

Laboratório Pessoal – 1

Lucas V Areal

Esse laboratório tem como finalidade estudo e aperfeiçoamento de habilidade técnicas adquiridas durante as aulas da faculdade tecnológica em segurança da informação pela FATEC – São Caetano do Sul. Todos os registros, dados, informações, endereços de rede ou endereços físicos, fotos, imagens e demais dados adquiridos, registrados ou documentados são fictícios e criados somente com finalidade de estudos.

Não é permitida a publicação, disseminação, uso indevido, alteração desse documento sem autorização expressa do autor.

Para o funcionamento adequado desse laboratório, foram utilizados os seguintes sistemas:

- VMWare workstation – Aplicativo para virtualização de máquinas para evitar o comprometimento a máquina hospedeira e também para possibilitar uma fácil recuperação dos sistemas utilizados em casos de infecção, bug, erros fatais e dentre outros;
- Kali Linux – Distribuição Linux baseada em Debian de código aberto, focado em segurança da informação, pentest, engenharia reversa, forense digital, cibersegurança ofensiva;
- Metasploitable2 – Máquina virtual deliberadamente vulnerável com finalidade de estudos e testes em ambientes controlados de segurança da informação, especialmente para pentest e análise de vulnerabilidades.

O preparo do ambiente foi realizado aplicando o processo de hardening da máquina hospedeira, de forma a blindá-la contra possíveis vazamentos ou contaminações do laboratório. Para esse processo, utilizei a virtualização através da VMware workstation de ambas as máquinas (Kali Linux e Metasploitable2), isolando a rede em modo Host-Only, ativei o firewall da máquina hospedeira, mantive o antivírus em execução durante todo o processo a fim de identificar possíveis vazamentos e rápida resposta para tratamento nessa situação, atualizado o sistema operacional hospedeiro, removidas todos os adaptadores não necessários para o laboratório das máquinas virtuais.

Abaixo você encontrará todas as etapas registradas com printscreens de todo o processo.

Identificação de Vulnerabilidades

Identificando os Hosts

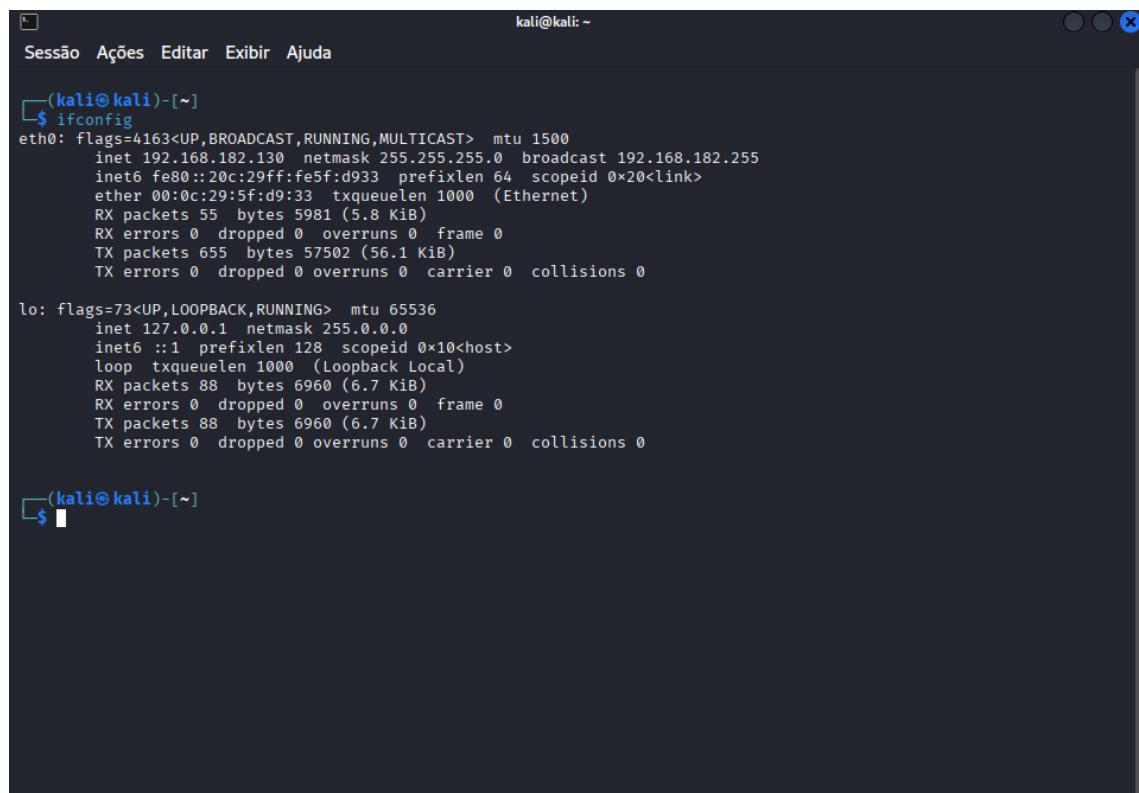
Foi utilizado o comando `ifconfig` para verificar a configuração de rede no modo host-only em ambas as máquinas, sendo a Metasploitable2 (vou chamar de vulnerável a partir deste momento) o **endereço IP 192.168.182.129** e a Kali Linux (vou chamar de Kali a partir deste momento) o **endereço IP 192.168.182.130**

