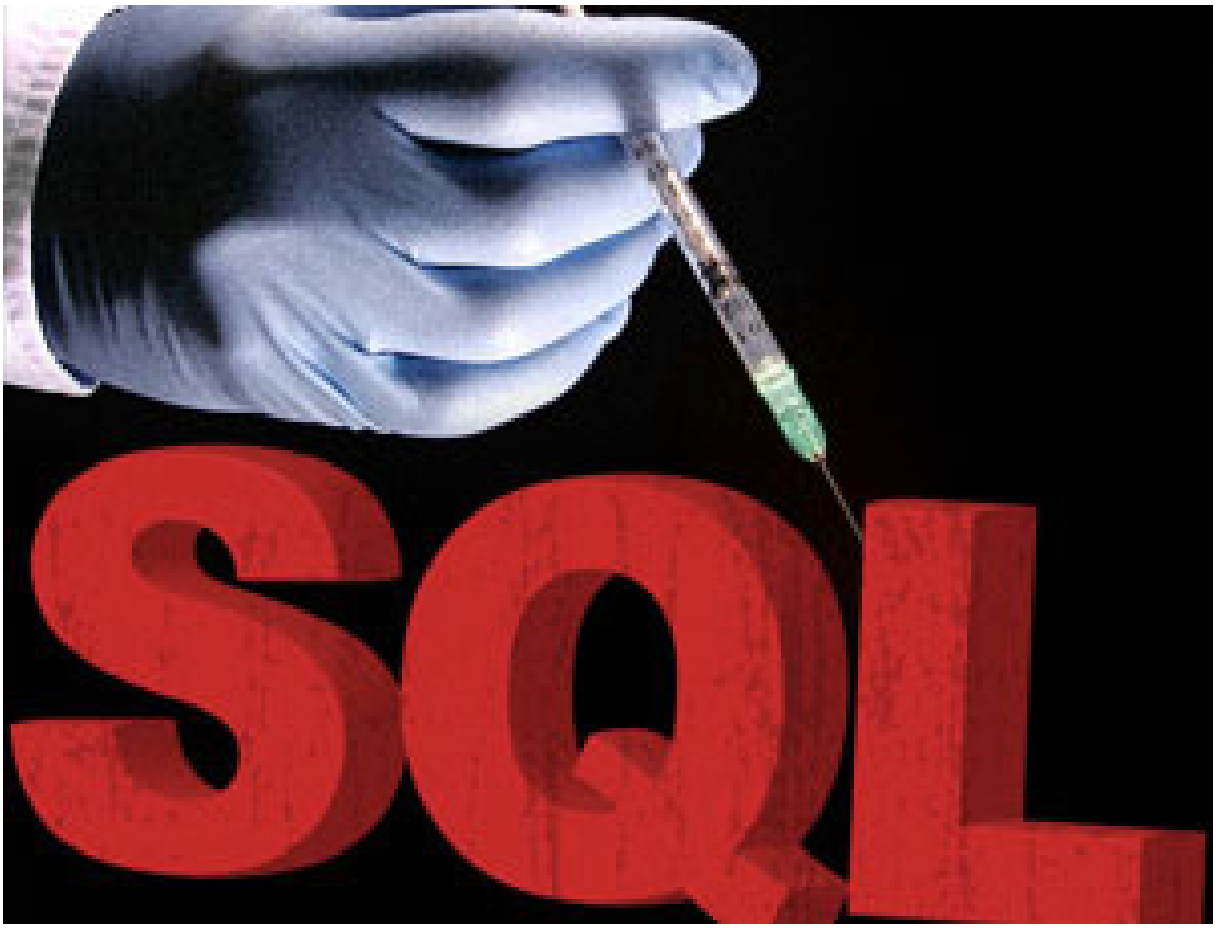
Criando um Scanner de SQL INJECTION



Do que prescisamos:

1. Python(http://www.python.org/download/) Eu uso a Versão 2.7.
2. Um Bom Celebro(Para Conseguir Ler).
3. Um Conhecimento Basico de Python
4. Ser persiste e Esperto.:-)

O Criando o Scanner...

Bom me nome é C4SS!0 G0M3S, a algum tempo vi uns tuturiais de um cara chamado INJ3CT0R P4CK3T, ensinando a criar varias ferramentas,
pena que o exploit-db DELETOU:-(.
Entao Resolvi criar esse tuturial mostrando como criar um scanner de SQL só q em python.

Chega de falar vamos ao trabalho:

Os Modulos necessarios httplib,urllib.
urllib ===> Permite Pegar o Conteudo todo de uma pagina
urllib.urlopen("http:/www.google.com").read() mostra todo os codigo HTML do google.

==========

```
#!/usr/bin/python

import urllib
```

==========

Erros de SQL em no MYSQL retorna o valor **Warning**: mysql_result():
Exemplo http://www.apostilando.com/pagina.php?cod=1' ,
Bom precisamos identificar tambem erros no oracle SQL,Portgress SQL,Microsoft SQL Server.

MYSQL ==> **Warning**: mysql_result():
MSSQL ==> [Microsoft][ODBC SQL Server Driver][SQL Server]
`ORACLE ==> Warning: ociexecute`
`POSTGRESS ==> Warning: pq_query[function.pg-query]:`

Usamos a Funçao do urllib

==========

host = urllib.urlopen("http://www.exploit-db.com.br/").read()
if host.find("**Warning**: mysql_result(): ") != -1:
    print "PAGE VULNERAVEL"

Com a funçao find procuramos pela STRING de erro de SQL se encontra retorna um valor diferente de -1.

