parameters(input_parameters):
13     print(input_parameters.param1)
14     print(input_parameters.param2)
15
16
17 parser = argparse.ArgumentParser(description='Testing parameters')
18 parser.add_argument("-p1", dest="param1", help="parameter1")
19 parser.add_argument("-p2", dest="param2", help="parameter2")
20
21 params = parser.parse_args()
```

params_global_argparse.py:13

- Python Line Breakpoint
 - params_global_argparse.py:1
- Python Exception Breakpoint

Enabled

Suspend: All Thread

Condition:

Log: "Breakpoint hit" message Stack trace

Evaluate and log:

Remove once hit

Disable until hitting the following breakpoint:

<None>

After hit: Disable again Leave enabled

```
11
12 def view_parameters(input_parameters):
13     print(input_parameters.param1)
14     print(input_parameters.param2)
15
```

Done

Debug: params_global_argparse

Debugger Console

Frames

- MainThread
- view_parameters, params_global_argp.
- <module>, params_global_argparse.py

Variables

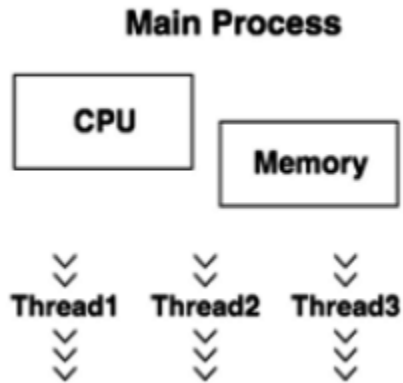
- input_parameters = (Parameters) <_main_...Parameter> object at 0x7f1217d734c0
 - param1 = (str) 'parameter1'
 - param2 = (str) 'parameter2'
- params = (Namespace) Namespace(param1='parameter1', param2='parameter2')
 - param1 = (str) 'parameter1'
 - param2 = (str) 'parameter2'
- parser = (ArgumentParser) ArgumentParser(prog='params_global_argparse.py', usage=None, description='Testing parameters', formatter_class=<class 'argparse...
- Special Variables
 - __file__ = (str) '/home/linux/PycharmProjects/demo/params_global_argparse.py'
 - __name__ = (str) '__main__'
 - __builtins__ = (module) <module 'builtins' (built-in)>

```
File Edit Format Run Options Window Help
1 try:
2     f = open('file.txt','r')
3 except Exception as exception:
4     print("File not found:",exception)

Python 3.8.2 Shell
File Edit Shell Debug Options Window Help
Python 3.8.2 (default, Apr  8 2020, 14:31:25)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: /home/linux/Desktop/demo.py =====
File not found: [Errno 2] No such file or directory: 'file.txt'
>>> |
```

Chapter 2: System Programming Packages

```
class Thread(_Verbose)
| A class that represents a thread of control.
|
| This class can be safely subclassed in a limited fashion.
|
| Method resolution order:
|   Thread
|   _Verbose
|   __builtin__.object
|
| Methods defined here:
|
| __init__(self, group=None, target=None, name=None, args=(), kwargs=None, verbose=None)
```



Chapter 3: Socket Programming

No Images

Chapter 4: HTTP Programming

Schemes

HTTP

HTTP Methods Testing different HTTP verbs



- DELETE** /delete "The request's DELETE parameters."
- GET** /get The request's query parameters.
- PATCH** /patch The request's PATCH parameters.
- POST** /post The request's POST parameters.
- PUT** /put The request's PUT parameters.

POST /post The request's POST parameters.

Parameters Cancel

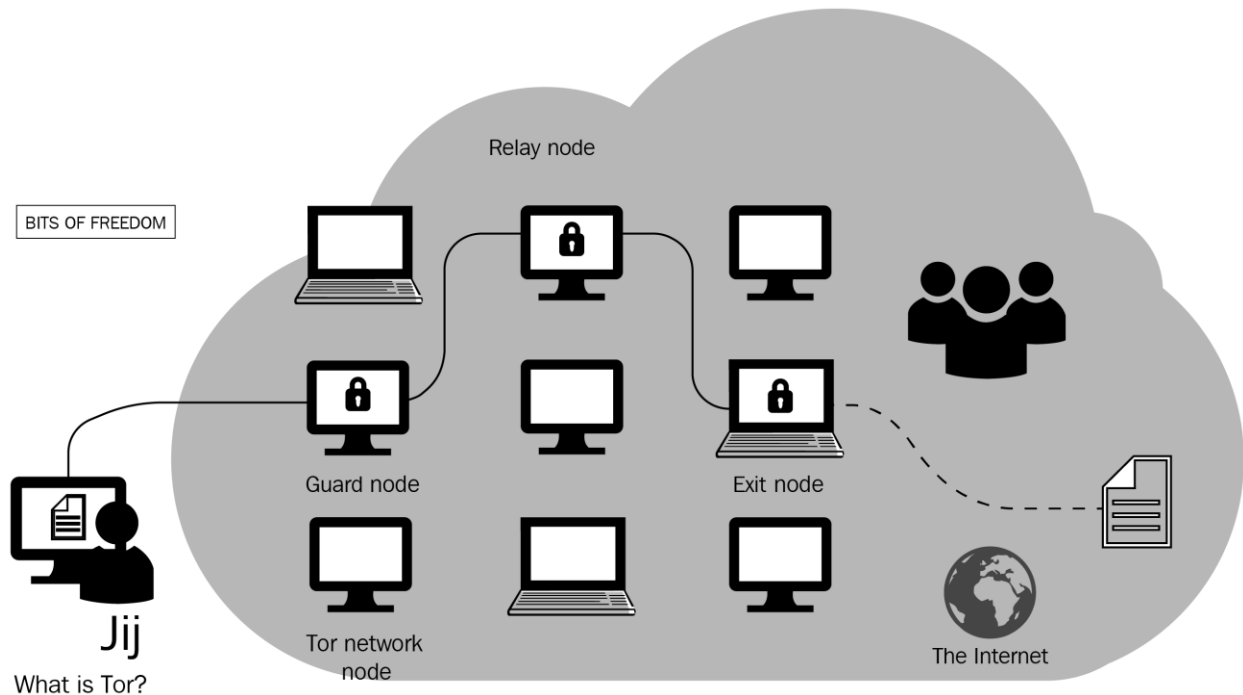
No parameters

Execute

Responses Response content type application/json v

Code	Description
200	<i>The request's POST parameters.</i>

Chapter 5: Connecting to the Tor Network and Discovering Hidden Services



Congratulations. Your browser is configured to use Tor.

Please refer to the [Tor website](#) for further information about using Tor safely. You are now free to browse the Internet anonymously.

```
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
   Loaded: loaded (/lib/systemd/system/tor.service; enabled; vendor preset: enab
   Active: active (exited) since jue 2020-03-19 22:28:59 CET; 3s ago
   Process: 3217 ExecReload=/bin/true (code=exited, status=0/SUCCESS)
   Process: 20228 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 20228 (code=exited, status=0/SUCCESS)
   Tasks: 0
   Memory: 0B
   CPU: 0 (by default, the Tor client uses port 9050)
   CGroup: /system.slice/tor.service

mar 19 22:28:59 jmoc-HP-Compaq-6005-Pro-SFF-PC systemd[1]: Starting Anonymizing
mar 19 22:28:59 jmoc-HP-Compaq-6005-Pro-SFF-PC systemd[1]: Started Anonymizing o
```



```
## Configuration file for a typical Tor user
## Last updated 22 September 2015 for Tor 0.2.7.3-alpha.
## (may or may not work for much older or much newer versions of Tor.)
##
## Lines that begin with "## " try to explain what's going on. Lines
## that begin with just "#" are disabled commands: you can enable them
## by removing the "#" symbol.
##
## See 'man tor', or https://www.torproject.org/docs/tor-manual.html,
## for more options you can use in this file.
##
## Tor will look for this file in various places based on your platform:
## https://www.torproject.org/docs/faq#torrc
##
## Tor opens a SOCKS proxy on port 9050 by default -- even if you don't
## configure one below. Set "SOCKSPort 0" if you plan to run Tor only
## as a relay, and not make any local application connections yourself.
#SOCKSPort 9050 # Default: Bind to localhost:9050 for local connections.
#SOCKSPort 192.168.0.1:9100 # Bind to this address:port too.
```

```
Tor 0.2.9.14 running on Linux with Libevent 2.0.21-stable,
Tor can't help you if you use it wrong! Learn how to be
Read configuration file "/etc/tor/torrc".
controlPort is open, but no authentication method has been
pgrade your Tor controller as soon as possible.
Opening Socks listener on 127.0.0.1:9050
Opening Control listener on 127.0.0.1:9051
Bootstrapped 0%: Starting
Bootstrapped 80%: Connecting to the Tor network
Bootstrapped 85%: Finishing handshake with first hop
Bootstrapped 90%: Establishing a Tor circuit
Tor has successfully opened a circuit. Looks like client
Bootstrapped 100%: Done
```

```

Bootstrapped 0%: Starting
Bootstrapped 5%: Connecting to directory server
Bootstrapped 10%: Finishing handshake with directory server
Bootstrapped 15%: Establishing an encrypted directory connection
Bootstrapped 20%: Asking for networkstatus consensus
Bootstrapped 25%: Loading networkstatus consensus
I learned some more directory information, but not enough to build a circuit:
Bootstrapped 40%: Loading authority key certs
Bootstrapped 45%: Asking for relay descriptors
I learned some more directory information, but not enough to build a circuit:
have 0% of guards bw, 0% of midpoint bw, and 0% of exit bw = 0% of path bw.)
Bootstrapped 50%: Loading relay descriptors
Bootstrapped 55%: Loading relay descriptors
Bootstrapped 61%: Loading relay descriptors
Bootstrapped 66%: Loading relay descriptors
Bootstrapped 72%: Loading relay descriptors
Bootstrapped 80%: Connecting to the Tor network
Bootstrapped 90%: Establishing a Tor circuit
Tor has successfully opened a circuit. Looks like client functionality is work
Bootstrapped 100%: Done

```

```

nyx - linux-hpcompaq6005prosfpc Tor 0.4.2.7 (recommended)
Relaying Disabled, Control Port (open): 9051
cpu: 0.0% tor, 1.5% nyx mem: 37 MB (1.1%) pid: 2499 uptime: 09:32

```

```

page 3 / 5 - m: menu, p: pause, h: page help, q: quit

```

```

Tor Configuration (press 'a' to show all options)

```

```

DataDirectory (General Option)

```

```

Value: /var/lib/tor (custom, Filename, usage: DIR)

```

```

Description: Store working data in DIR. Can not be changed while tor is running. (Default: ~/.tor if your
home directory is not /; otherwise, @LOCALSTATEDIR@/lib/tor. On Windows, the default is your Application-
Data folder.)

```

BandwidthBurst	1 GB	Maximum bandwidth usage limit
BandwidthRate	1 GB	Average bandwidth usage limit
ControlPort	9051	Port providing access to tor controllers (nyx, vidalia, etc)
CookieAuthentication	False	If set, authenticates controllers via a cookie
DataDirectory	/var/lib/tor	Location for storing runtime data (state, keys, etc)
HashedControlPassword	<none>	Hash of the password for authenticating to the control port
Log	notice syslog	Runlevels and location for tor logging
RelayBandwidthBurst	0 B	Maximum bandwidth usage limit for relaying
RelayBandwidthRate	0 B	Average bandwidth usage limit for relaying
RunAsDaemon	False	Toggles if tor runs as a daemon process
User	<none>	UID for the process when started

```
nyx - linux-hpcompaq6005prosffpc Tor 0.4.2.7 (recommended)
Relaying Disabled, Control Port (open): 9051
cpu: 0.2% tor, 1.7% nyx mem: 37 MB (1.1%) pid: 2499 uptime: 25:20
page 2 / 5 - m: menu, p: pause, h: page help, q: quit
Connections (1 outbound, 11 circuit, 1 control):
185.255.105.40:51608 --> 64.227.73.144:9001 (us) +23.2m (OUTBOUND)
185.255.105.40 --> 51.89.200.121:443 (fr) Purpose: General, Circuit ID: 84 1.0m (CIRCUIT)
├── 64.227.73.144:9001 (us) 1 / Guard
├── 80.241.215.37:9001 (de) 2 / Middle
└── 51.89.200.121:443 (fr) 3 / End
185.255.105.40 --> 62.171.133.250:443 (de) Purpose: General, Circuit ID: 81 2.0m (CIRCUIT)
├── 64.227.73.144:9001 (us) 1 / Guard
├── 5.79.90.24:443 (nl) 2 / Middle
└── 62.171.133.250:443 (de) 3 / End
185.255.105.40 --> 85.248.227.164:9002 (sk) Purpose: General, Circuit ID: 80 2.5m (CIRCUIT)
├── 64.227.73.144:9001 (us) 1 / Guard
├── 163.172.53.201:443 (fr) 2 / Middle
└── 85.248.227.164:9002 (sk) 3 / End
185.255.105.40 --> 137.74.19.202:20 (fr) Purpose: General, Circuit ID: 77 3.0m (CIRCUIT)
├── 64.227.73.144:9001 (us) 1 / Guard
├── 85.10.240.138:443 (de) 2 / Middle
└── 137.74.19.202:20 (fr) 3 / End
```

AHMIA.FI - MSYDQSTLZZKZERDG.ONION

AHMIA

Ahmia searches hidden services on the Tor network. To access these hidden services, you need the [Tor browser bundle](#). Abuse material is not allowed on Ahmia. See our [service blacklist](#) and report abuse material if you find it in the index. It will be removed as soon as possible.

For more about Ahmia, see [indexing information](#) , [contribute to the source code](#).

The Tor Project

Onion service: msydstlz2kzerdg.onion

Usage: python3 onioff.py {onion} [options]

Options:

--version show program's version number and exit
-h, --help show this help message and exit
-f FILE, --file=FILE name of onion file
-o OUTPUT_FILE, --output=OUTPUT_FILE
 output filename
-a, --active log active onions only to output file

Examples:

```
python3 onioff.py http://xmh57jrzrnw6insl.onion/  
python3 onioff.py -f ~/onions.txt -o ~/report.txt -a  
python3 onioff.py https://facebookcorewwi.onion/ -o ~/report.txt
```

```
[+] Commencing Onion Inspection  
[+] Tor Running Normally  
[!] Inspecting Onion --> http://xmh57jrzrnw6insl.onion/  
[+] Sending Request  
[+] Onion Up & Running --> ACTIVE  
[+] Retrieving Onion Title  
[+] Onion Title --> TORCH: Tor Search!  
[!] Inspecting Onion --> http://facebookcorewwi.onion/  
[+] Sending Request  
[+] Onion Up & Running --> ACTIVE  
[+] Retrieving Onion Title  
[+] Onion Title --> Facebook – Log In or Sign Up  
[!] Inspecting Onion --> http://sms4tor3vcr2geip.onion/  
[+] Sending Request  
[-] Onion Down --> INACTIVE
```

```

$ docker run -e DEBUG_LEVEL=1 --rm -it milesrichardson/onion-nmap -p 80,443 facebookcorewwi.onion
[tor_wait] Wait for Tor to boot... (might take a while)
[tor_wait retry 0] Check socket is open on localhost:9050...
[tor_wait retry 0] Socket OPEN on localhost:9050
[tor_wait retry 0] Check SOCKS proxy is up on localhost:9050 (timeout 2 )...
[tor_wait retry 0] SOCKS proxy DOWN on localhost:9050, try again...
[tor_wait retry 1] Check socket is open on localhost:9050...
[tor_wait retry 1] Socket OPEN on localhost:9050
[tor_wait retry 1] Check SOCKS proxy is up on localhost:9050 (timeout 4 )...
[tor_wait retry 1] SOCKS proxy UP on localhost:9050
[tor_wait] Done. Tor booted.
[nmap onion] nmap -p 80,443 facebookcorewwi.onion
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/libproxychains4.so
[proxychains] DLL init: proxychains-ng 4.12

Starting Nmap 7.60 ( https://nmap.org ) at 2019-08-24 14:54 UTC
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... facebookcorewwi.onion:80 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... facebookcorewwi.onion:443 ... OK
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0

```

```

building circuit...
{'origin': '209.141.41.103'}
renewing circuit...
{'origin': '205.185.124.65'}
Server nginx
Date Mon, 06 Apr 2020 13:28:25 GMT
Content-Type text/html; charset=UTF-8
Transfer-Encoding chunked
Connection keep-alive
Vary Accept-Encoding
ETag W/"5e87b9a5-1531"
Strict-Transport-Security max-age=0
X-Frame-Options SAMEORIGIN
Content-Security-Policy default-src https: blob: data: 'unsafe-inline' 'unsafe-eval'; frame-ancestors 'self'
X-XSS-Protection 1;mode=block
X-Content-Type-Options nosniff
Referrer-Policy origin
Expect-CT max-age=0
Expires Mon, 06 Apr 2020 13:28:24 GMT
Cache-Control no-cache
Content-Encoding gzip

```

```

.. data:: Signal (enum)

Signals that the tor process will accept.

.. versionchanged:: 1.3.0
   Added the HEARTBEAT signal.

=====
Signal          Description
=====
**RELOAD** or **HUP**    reloads our torrc
**SHUTDOWN** or **INT**  shut down, waiting ShutdownWaitLength first if we're a relay
**DUMP** or **USR1**     dumps information about open connections and circuits to our log
**DEBUG** or **USR2**    switch our logging to the DEBUG runlevel
**HALT** or **TERM**     exit tor immediately
**NEWNYM**              switch to new circuits, so new application requests don't share any circuits
**CLEARDNSCACHE**       clears cached DNS results
**HEARTBEAT**           trigger a heartbeat log message
=====

```

```

432 3.7. SIGNAL
433
434 Sent from the client to the server. The syntax is:
435
436 "SIGNAL" SP Signal CRLF
437
438 Signal = "RELOAD" / "SHUTDOWN" / "DUMP" / "DEBUG" / "HALT" /
439 "HUP" / "INT" / "USR1" / "USR2" / "TERM" / "NEWNYM" /
440 "CLEARDNSCACHE" / "HEARTBEAT" / "ACTIVE" / "DORMANT"
441
442 The meaning of the signals are:
443
444 RELOAD -- Reload: reload config items.
445 SHUTDOWN -- Controlled shutdown: if server is an OP, exit immediately.
446 If it's an OR, close listeners and exit after
447 ShutdownWaitLength seconds.
448 DUMP -- Dump stats: log information about open connections and
449 circuits.
450 DEBUG -- Debug: switch all open logs to loglevel debug.
451 HALT -- Immediate shutdown: clean up and exit now.
452 CLEARNSCACHE -- Forget the client-side cached IPs for all hostnames.
453 NEWNYM -- Switch to clean circuits, so new application requests
454 don't share any circuits with old ones. Also clears
455 the client-side DNS cache. (Tor MAY rate-limit its
456 response to this signal.)
457 HEARTBEAT -- Make Tor dump an unscheduled Heartbeat message to log.
458 DORMANT -- Tell Tor to become "dormant". A dormant Tor will
459 try to avoid CPU and network usage until it receives
460 user-initiated network request. (Don't use this
461 on relays or hidden services yet!)
462 ACTIVE -- Tell Tor to stop being "dormant", as if it had received
463 a user-initiated network request.

```

```

Circuit 10 (GENERAL)
|- CE3FE883C6C9EF475EA097DC3E33A6F32B852DA1 (AIKO, 78.129.218.56)
|- 12CF6DB4DAE106206D6C6B09988E865C0509843B (ATZv5, 159.69.114.110)
+- E19D4503D2FD584C8099A954270A9BC819596E74 (Unnamed, 51.68.206.35)

Circuit 11 (GENERAL)
|- CE3FE883C6C9EF475EA097DC3E33A6F32B852DA1 (AIKO, 78.129.218.56)
|- 44DF1007B545B4D8057F279025EBB33CF99BE227 (Kroell, 80.241.214.102)
+- 9612664500871798CFB52E8A71A956F316AA0503 (Polaris, 130.230.113.235)

Circuit 12 (GENERAL)
|- CE3FE883C6C9EF475EA097DC3E33A6F32B852DA1 (AIKO, 78.129.218.56)
|- 9E1E4F5B5F94812D02C4D18CB4086CE71CA5C614 (torpidsDEhetzner1, 78.46.217.214)
+- 615ABEA2DE76EB3760BC51E7306BAA59F15CD8F2 (Cloud, 5.135.158.101)

Circuit 13 (GENERAL)
|- CE3FE883C6C9EF475EA097DC3E33A6F32B852DA1 (AIKO, 78.129.218.56)
|- 91B14EB2893544F0EC8F16086261A10B8E46B5C5 (okthx, 163.172.210.167)
+- 03EE7DDD931D92BB57B81B3038AE7C40A08AB237 (Shockrealm, 123.30.128.138)

Circuit 14 (GENERAL)
|- CE3FE883C6C9EF475EA097DC3E33A6F32B852DA1 (AIKO, 78.129.218.56)

```

DuckDuckGo's introduction points are...