O Codigo Final do Scanner:

```
#!/usr/bin/python
#
#Criado por C4SS!0 G0M3S
#Site www.exploit-br.org
#E-mail Louredo_@hotmail.com
#
#

import urllib
import httplib
import os
import sys

if os.name == "nt":
    os.system("cls")
    os.system("color 4f")
else:
    os.system("clear")


def usage():
    print """

          ================================================
          ================================================
          ============SQL INJECTION SCANNER===============
          ============Criado por C4SS!0 G0M3S==============
```

```
        ============Louredo_@hotmail.com==================
        ================================================
        ================================================

"""
def scanner(url):
    try:
        page = urllib.urlopen(url).read()
    except:
        print "[-]Erro ao se Conectar no Servidor\n"
        return(0)
    sqls = ("mysql_result(): supplied argument is not a valid MySQL result
resource in","[Microsoft][ODBC SQL Server Driver][SQL Server]","Warning:
ociexecute","Warning: pq_query[function.pg-query]:")
    i=0
    page = str(page.lower())
    while i<len(sqls):
        sql = str(sqls[i]).lower()
        if page.find(sql[i]) == -1:
            check=0
        else:
            check=1
        i+=1
    if check == 0:
        print "[-]"+url+"     <Nao Vulneravel>"
    else:
        print "[+]"+url+"     <Vulneravel>"


def main(args):
    if len(args)!=2:
        usage()
        print "\t\t[-]Modo de Uso: %s <File>\n" % sys.argv[0]
        print "\t\t[-]Exemplo: %s Site.txt\n"  % sys.argv[0]
        sys.exit(0)
    usage()
    try:
        f = open(str(sys.argv[1]),"r")
         urls = f.readlines()
    except:
        print "[+]Erro ao Abrir o Arquivo "+sys.argv[1]+""
         return(-1)
```

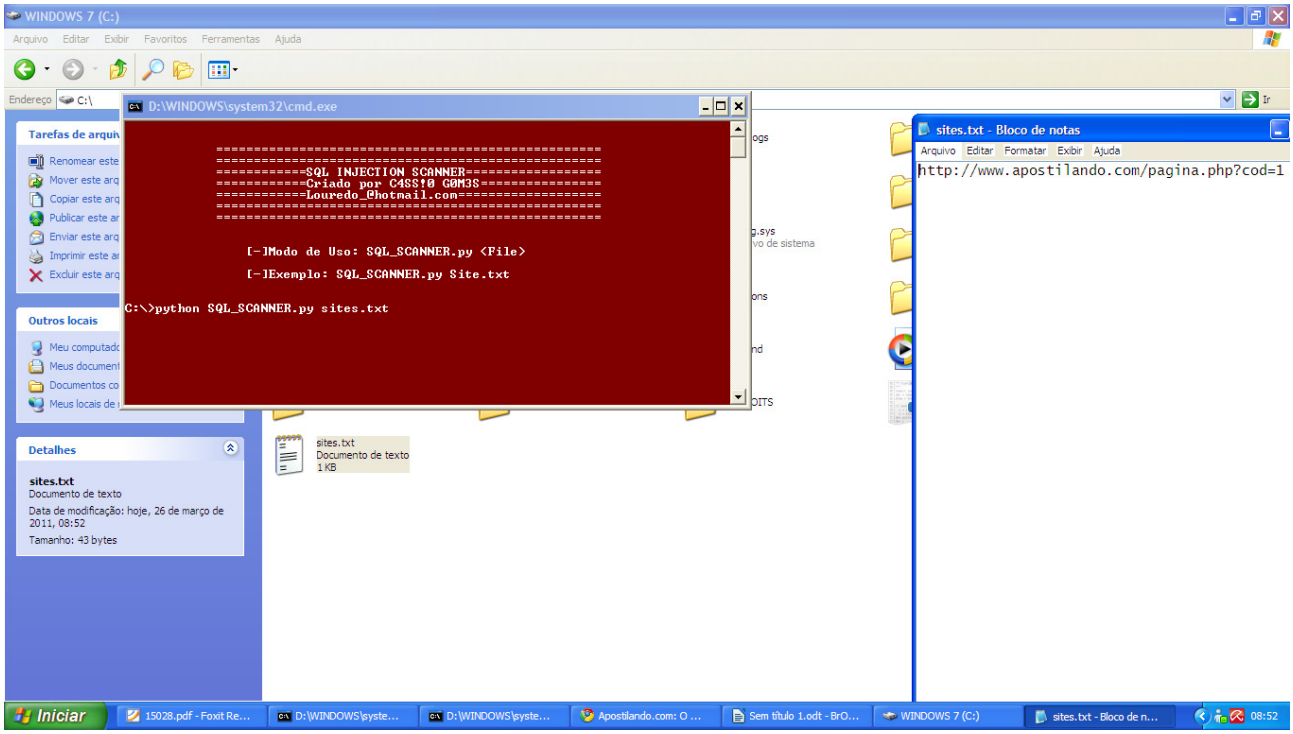
```
    f.close()
    i=0
    while i<len(urls):
        if urls[i].find("http://") == -1:
            urls[i] = "http://" + urls[i]
        urls[i] = urls[i].replace("\n","")
        a = scanner(urls[i]+"'")
        i+=1

if 0xffffffff > 0xffffff:
    main(sys.argv)
```

Download: http://www.mediafire.com/?ltan89moim4m600

Executando:

Copie ele para uma pasta, eu coloca no disco C:\ vá no CMD e digite cd c:\
depois digite python SQL_SCANNER.py sites.txt
sites.txt sera o arquivo que tera todos os URLS que sera scanneados um em cada linha.



Bom Galera por hoje é usem com cuidado o scanner ATÉ MAIS VALEU!!!!!!

Name: C4SS!0 G0M3S
E-mail: Louredo_@hotmail.com
Site: www.exploit-br.org