```
I 209.59.173.26:443 => 3b5ji6reaxcbecgfpuzo2himulv6soxw
82.197.218.97:9001 => jtkn77xts4ojakrccagzchfmmmon6f324
51.77.251.192:443 => v33md65a7qlpjeywhc7qmuefx2nh2ip
145.220.0.15:9001 => 3nnbaaks7n4tp4bpac253775aetytqsc
194.55.13.50:9001 => 7v43p6jdbbmljdtv6oewmgcay4bfcedy
212.51.134.4:9001 => ejgd3uo763yreglajbynjcktespohqtp
173.212.239.78:9201 => hm7ukg6vr6lnyduow7ib6ie7zcadym67
85.17.127.129:443 => nqzttw63upp6pj4c4qgls4gcogv75uiz
54.38.145.211:80 => s3h6c6fb2esitwovtigk4f76q322hj47
87.246.156.175:9001 => d4hokdo3mcksqhfjnpwif7zvpnt3vr7u
```

Links Found - 52

```
-----
http://ow24et3tetp6tvmk.onion/ OnionWallet Anonymous and secure Bitcoin Wallet and Bitcoin
Tor Web Wallet
http://y3fpieiezy2sin4a.onion/ HQER - High Quality Euro Counterfeits - best counterfeit
http://ow24et3tetp6tvmk.onion/ OnionWallet Anonymous and secure Bitcoin Wallet and Bitcoin
Tor Web Wallet
http://y3fpieiezy2sin4a.onion/ HQER - High Quality Euro Counterfeits - best counterfeit
http://y3fpieiezy2sin4a.onion/index.php HQER - High Quality Euro Counterfeits - best counterfeit
http://ow24et3tetp6tvmk.onion/login.php OnionWallet Anonymous and secure Bitcoin Wallet and Bitcoin
Tor Web Wallet
http://ow24et3tetp6tvmk.onion/login.php OnionWallet Anonymous and secure Bitcoin Wallet and Bitcoin
Tor Web Wallet
http://y3fpieiezy2sin4a.onion/index.php HQER - High Quality Euro Counterfeits - best counterfeit
http://qkj4drtgvpm7eec1.onion/ Counterfeit USD - High quality USD Counterfeits - Best USD
USD banknotes with Bitcoin
http://sblqp5utjj3bu2ec.onion/ Escrow Service for Bitcoin and other cryptocurrencies | Bit
http://sblqp5utjj3bu2ec.onion/ Escrow Service for Bitcoin and other cryptocurrencies | Bit
http://3n3w4m56atug7osb.onion/ Apple Market - Stolen & Carded Merchandise | iPhone XS / XS
|Buy safe with
bitcoin | Apple |
http://3n3w4m56atug7osb.onion/ Apple Market - Stolen & Carded Merchandise | iPhone XS / XS
|Buy safe with
bitcoin | Apple |
http://ndntmfusjmj6tkp1.onion/bitcoin.html
Hidden Wiki .Onion UrIs / What is Bitcoin? - Blockchain analysis, Cryptography
http://ndntmfusjmj6tkp1.onion/bitcoin.html
Hidden Wiki .Onion UrIs / What is Bitcoin? - Blockchain analysis, Cryptography
```

```
crawled.txt
1 http://2kka4f23pcxgqkpv.onion/
2 http://2kka4f23pcxgqkpv.onion/index.php
3 http://2kka4f23pcxgqkpv.onion/info.php
4 http://2kka4f23pcxgqkpv.onion/login.php
5 http://2kka4f23pcxgqkpv.onion/register.php
6 http://2ljfiwqcup2kc3u3.onion/about.html
7 http://2ljfiwqcup2kc3u3.onion/faq.html
8 http://2pneiouz2aj27kjs.onion
9 http://2pneiouz2aj27kjs.onion/
10 http://2zyakjq2hvtbg6qd.onion/
11 http://3c3bdbvvhb7j6yab2.onion/
12 http://3dbr5t4pygahedms.onion/
13 http://3dbr5t4pygahedms.onion/index.php
14 http://3g2upl4pq6kufc4m.onion/
15 http://3i6u7z5qoacdnds3.onion/
```

Línea 22, Columna 51 INSERTAR es_ES

```
Queue_url 6427 | Crawled_url 797
http://kenny7svk4sg2mcj.onion/
Thread-22 now crawl starts http://kenny7svk4sg2mcj.onion/
Queue_url 6427 | Crawled_url 797
http://stacvvulbayktqlf.onion/img/stacvvulbayktqlf/gallery_05.jpg
Thread-30 now crawl starts http://stacvvulbayktqlf.onion/img/stacvvulbayktqlf/gallery_05.jpg
Queue_url 6427 | Crawled_url 797
http://lg7iwjj3ajzz2cmd.onion/index.php/store-listing/
Thread-15 now crawl starts http://lg7iwjj3ajzz2cmd.onion/index.php/store-listing/
Queue_url 6427 | Crawled_url 797
http://hidden24vowyr cic.onion/index.php?route=product/product&path=62&product_id=271
Thread-46 now crawl starts http://hidden24vowyr cic.onion/index.php?route=product/product&path=62&product_id=271
Queue_url 6429 | Crawled_url 798
HTTP Error 404: Not Found
http://deepmartyqzffl5n.onion/products/paypal-transfer-2000/
Thread-11 now crawl starts http://deepmartyqzffl5n.onion/products/paypal-transfer-2000/
Queue_url 6428 | Crawled_url 799
```


Chapter 6: Gathering Information from Servers

REST API Documentation

The base URL for all of these methods is:

```
https://api.shodan.io
```

Note: All API methods are rate-limited to 1 request/ second.

Shodan Search Methods

GET /shodan/host/{ip}

GET /shodan/host/count

GET /shodan/host/search

GET /shodan/host/search/facets

GET /shodan/host/search/filters

GET /shodan/host/search/tokens

GET /shodan/ports

LOOK FOR SUBDOMAINS

Sub-domain enumeration. Discover hosts related to a specific domain.

Results for your query: *www.python.org*

75 results found.

Showing 1 to 75 of 75 entries.

Domains

[chat.uk.python.org](#)

[empleo.es.python.org](#)

[dinsdale.python.org](#)

[pycon-archives.python.org](#)

[comunidad.es.python.org](#)

BINARYEDGE.IO - WE SCAN THE ENTIRE INTERNET
TO HELP YOU UNDERSTAND WHAT IS BEING EXPOSED

FILTER BY:

- ICS DATABASE IOT
 MALWARE WEBSERVER CAMERA

Ports	Entries*	Products	Entries	Countries	Entries	ASNs	Entries
443/tcp	456	Apache	34	United States	336	54113 FASTLY, US	334
80/tcp	142	Apache httpd	31	Germany	33	14061 DIGITALOCEAN-ASN, US	34
9999/tcp	4	nginx	29	France	28	63949 LINODE-AP Linode, LLC, US	33
5000/tcp	1	nginx/1.10.3 (Ubuntu)	17	United Kingdom	21	47570 V2O-SIA-AS, LV	18
8000/tcp	1	nginx/1.10.3	16	Latvia	18	20473 AS-CHOOPA, US	15

attack	Update HTTP Response Splitting resources	5 months ago
discovery	added php scheme	5 months ago
docs	from https://github.com/attackercan/	4 years ago
regex	cross-updating with https://github.com/andresiancho/w3af/blob/master...	4 years ago
web-backdoors	Add files in asmx format	9 months ago
wordlists-misc	Resolvers file for subdomain brute force	2 years ago
wordlists-user-passwd	Update readme.txt	8 months ago
.gitignore	added Null representations for double encoding, format string %* and ...	3 years ago
README.md	Update README.md	8 months ago
_copyright.txt	Update _copyright.txt	9 months ago
fuzzdb-icon.png	Add files via upload	8 months ago
fuzzdb.png	Add files via upload	8 months ago
..		
GenericBlind.txt	Removed PGSQL per Issue #2	3 years ago
Generic_SQLI.txt	<u>Fix #144</u>	4 years ago
MSSQL.txt	Added a numeric check	16 months ago
MSSQL_blind.txt	<u>Fix #144</u>	4 years ago
MySQL.txt	<u>Fix #144</u>	4 years ago
MySQL_MSSQL.txt	<u>Fix #144</u>	4 years ago
README.md	Typo	5 years ago
oracle.txt	<u>Fix #144</u>	4 years ago
xplatform.txt	<u>Fix #144</u>	4 years ago

Chapter 7: Interacting with FTP, SFTP, and SSH Servers

```
(gen) banner: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
(gen) software: OpenSSH 7.6p1
(gen) compatibility: OpenSSH 7.3+, Dropbear SSH 2016.73+
(gen) compression: enabled (zlib@openssh.com)

# key exchange algorithms
(key) curve25519-sha256 -- [warn] unknown algorithm
(key) curve25519-sha256@libssh.org -- [info] available since OpenSSH 6.5, Dropbear SSH 2013.62
(key) ecdh-sha2-nistp256 -- [fail] using weak elliptic curves
(key) ecdh-sha2-nistp256 -- [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(key) ecdh-sha2-nistp384 -- [fail] using weak elliptic curves
(key) ecdh-sha2-nistp384 -- [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(key) ecdh-sha2-nistp521 -- [fail] using weak elliptic curves
(key) ecdh-sha2-nistp521 -- [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(key) diffie-hellman-group-exchange-sha256 -- [warn] using custom size modulus (possibly weak)
(key) diffie-hellman-group-exchange-sha256 -- [info] available since OpenSSH 4.4
(key) diffie-hellman-group16-sha512 -- [info] available since OpenSSH 7.3, Dropbear SSH 2016.73
(key) diffie-hellman-group18-sha512 -- [info] available since OpenSSH 7.3
(key) diffie-hellman-group14-sha256 -- [info] available since OpenSSH 7.3, Dropbear SSH 2016.73
(key) diffie-hellman-group14-sha1 -- [warn] using weak hashing algorithm
(key) diffie-hellman-group14-sha1 -- [info] available since OpenSSH 3.9, Dropbear SSH 0.53

# host-key algorithms
(key) ssh-rsa -- [info] available since OpenSSH 2.5.0, Dropbear SSH 0.28
(key) rsa-sha2-512 -- [info] available since OpenSSH 7.2
(key) rsa-sha2-256 -- [info] available since OpenSSH 7.2
(key) ecdsa-sha2-nistp256 -- [fail] using weak elliptic curves
(key) ecdsa-sha2-nistp256 -- [warn] using weak random number generator could reveal the key
(key) ecdsa-sha2-nistp256 -- [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(key) ssh-ed25519 -- [info] available since OpenSSH 6.5

# encryption algorithms (ciphers)
(enc) chacha20-poly1305@openssh.com -- [info] available since OpenSSH 6.5
(enc) chacha20-poly1305@openssh.com -- [info] default cipher since OpenSSH 6.9.
(enc) aes128-ctr -- [info] available since OpenSSH 3.7, Dropbear SSH 0.52
(enc) aes192-ctr -- [info] available since OpenSSH 3.7
```

Key Exchange Algorithms

<code>diffie-hellman-group14-sha256</code>	Diffie-Hellman with 2048-bit Oakley Group 14 with SHA-256 hash ⓘ Oakley Group 14 should be secure for now.	Secure
<code>diffie-hellman-group16-sha512</code>	Diffie-Hellman with 4096-bit MODP Group 16 with SHA-512 hash ⓘ	Secure
<code>diffie-hellman-group18-sha512</code>	Diffie-Hellman with 8192-bit MODP Group 18 with SHA-512 hash ⓘ	Secure
<code>diffie-hellman-group-exchange-sha256</code>	Diffie-Hellman with MODP Group Exchange with SHA-256 hash ⓘ	Secure
<code>curve25519-sha256</code>	Elliptic Curve Diffie-Hellman on Curve25519 with SHA-256 hash ⓘ	Secure
<code>curve25519-sha256@libssh.org</code>	Elliptic Curve Diffie-Hellman on Curve25519 with SHA-256 hash ⓘ	Secure
<code>ecdh-sha2-nistp256</code>	Elliptic Curve Diffie-Hellman on NIST P-256 curve with SHA-256 hash ⓘ Possible NSA backdoor.	Secure
<code>ecdh-sha2-nistp384</code>	Elliptic Curve Diffie-Hellman on NIST P-384 curve with SHA-384 hash ⓘ Possible NSA backdoor.	Secure
<code>ecdh-sha2-nistp521</code>	Elliptic Curve Diffie-Hellman on NIST P-521 curve with SHA-512 hash ⓘ Possible NSA backdoor.	Secure
<code>diffie-hellman-group14-sha1</code>	Diffie-Hellman with 2048-bit Oakley Group 14 with SHA-1 hash ⓘ Oakley Group 14 should be secure for now. SHA-1 is becoming obsolete, consider using SHA-256 version.	Weak

Server Host Key Algorithms

<code>ssh-ed25519</code>	Ed25519, an Edwards-curve Digital Signature Algorithm (EdDSA) ⓘ	Secure
<code>ssh-ed25519</code>	Ed25519, an Edwards-curve Digital Signature Algorithm (EdDSA) ⓘ	Secure

Chapter 8: Working with Nmap Scanner

```
Nmap 7.60 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
```

Chapter 9: Interacting with Vulnerability Scanners

Nessus - 8.11.0				View Release Notes
Nessus-8.11.0-debian6_i386.deb	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 i386(32-bit)	38.8 MB	Jul 14, 2020	Checksum
Nessus-8.11.0-amzn.x86_64.rpm	Amazon Linux 2015.03, 2015.09, 2017.09, Amazon Linux 2	41.2 MB	Jul 14, 2020	Checksum
Nessus-8.11.0-x64.msi	Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, 8, 10, Server 2016, Server 2019 (64-bit)	75.7 MB	Jul 14, 2020	Checksum
Nessus-8.11.0-Win32.msi	Windows 7, 8, 10 (32-bit)	69.8 MB	Jul 14, 2020	Checksum

Welcome to Nessus Essentials ✕

To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.

Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

Targets

Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

My Host Discovery Scan Results ✕

Nessus found the following hosts listed below from your list of targets (127.0.0.1).

To launch your first basic network scan, select the hosts you want to scan. These hosts count towards the 16 host limit on your license.

<input checked="" type="checkbox"/>	IP	DNS
<input checked="" type="checkbox"/>	127.0.0.1	localhost

Discovery Complete!

[Back](#)

[Run Scan](#)

My Basic Network Scan

[Back to My Scans](#)

Configure

Audit Trail

Launch ▾

Report ▾

Export ▾

Hosts 1

Vulnerabilities 39

History 1

Filter ▾

Search Hosts



1 Host

<input type="checkbox"/> Host	Vulnerabilities ▾
<input type="checkbox"/> 127.0.0.1	<div style="display: flex; align-items: center;"><div style="width: 15px; height: 15px; background-color: orange; margin-right: 5px;"></div>15 <div style="width: 100px; height: 15px; background-color: blue; margin-left: 10px; display: flex; align-items: center; justify-content: center;">123</div> ✕</div>

Scan Details

Policy: Basic Network Scan
Status: Completed
Scanner: Local Scanner
Start: August 8 at 10:02 PM
End: August 8 at 10:14 PM
Elapsed: 12 minutes

Scan Templates


[Back to Scans](#)

Scanner

Search Library




DISCOVERY




Host Discovery
A simple scan to discover live hosts and open ports.


VULNERABILITIES



Basic Network Scan
A full system scan suitable for any host.




Advanced Scan
Configure a scan without using any recommendations.



Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.




Malware Scan
Scan for malware on Windows and Unix systems.




Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

UPGRADE




Web Application Tests
Scan for published and unknown web vulnerabilities.




Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.



Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.



Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.



DROWN Detection
Remote checks for CVE-2016-0800.

Vulnerabilities 39

Filter Search Vulnerabilities 39 Vulnerabilities

Sev	Name	Family	Count	
MIXED	SSL (Multiple Issues)	General	34	
MIXED	TLS (Multiple Issues)	Service detection	13	
MEDIUM	SSL Certificate Signed Using Weak Hashing Al...	General	1	
INFO	Netstat Portscanner (SSH)	Port scanners	13	
INFO	Remote listeners enumeration (Linux / AIX)	Service detection	12	
INFO	Service Detection	Service detection	11	
INFO	HTTP (Multiple Issues)	Web Servers	9	
INFO	SSH (Multiple Issues)	General	6	
INFO	SSL / TLS Versions Supported	General	5	
INFO	DMI (Multiple Issues)	General	3	

Host Details

IP: 127.0.0.1
 DNS: localhost
 MAC: 02:42:DC:81:03:61
 A0:D3:C1:9C:69:72
 A2:D3:C8:DA:07:43
 A4:4E:31:D8:C2:80
 OS: Linux Kernel 5.3.0-42-generic on Debian buster/sid
 Start: August 8 at 10:02 PM
 End: August 8 at 10:14 PM
 Elapsed: 12 minutes
 KB: [Download](#)

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

My Basic Network Scan / Plugin #35291

[Back to Vulnerabilities](#)

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

Vulnerabilities 39

MEDIUM SSL Certificate Signed Using Weak Hashing Algorithm

Plugin Details

Severity: Medium
 ID: 35291
 Version: 1.31
 Type: remote
 Family: General
 Published: January 5, 2009
 Modified: April 27, 2020

Risk Information

Risk Factor: Medium
 CVSS v3.0 Base Score 7.5
 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/L:H/A:N
 CVSS v3.0 Temporal Vector: CVSS:3.0/E:P/RL:O/RC:C
 CVSS v3.0 Temporal Score: 6.7
 CVSS Base Score: 5.0
 CVSS Temporal Score: 3.9
 CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunseting of the SHA-1 cryptographic hash algorithm.





Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

See Also

<https://tools.ietf.org/html/rfc3279>
<http://www.nessus.org/u?9bb87bf2>
<http://www.nessus.org/u?e120eea1>
<http://www.nessus.org/u?5d894816>
<http://www.nessus.org/u?51db68aa>
<http://www.nessus.org/u?9dc7fbfa>

E	Paquete	Versión instalada	Última versión	Descripción
	greenbone-security-assistant		7.0.2+dfsg.1-2build1	remote network security auditor - web interface
	greenbone-security-assistant-cor		7.0.2+dfsg.1-2build1	architecture independent files for greenbone-security-assistant
<input type="checkbox"/>	libopenvas-dev		9.0.1-4	remote network security auditor - static libraries and headers
<input type="checkbox"/>	libopenvas-doc		9.0.1-4	remote network security auditor - libraries documentation
	libopenvas9		9.0.1-4	remote network security auditor - shared libraries
	openvas		9.0.2	remote network security auditor - dummy package
	openvas-cli		1.4.5-1	Command Line Tools for OpenVAS
	openvas-manager		7.0.2-2	Manager Module of OpenVAS
	openvas-manager-common		7.0.2-2	architecture independent files for openvas-manager
<input type="checkbox"/>	openvas-nasl		9.0.1-4	remote network security auditor - nasl tool
	openvas-scanner		5.1.1-3	remote network security auditor - scanner

```

root@kali:~# openvas-setup
[>] Checking redis.conf
[*] Editing redis.conf

[>] Checking openvassd.conf
[*] Adding to openvassd.conf

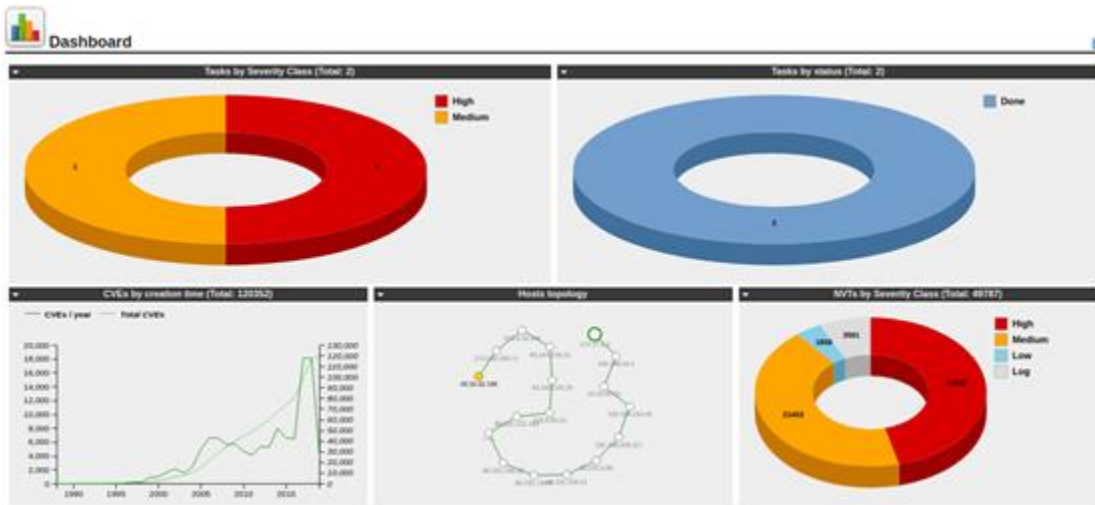
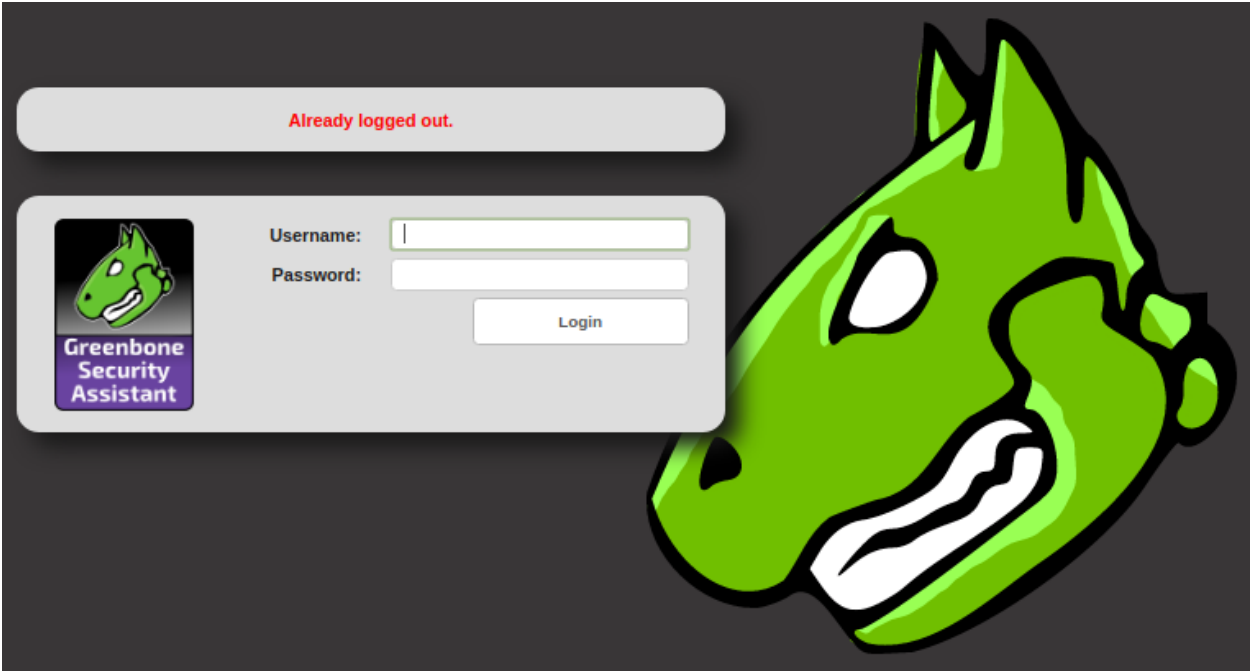
[>] Restarting redis-server

[>] Checking OpenVAS certificate infrastructure
OK: Directory for keys (/var/lib/openvas/private/CA) exists.
OK: Directory for certificates (/var/lib/openvas/CA) exists.
OK: CA key found in /var/lib/openvas/private/CA/cakey.pem
OK: CA certificate found in /var/lib/openvas/CA/cacert.pem
OK: CA certificate verified.
OK: Certificate /var/lib/openvas/CA/clientcert.pem verified.
OK: Certificate /var/lib/openvas/CA/servercert.pem verified.

OK: Your OpenVAS certificate infrastructure passed validation.

[>] Updating OpenVAS feeds
[*] [1/3] Updating: NVT

```



New Target



Name localhost

Comment

Hosts Manual 127.0.0.1
 From file Seleccionar archivo Ningún archivo seleccionado
 From host assets (0 hosts)

Exclude Hosts

Reverse Lookup Only Yes No

Reverse Lookup Unify Yes No

Port List All IANA assigned TCP an... *

Alive Test Scan Config Default

Credentials for authenticated checks

SSH -- on port 22 *

SMB -- *

ESXi -- *

SNMP -- *

Create

New Task

Name localhost

Comment

Scan Targets localhost

Alerts

Schedule -- Once

Add results to Assets yes no

Apply Overrides yes no

Min QoD 70 %

Alterable Task yes no

Auto Delete Reports Do not automatically delete reports
 Automatically delete oldest reports but always keep newest 5 reports

Scanner OpenVAS Default

Scan Config Full and fast

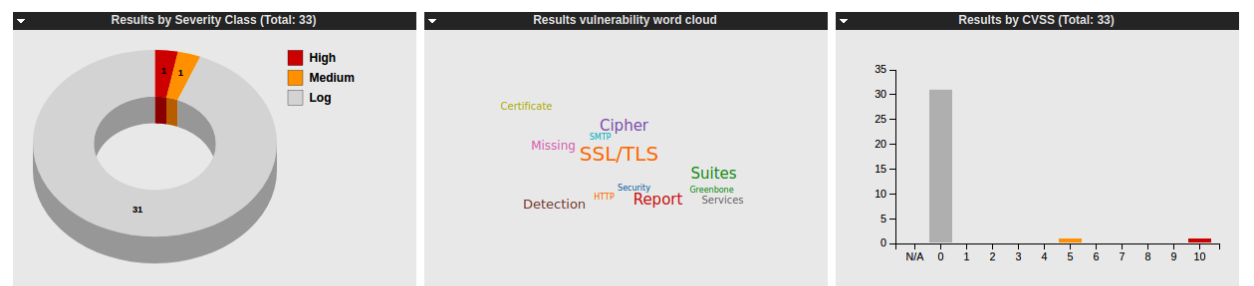
Network Source Interface

Order for target hosts Sequential

Maximum concurrently executed NVTs per host 4

Maximum concurrently scanned hosts 20

Create



1 - 10 of 33

Vulnerability	Severity	QoD	Host	Location	Created
CPE Inventory	0.0 (Log)	80%	127.0.0.1	general/CPE-T	Thu Aug 6 21:32:53 2020
DIRB (NASL wrapper)	0.0 (Log)	98%	127.0.0.1	443/tcp	Thu Aug 6 21:29:21 2020
OpenVAS / Greenbone Vulnerability Manager Default Credentials	10.0 (High)	100%	127.0.0.1	9390/tcp	Thu Aug 6 21:25:29 2020
wapiti (NASL wrapper)	0.0 (Log)	98%	127.0.0.1	443/tcp	Thu Aug 6 21:24:48 2020
SSL/TLS: HTTP Strict Transport Security (HSTS) Missing	0.0 (Log)	80%	127.0.0.1	443/tcp	Thu Aug 6 21:23:05 2020



Result: OpenVAS / Greenbone Vulnerability Manager Default Credentials

ID: 2ce3a347-6c6a-4178-a607-9b80777d4
Created: Thu Aug 6 21:25:29 2020
Modified: Thu Aug 6 21:25:29 2020
Owner: admin

Vulnerability	Severity	QoD	Host	Location	Actions
OpenVAS / Greenbone Vulnerability Manager Default Credentials	10.0 (High)	100%	127.0.0.1	9390/tcp	

Summary
The remote OpenVAS / Greenbone Vulnerability Manager is installed/configured in a way that it has account(s) with default passwords enabled.

Vulnerability Detection Result
It was possible to login using the following credentials (username:password:role):
admin:admin:Admin

Impact
This issue may be exploited by a remote attacker to gain access to sensitive information or modify system configuration.

Solution
Solution type: Workaround
Change the password of the mentioned account(s).

Vulnerability Insight
It was possible to login with default credentials: admin/admin, sadmin/changeme, observer/observer or admin/openvas.

Vulnerability Detection Method
Try to login with default credentials via the OMP/GMP protocol.
Details: [OpenVAS / Greenbone Vulnerability Manager Default Credentials \(OID: 1.3.6.1.4.1.25623.1.0.108554\)](#)

Anonymous X...

Filter:
autoup=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort=reverse=severity levels=html min_qod=70



Report: Summary and Download

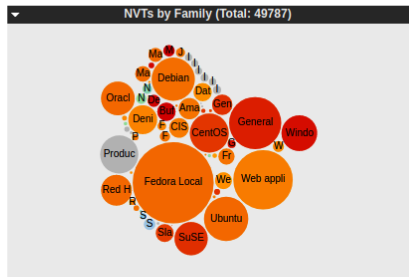
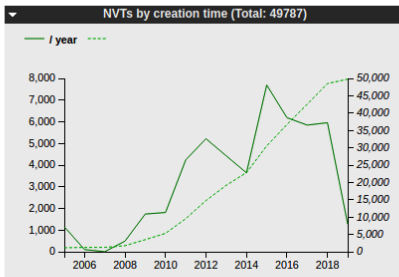
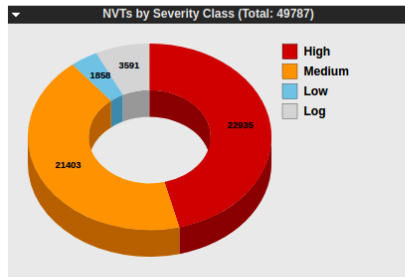
ID: 4ba81ad5-d5
Modified: Thu Aug 6 21:25:29 2020
Created: Thu Aug 6 21:25:29 2020
Owner: admin

Result of Task: localhost
Scan initiated: Thu Aug 6 21:08:29 2020 UTC
Scan started: Thu Aug 6 21:09:05 2020 UTC
Scan ended: Thu Aug 6 21:33:04 2020 UTC
Scan duration: 23 minutes 59 seconds
Scan status: Done

Network Source Interface:	High	Medium	Low	Log	False Pos.	Total	Run Alert	Download
Full report:	1	1	0	31	0	33		Topology SVG
Filtered report:	1	1	0	0	0	2		Anonymous...



NVTs (49787 of 49787)



Name	Family	Created	Modified	Version	CVE	Severity	QoD
Debian LTS Advisory ([SECURITY] [DLA 1749-1] gotang security update)	Debian Local Security Checks	Wed Apr 3 2019	Wed Apr 3 2019	2019-04-03T20:00:00+0000	CVE-2019-9741	4.3	97%
Debian LTS Advisory ([SECURITY] [DLA 1748-1] apache2 security update)	Debian Local Security Checks	Wed Apr 3 2019	Wed Apr 3 2019	2019-04-03T20:00:00+0000	CVE-2019-0217 CVE-2019-0220	5.0	97%
Kentico <= 12.0.14 Remote Code Execution Vulnerability	Web application abuses	Wed Apr 3 2019	Wed Apr 3 2019	2019-04-03T09:02:33+0000	CVE-2019-10068	7.5	30%

Chapter 10: Identifying Server Vulnerabilities in Web Applications



Vulnerable test websites for [Acunetix Web Vulnerability Scanner](#).

Name	URL	Technologies	Resources
SecurityTweets	http://testhtml5.vulnweb.com	nginx, Python, Flask, CouchDB	Review Acunetix HTML5 scanner or learn more on the topic.
Acuart	http://testphp.vulnweb.com	Apache, PHP, MySQL	Review Acunetix PHP scanner or learn more on the topic.
Acuforum	http://testasp.vulnweb.com	IIS, ASP, Microsoft SQL Server	Review Acunetix SQL scanner or learn more on the topic.
Acublog	http://testaspnet.vulnweb.com	IIS, ASP.NET, Microsoft SQL Server	Review Acunetix network scanner or learn more on the topic.
REST API	http://rest.vulnweb.com/	Apache, PHP, MySQL	Review Acunetix scanner or learn more on the topic.

← → ↻ 🏠 testphp.vulnweb.com/search.php?test=query

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)

searched for:

searched for:

xss

OK

Usage: python sqlmap [options]

Options:

-h, --help Show basic help message and exit
-hh Show advanced help message and exit
--version Show program's version number and exit
-v VERBOSE Verbosity level: 0-6 (default 1)

Target:

At least one of these options has to be provided to define the target(s)

-u URL, --url=URL Target URL (e.g. "http://www.site.com/vuln.php?id=1")
-g GOOGLEDORK Process Google dork results as target URLs

Request:

These options can be used to specify how to connect to the target URL

--data=DATA Data string to be sent through POST
--cookie=COOKIE HTTP Cookie header value
--random-agent Use randomly selected HTTP User-Agent header value
--proxy=PROXY Use a proxy to connect to the target URL
--tor Use Tor anonymity network
--check-tor Check to see if Tor is used properly

Enumeration:

These options can be used to enumerate the back-end database management system information, structure and data contained in the tables. Moreover you can run your own SQL statements

```
-a, --all           Retrieve everything
-b, --banner       Retrieve DBMS banner
--current-user    Retrieve DBMS current user
--current-db      Retrieve DBMS current database
--passwords       Enumerate DBMS users password hashes
--tables          Enumerate DBMS database tables
--columns         Enumerate DBMS database table columns
--schema          Enumerate DBMS schema
--dump            Dump DBMS database table entries
--dump-all        Dump all DBMS databases tables entries
-D DB             DBMS database to enumerate
-T TBL           DBMS database table(s) to enumerate
-C COL           DBMS database table column(s) to enumerate
```

```
Database: information_schema
Table: engines
[8 entries]
```

XA	ENGINE	COMMENT	SUPPORT	SAVEPOINTS	TRANSACTIONS
YES	InnoDB	Supports transactions, row-level locking, and foreign keys	YES	YES	YES
NO	MRG_MYISAM	Collection of identical MyISAM tables	YES	NO	NO
NO	BLACKHOLE	/dev/null storage engine (anything you write to it disappears)	YES	NO	NO
NO	CSV	CSV storage engine	YES	NO	NO
NO	MEMORY	Hash based, stored in memory, useful for temporary tables	YES	NO	NO
NULL	FEDERATED	Federated MySQL storage engine	NO	NULL	NULL
NO	ARCHIVE	Archive storage engine	YES	NO	NO
NO	MyISAM	Default engine as of MySQL 3.23 with great performance	DEFAULT	NO	NO



IPv4 Hosts

OpenSSL 1.0.1

Expand

Register
Sign In

Protocol:

1.35M 80/http
1.22M 443/https
434.11K 22/ssh
345.83K 21/ftp
291.83K 3306/mysql
[More](#)

Tag:

1.62M http
1.16M https
434.11K ssh
345.83K ftp
316.18K smtp
[More](#)

212.63.193.8

SPACEDUMP-AS This ASN is located on STHIX at Tulegatan Stokab (30880) Sweden
> Unix 80/http
404 Not Found
80.http.get.body: OpenSSL / 1.0.1 PHP/5.2.17 Server at

45.55.115.225

DIGITALOCEAN-ASN (14061) San Francisco, California, United States
CentOS 22/ssh, 3306/mysql, 443/https, 80/http
503 Service Unavailable droppanel-Healthcheck-1.0.1-1732
DATABASE MYSQL

107.170.246.84 (droppanel-healthcheck-1.0.1-1732)

DIGITALOCEAN-ASN (14061) San Francisco, California, United States
CentOS 22/ssh, 3306/mysql, 443/https, 80/http
503 Service Unavailable droppanel-Healthcheck-1.0.1-1732
DATABASE MYSQL

Verified Has App

▼ Filters

Show 15 ▼


Search: ✕

Date	D	A	V	Title	Type	Platform	Author
2014-04-24	↓	✓		OpenSSL TLS Heartbeat Extension - 'Heartbleed' Information Leak (2) (DTLS Support)	Remote	Multiple	Ayman Sagy
2014-04-10	↓	✓		OpenSSL TLS Heartbeat Extension - 'Heartbleed' Information Leak (1)	Remote	Multiple	prdelka
2014-04-09	↓	✓		OpenSSL 1.0.1f TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure (Multiple SSL/TLS Versions)	Remote	Multiple	Fitzl Csaba
2014-04-08	↓	✓		OpenSSL TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure	Remote	Multiple	Jared Stafford

Heartbleed

Heartbleed Heartbleed Vulnerable

Cryptographic Configuration

SSLv3 Support True  This host is vulnerable to the [POODLE attack](#).

Export DHE False

Export RSA False

DHE Support True



Protocol Details

	No, server keys and hostname not seen elsewhere with SSLv2
DROWN	(1) For a better understanding of this test, please read this longer explanation (2) Key usage data kindly provided by the Censys network search engine; original DROWN website here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) SSL 3: 0xa, TLS 1.0: 0xa
POODLE (SSLv3)	Vulnerable INSECURE (more info) SSL 3: 0xa
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info) TLS 1.2 : 0x000a
GOLDENDOODLE	No (more info) TLS 1.2 : 0x000a
OpenSSL 0-Length	No (more info) TLS 1.2 : 0x000a
Sleeping POODLE	No (more info) TLS 1.2 : 0x000a
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	Yes INSECURE (more info)
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	Yes (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	Yes EXPLOITABLE (more info)

```
Usage: sslyze [options] target1.com target2.com:443 target3.com:443{ip} etc...
```

Options:

```
--version          show program's version number and exit
-h, --help        show this help message and exit
--regular         Regular HTTPS scan; shortcut for --sslv2 --sslv3
                  --tlsv1 --tlsv1_1 --tlsv1_2 --tlsv1_3 --reneg --resum
                  --certinfo --http_get --hide_rejected_ciphers
                  --compression --heartbleed --openssl_ccs --fallback
                  --robot
```

Trust stores options:

```
--update_trust_stores
Update the default trust stores used by SSLyze. The latest stores will be downloaded from https://github.com/nabla-c0d3/trust_stores_observatory. This option is meant to be used separately, and will silence any other command line option supplied to SSLyze.
```

Chapter 11: Security and Vulnerabilities in Python Modules

Warning: Executing shell commands that incorporate unsanitized input from an untrusted source makes a program vulnerable to shell injection, a serious security flaw which can result in arbitrary command execution. For this reason, the use of `shell=True` is **strongly discouraged** in cases where the command string is constructed from external input:

```
>>> from subprocess import call
>>> filename = input("What file would you like to display?\n")
What file would you like to display?
non_existent; rm -rf / #
>>> call("cat " + filename, shell=True) # Uh-oh. This will end badly...
```

`shell=False` disables all shell based features, but does not suffer from this vulnerability; see the Note in the `Popen` constructor documentation for helpful hints in getting `shell=False` to work.

When using `shell=True`, `pipes.quote()` can be used to properly escape whitespace and shell metacharacters in strings that are going to be used to construct shell commands.

```
usage: bandit [-h] [-r] [-a {file,vuln}] [-n CONTEXT_LINES] [-c CONFIG_FILE]
             [-p PROFILE] [-t TESTS] [-s SKIPS] [-l] [-i]
             [-f {csv,custom,html,json,screen,txt,xml,yaml}]
             [--msg-template MSG_TEMPLATE] [-o [OUTPUT_FILE]] [-v] [-d]
             [--ignore-nosec] [-x EXCLUDED_PATHS] [-b BASELINE]
             [--ini INI_PATH] [--version]
             [targets [targets ...]]
```

Bandit - a Python source code security analyzer

positional arguments:

targets source file(s) or directory(s) to be tested

optional arguments:

-h, --help show this help message and exit
-r, --recursive find and process files in subdirectories
-a {file,vuln}, --aggregate {file,vuln} aggregate output by vulnerability (default) or by filename
-n CONTEXT_LINES, --number CONTEXT_LINES maximum number of code lines to output for each issue
-c CONFIG_FILE, --configfile CONFIG_FILE optional config file to use for selecting plugins and overriding defaults
-p PROFILE, --profile PROFILE profile to use (defaults to executing all tests)
-t TESTS, --tests TESTS comma-separated list of test IDs to run

Metrics:

Total lines of code: 110675

Total lines skipped (#nosec): 0

blacklist: Consider possible security implications associated with subprocess module.

Test ID: B404

Severity: LOW

Confidence: HIGH

File: [libcloud/contrib/generate_provider_logos_collage_image.py](#)

More info: http://docs.openstack.org/developer/bandit/blacklists/blacklist_imports.html#b404-import_subprocess

```
31     import argparse
32     import subprocess
33     import random
```

subprocess_popen_with_shell_equals_true: subprocess call with shell=True identified, security issue.

Test ID: B602

Severity: HIGH

Confidence: HIGH

File: [libcloud/contrib/generate_provider_logos_collage_image.py](#)

More info: http://docs.openstack.org/developer/bandit/plugins/subprocess_popen_with_shell_equals_true.html

```
76         cmd = cmd % values
77         subprocess.call(cmd, shell=True)
78
```

subprocess_popen_with_shell_equals_true: subprocess call with shell=True identified, security issue.

Test ID: B602

Severity: HIGH

Confidence: HIGH

Plugin ID Groupings

ID	Description
B1xx	misc tests
B2xx	application/framework misconfiguration
B3xx	blacklists (calls)
B4xx	blacklists (imports)
B5xx	cryptography
B6xx	injection
B7xx	XSS

```
>> Issue: [B602:subprocess_popen_with_shell_equals_true] subprocess call with shell=True seems safe, but may be changed
in the future, consider rewriting without shell
Severity: Low Confidence: High
Location: subprocess_shell.py:12
More Info: https://bandit.readthedocs.io/en/latest/plugins/b602_subprocess_popen_with_shell_equals_true.html
10     pop('/bin/gcc --version', shell=True)
11     Popen('/bin/gcc --version', shell=True)
12
-----
>> Issue: [B604:any_other_function_with_shell_equals_true] Function call with shell=True parameter identified, possible
security issue.
Severity: Medium Confidence: Low
Location: subprocess_shell.py:12
More Info: https://bandit.readthedocs.io/en/latest/plugins/b604_any_other_function_with_shell_equals_true.html
11     pop('/bin/gcc --version', shell=True)
12     Popen('/bin/gcc --version', shell=True)
13
```

```
>> Issue: [B608:hardcoded_sql_expressions] Possible SQL injection vector through string-based query construction.
Severity: Medium Confidence: Low
Location: sql_statements.py:4
More Info: https://bandit.readthedocs.io/en/latest/plugins/b608_hardcoded_sql_expressions.html
3     # bad
4     query = "SELECT * FROM foo WHERE id = '%s'" % identifier
5     query = "INSERT INTO foo VALUES ('a', 'b', '%s')" % value
-----
>> Issue: [B608:hardcoded_sql_expressions] Possible SQL injection vector through string-based query construction.
Severity: Medium Confidence: Low
Location: sql_statements.py:5
More Info: https://bandit.readthedocs.io/en/latest/plugins/b608_hardcoded_sql_expressions.html
4     query = "SELECT * FROM foo WHERE id = '%s'" % identifier
5     query = "INSERT INTO foo VALUES ('a', 'b', '%s')" % value
6     query = "DELETE FROM foo WHERE id = '%s'" % identifier
-----
>> Issue: [B608:hardcoded_sql_expressions] Possible SQL injection vector through string-based query construction.
Severity: Medium Confidence: Low
Location: sql_statements.py:6
More Info: https://bandit.readthedocs.io/en/latest/plugins/b608_hardcoded_sql_expressions.html
5     query = "INSERT INTO foo VALUES ('a', 'b', '%s')" % value
6     query = "DELETE FROM foo WHERE id = '%s'" % identifier
7     query = "UPDATE foo SET value = 'b' WHERE id = '%s'" % identifier
```

ID	Name	Calls	Severity
B301	pickle	<ul style="list-style-type: none">• pickle.loads• pickle.load• pickle.Unpickler• cPickle.loads• cPickle.load• cPickle.Unpickler• dill.loads• dill.load• dill.Unpickler	Medium

```

143 + def _encode_invalid_chars(component, allowed_chars, encoding='utf-8'):
144 +     """Percent-encodes a URI component without reapplying
145 +     onto an already percent-encoded component. Based on
146 +     rfc3986.normalizers.encode_component()
147 +     """
148 +     if component is None:
149 +         return component
150 +
151 +     # Try to see if the component we're encoding is already percent-encoded
152 +     # so we can skip all '%' characters but still encode all others.
153 +     percent_encodings = len(normalizers.PERCENT_MATCHER.findall(
154 +         compat.to_str(component, encoding)))
155 +
156 +     uri_bytes = component.encode('utf-8', 'surrogatepass')
157 +     is_percent_encoded = percent_encodings == uri_bytes.count(b'%')
158 +
159 +     encoded_component = bytearray()
160 +
161 +     for i in range(0, len(uri_bytes)):
162 +         # Will return a single character bytestring on both Python 2 & 3
163 +         byte = uri_bytes[i:i+1]
164 +         byte_ord = ord(byte)
165 +         if ((is_percent_encoded and byte == b'%')
166 +             or (byte_ord < 128 and byte.decode() in allowed_chars)):
167 +             encoded_component.extend(byte)

```

General Options:

```

-h, --help                Show help.
--isolated                Run pip in an isolated mode, ignoring environment variables and user configuration.
-v, --verbose            Give more output. Option is additive, and can be used up to 3 times.
-V, --version            Show version and exit.
-q, --quiet              Give less output. Option is additive, and can be used up to 3 times (corresponding to
                        WARNING, ERROR, and CRITICAL logging levels).
--log <path>            Path to a verbose appending log.
--proxy <proxy>          Specify a proxy in the form [user:passwd@]proxy.server:port.
--retries <retries>     Maximum number of retries each connection should attempt (default 5 times).
--timeout <sec>         Set the socket timeout (default 15 seconds).
--exists-action <action> Default action when a path already exists: (s)witch, (i)gnore, (w)ipe, (b)ackup,
                        (a)abort).
--trusted-host <hostname> Mark this host as trusted, even though it does not have valid or any HTTPS.
--cert <path>           Path to alternate CA bundle.
--client-cert <path>   Path to SSL client certificate, a single file containing the private key and the
                        certificate in PEM format.

```


Search

python security



All (35)

Projects (2)

People (0)

Queries (28)

Help (5)

Queries (28)

Binding a socket to all network interfaces (py/bind-socket-all-network-interfaces)

Binding a socket to all interfaces opens it up to traffic from any IPv4 address and is therefore associated with security risks.

'input' function used in Python 2 (py/use-of-input)

The built-in function 'input' is used which, in Python 2, can allow arbitrary code to be run.

Use of insecure SSL/TLS version (py/insecure-protocol)

Using an insecure SSL/TLS version may leave the connection vulnerable to attacks.

Default version of SSL/TLS may be insecure (py/insecure-default-protocol)

Leaving the SSL/TLS version unspecified may result in an insecure default protocol being used.


Reflected server-side cross-site scripting (py/reflective-xss)

Writing user input directly to a web page allows for a cross-site scripting vulnerability.

Incomplete URL substring sanitization (py/incomplete-url-substring-sanitization)

Chapter 12: Python Tools for Forensics Analysis

Nombre	Tipo	Esquema
[-] Tablas (13)		
+ Category		CREATE TABLE "Category" ("Id" INTEGER PRIMARY
+ Customer		CREATE TABLE "Customer" ("Id" VARCHAR(8000) P
+ CustomerCustomerDemo		CREATE TABLE "CustomerCustomerDemo" ("Id" VA
+ CustomerDemographic		CREATE TABLE "CustomerDemographic" ("Id" VAR
+ Employee		CREATE TABLE "Employee" ("Id" INTEGER PRIMAR
+ EmployeeTerritory		CREATE TABLE "EmployeeTerritory" ("Id" VARCHAI
+ Order		CREATE TABLE "Order" ("Id" INTEGER PRIMARY KE
+ OrderDetail		CREATE TABLE "OrderDetail" ("Id" VARCHAR(8000
+ Product		CREATE TABLE "Product" ("Id" INTEGER PRIMARY I
+ Region		CREATE TABLE "Region" ("Id" INTEGER PRIMARY K
+ Shipper		CREATE TABLE "Shipper" ("Id" INTEGER PRIMARY I
+ Supplier		CREATE TABLE "Supplier" ("Id" INTEGER PRIMARY
+ Territory		CREATE TABLE "Territory" ("Id" VARCHAR(8000) PF
Índices (0)		
[-] Vistas (1)		
+ ProductDetails_V		CREATE VIEW [ProductDetails_V] as select p.*, c.Ca
Disparadores (0)		

SQL 1 

```
1 SELECT name FROM sqlite_master WHERE type='table';
```

	name
1	Employee
2	Category
3	Customer
4	Shipper
5	Supplier
6	Order
7	Product

Enter pcap file path: Browse Analyze!

Output directory path: Browse zoomIn zoomOut

Traffic: All From: All To: All InteractiveMagic! Visualize!

Select Packet Capture File!

Directorio:

- maliciousTraffic.pcap
- tamu_drivebyinc_0_intrusion.pcap
- tamu_microservice_0_intrusion.pcap
- tamu_readingrainbow_0_network_enumeration.pcap
- test.pcap
- torExample.pcap

Nombre de archivo: Abrir

Archivos de tipo: All (*.pcap,*.pcapng) Cancelar

Description:
PcapXray is an aid for
It is a tool aimed to simplyfy
This prototype aims to accom

1. Web Traffic
2. Tor Traffic
3. Malicious Traffic
4. Device/Traffic Details
5. Covert Communication

Please contact me @ spg349

Enter pcap file path: Browse Analyze!

Output directory path: Browse zoomIn zoomOut

Traffic: All From: All To: All InteractiveMagic! Visualize!

```

graph LR
    A((192.168.0.6  
78.4f.43.59.c1.6f  
Apple, Inc.))
    B((04.2000.71d6.400.3cc2.834.5d8e.c6bd  
54.13.79.f3.66.d2))
    C((54.13.79.f3.66.d2  
PossibleGateway))
    A -- TOR: 158.69.204.36 --> C
    A -- DNS: 209.18.47.61 --> C
    A -- HTTPS: 52.84.26.48: server-52-84-26-48.ewr50.r.cloudfront.net --> C
    B -- HTTPS: 2607.f8b0.400d.c00..93: qn-in-x93.1e100.net --> C
    B -- HTTPS: 2607.f8b0.4006.819..200e: lga34s19-in-x0e.1e100.net --> C
  
```

Chapter 13: Extracting Geolocation and Metadata from Documents, Images, and Browsers

HACKER TARGET SCANNERS TOOLS RESEARCH SERVICES

GeoIP – IP Location Lookup

Find the location of an IP address with this **GeoIP lookup** tool.


GET THE IP LOCATION

Nombre	Tipo	Esquema
- Tablas (13)		
+ moz_anno_attributes		CREATE TABLE moz_anno_attributes (id INTEGE
+ moz_annos		CREATE TABLE moz_annos (id INTEGER PRIMAR
+ moz_bookmarks		CREATE TABLE moz_bookmarks (id INTEGER PRI
+ moz_bookmarks_deleted		CREATE TABLE moz_bookmarks_deleted (guid T
+ moz_historyvisits		CREATE TABLE moz_historyvisits (id INTEGER PF
+ moz_inpuhistory		CREATE TABLE moz_inpuhistory (place_id INTE
+ moz_items_annos		CREATE TABLE moz_items_annos (id INTEGER P
+ moz_keywords		CREATE TABLE moz_keywords (id INTEGER PRIM
+ moz_meta		CREATE TABLE moz_meta (key TEXT PRIMARY K
+ moz_origins		CREATE TABLE moz_origins (id INTEGER PRIMAF
+ moz_places		CREATE TABLE moz_places (id INTEGER PRIMAR
+ sqlite_sequence		CREATE TABLE sqlite_sequence(name,seq)
+ sqlite_stat1		CREATE TABLE sqlite_stat1(tbl,idx,stat)

Name	Type	Schema
▼ Tables (12)		
> downloads		CREATE TABLE downloads (id INTEGER PRIMARY KEY, guid VARCHAR NOT NULL, current_path LONGVARCH
> downloads_slices		CREATE TABLE downloads_slices (download_id INTEGER NOT NULL, offset INTEGER NOT NULL, received_byt
> downloads_url_chains		CREATE TABLE downloads_url_chains (id INTEGER NOT NULL, chain_index INTEGER NOT NULL, url LONGVARC
> keyword_search_terms		CREATE TABLE keyword_search_terms (keyword_id INTEGER NOT NULL, url_id INTEGER NOT NULL, lower_terr
> meta		CREATE TABLE meta(key LONGVARCHAR NOT NULL UNIQUE PRIMARY KEY, value LONGVARCHAR)
> segment_usage		CREATE TABLE segment_usage (id INTEGER PRIMARY KEY, segment_id INTEGER NOT NULL, time_slot INTEGE
> segments		CREATE TABLE segments (id INTEGER PRIMARY KEY, name VARCHAR, url_id INTEGER NON NULL)
> sqlite_sequence		CREATE TABLE sqlite_sequence(name,seq)
> typed_url_sync_metadata		CREATE TABLE typed_url_sync_metadata (storage_key INTEGER PRIMARY KEY NOT NULL, value BLOB)
> urls		CREATE TABLE "urls"(id INTEGER PRIMARY KEY AUTOINCREMENT, url LONGVARCHAR, title LONGVARCHAR, r
> visit_source		CREATE TABLE visit_source(id INTEGER PRIMARY KEY, source INTEGER NOT NULL)
> visits		CREATE TABLE visits(id INTEGER PRIMARY KEY, url INTEGER NOT NULL, visit_time INTEGER NOT NULL, from_v
▼ Indices (11)		
> keyword_search_terms_in...		CREATE INDEX keyword_search_terms_index1 ON keyword_search_terms (keyword_id, lower_term)
> keyword_search_terms_in...		CREATE INDEX keyword_search_terms_index2 ON keyword_search_terms (url_id)
> keyword_search_terms_in...		CREATE INDEX keyword_search_terms_index3 ON keyword_search_terms (term)
> segment_usage_time_slo...		CREATE INDEX segment_usage_time_slot_segment_id ON segment_usage(time_slot, segment_id)
> segments_name		CREATE INDEX segments_name ON segments(name)
> segments_url_id		CREATE INDEX segments_url_id ON segments(url_id)
> segments_usage_seg_id		CREATE INDEX segments_usage_seg_id ON segment_usage(segment_id)
> urls_url_index		CREATE INDEX urls_url_index ON urls (url)
> visits_from_index		CREATE INDEX visits_from_index ON visits (from_visit)

Name	Type	Schema
▼ Tables (12)		
▼ downloads		CREATE TABLE downloads (id INTEGER PRIMARY KEY, guid VARCHAR NOT NULL, current_path LONGVARCH
id	INTEGER	`id` INTEGER
guid	VARCHAR	`guid` VARCHAR NOT NULL
current_path	LONGVARCHAR	`current_path` LONGVARCHAR NOT NULL
target_path	LONGVARCHAR	`target_path` LONGVARCHAR NOT NULL
start_time	INTEGER	`start_time` INTEGER NOT NULL
received_bytes	INTEGER	`received_bytes` INTEGER NOT NULL
total_bytes	INTEGER	`total_bytes` INTEGER NOT NULL
state	INTEGER	`state` INTEGER NOT NULL
danger_type	INTEGER	`danger_type` INTEGER NOT NULL
interrupt_reason	INTEGER	`interrupt_reason` INTEGER NOT NULL
hash	BLOB	`hash` BLOB NOT NULL
end_time	INTEGER	`end_time` INTEGER NOT NULL
opened	INTEGER	`opened` INTEGER NOT NULL
referrer	VARCHAR	`referrer` VARCHAR NOT NULL
site_url	VARCHAR	`site_url` VARCHAR NOT NULL
tab_url	VARCHAR	`tab_url` VARCHAR NOT NULL
tab_referrer_url	VARCHAR	`tab_referrer_url` VARCHAR NOT NULL
http_method	VARCHAR	`http_method` VARCHAR NOT NULL
by_ext_id	VARCHAR	`by_ext_id` VARCHAR NOT NULL
by_ext_name	VARCHAR	`by_ext_name` VARCHAR NOT NULL
etag	VARCHAR	`etag` VARCHAR NOT NULL

Hindsight is a free tool for analyzing web artifacts. To get started, select the 'Input Type' below and fill out the 'Input Path' field. Review the plugins and options on the right, and hit the 'Run' button at the bottom.

Inputs	
Input Type: <input type="text" value="Chrome"/>	Profile Path: <input type="text" value="/home/linux/.config/google-chrome/Default"/>
	Cache Path: <input type="text"/>
<p>Description: Chrome is a free web browser from Google that runs on Windows, Linux, OS X, IOS, and Android. Each user's web history and configuration information is stored under their user directory, so there may be multiple sets of browser data on the system.</p> 	
Available Decryption: Windows <input checked="" type="checkbox"/> Mac <input checked="" type="checkbox"/> Linux <input type="checkbox"/>	
Default Locations: Windows XP: %userdir%\Local Settings\Application Data\Google\Chrome\User Data Vista/7/8/10: %userdir%\AppData\Local\Google\Chrome\User Data Linux: %userdir%\config/google-chrome OSX/macOS: %userdir%\Library/Application Support/Google/Chrome/Default IOS: %userdir%\Applications\com.google.chrome.ios\Library\Application Support\Google\Chrome	

Plugin Selector
<input checked="" type="checkbox"/> Chrome Extension Names [v20150125]
<input checked="" type="checkbox"/> Generic Timestamp Decoder [v20160907]
<input checked="" type="checkbox"/> Google Analytics Cookie Parser [v20170130]
<input checked="" type="checkbox"/> Google Searches [v20160912]
<input checked="" type="checkbox"/> Load Balancer Cookie Decoder [v20200213]
<input checked="" type="checkbox"/> Quantcast Cookie Parser [v20160907]
<input checked="" type="checkbox"/> Query String Parser [v20170225]
<input checked="" type="checkbox"/> Time Discrepancy Finder [v20170129]

Options Selector
Log Path: <input type="text" value="hindsight.log"/>
Timezone: <input type="text" value="Pacific [-8/-7]"/>
<input type="button" value="Run"/>

Chapter 14: Cryptography and Steganography

No Images