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:0b:15:d3
          inet addr:192.168.182.129 Bcast:192.168.182.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe0b:15d3/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:20 errors:0 dropped:0 overruns:0 frame:0
             TX packets:76 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:3148 (3.0 KB) TX bytes:10363 (10.1 KB)
             Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
             UP LOOPBACK RUNNING MTU:16436 Metric:1
             RX packets:261 errors:0 dropped:0 overruns:0 frame:0
             TX packets:261 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:0
             RX bytes:103657 (101.2 KB) TX bytes:103657 (101.2 KB)

msfadmin@metasploitable:~$ _
```

Figura 1 - configuração de rede metasploitable2



A screenshot of a terminal window titled "kali@kali: ~". The window has a dark theme with white text. The title bar includes standard window controls (minimize, maximize, close). The menu bar at the top has options: Sessão, Ações, Editar, Exibir, Ajuda. Below the menu is a command-line interface. The user has run the command `ifconfig`. The output shows two network interfaces: `eth0` and `lo`. The `eth0` interface is an Ethernet connection with MAC address `00:0c:29:0b:15:d3`, IP address `192.168.182.130`, subnet mask `255.255.255.0`, broadcast address `192.168.182.255`, and MTU of 1500. It has received 20 packets and transmitted 76 packets. The `lo` interface is a loopback connection with IP address `127.0.0.1` and MTU of 16436. Both interfaces show 0 errors, 0 dropped packets, and 0 overruns.

```
kali@kali: ~
Sessão Ações Editar Exibir Ajuda
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.182.130 netmask 255.255.255.0 broadcast 192.168.182.255
          inet6 fe80::20c:29ff:fe0b:15d3/64 scopeid 0x20<link>
            ether 00:0c:29:0b:15:d3 txqueuelen 1000 (Ethernet)
            RX packets 55 bytes 5981 (5.8 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 655 bytes 57502 (56.1 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
      loop txqueuelen 1000 (Loopback Local)
      RX packets 88 bytes 6960 (6.7 KiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 88 bytes 6960 (6.7 KiB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kali)-[~]
$
```

Figura 2 - configuração de rede Kali Linux

Mapeamento de portas e serviços

Após identificação de ambas as redes, utilizei o comando `nmap -sV -sC -O 192.168.182.129 -oN resultados_scan.txt` para a descoberta do host e portas e salvar em um arquivo normal de texto. A opção `-sV` utilizada para sondar as portas abertas para determinar informações de serviços e versões, a opção `-sC` habilita o Nmap Script Engine, executando scripts padrões que automatizam tarefas de descoberta, enumeração e detecção de vulnerabilidades e `-O` para determinar o tipo de sistema operacional em uso, enquanto a opção `-oN` é utilizada para salvar em um arquivo normal de texto.

```
(kali㉿kali)-[~]
└─$ nmap -sV -sC 192.168.182.129 -oN resultado_scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 18:00 -03
Nmap scan report for 192.168.182.129
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-syst:
|_STAT:
| FTP server status:
|   Connected to 192.168.182.130
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cfc:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8
BITMIME, DSN
53/tcp    open  domain       ISC BIND 9.4.2
| dns-nsid:
|_bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp    rpcbind
|   100000  2          111/udp   rpcbind
|   100003  2,3,4     2049/tcp   nfs
|   100003  2,3,4     2049/udp   nfs
|   100005  1,2,3     51630/tcp  mountd
|   100005  1,2,3     54861/udp  mountd
|   100021  1,3,4     46957/udp  nlockmgr
|   100021  1,3,4     55193/tcp  nlockmgr
|   100024  1          43371/tcp  status
```

Figura 3 - parte 1 do scan nmap

```

Sessão 74685 Editar Exportar PyAdd
| 100024 1      43371/tcp  status
|_ 100024 1      54089/udp  status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec      netkit-rsh rexecd
513/tcp open  login?
514/tcp open  shell     Netkit rshd
1099/tcp open  java-rmi  GNU Classpath grmiregistry
1524/tcp open  bindshell Metasploitable root shell
2049/tcp open  nfs      2-4 (RPC #100003)
2121/tcp open  ftp      ProFTPD 1.3.1
3306/tcp open  mysql    MySQL 5.0.51a-3ubuntu5
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 8
| Capabilities flags: 43564
| Some Capabilities: Support41Auth, SupportsTransactions, Speaks41ProtocolNew, SwitchToSSLAfterHandshake, LongColu
mnFlag, SupportsCompression, ConnectWithDatabase
| Status: Autocommit
|_ Salt: 1.3$.-Y$B =0$7W0+$s8
5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no su
ch thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_ Not valid after: 2010-04-16T14:07:45
|_ssl-date: 2025-12-09T20:16:41+00:00; -47m06s from scanner time.
5900/tcp open  vnc      VNC (protocol 3.3)
| vnc-info:
| Protocol version: 3.3
| Security types:
|_ VNC Authentication (2)
6000/tcp open  X11      (access denied)
6667/tcp open  irc      UnrealIRCd
8009/tcp open  ajp13    Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  unknown
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
MAC Address: 00:0C:29:0B:15:D3 (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_
kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable

```

Figura 4 - parte 2 do scan nmap

```

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2025-12-09T15:16:18-05:00
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: 53m00s, deviation: 2h53m24s, median: -47m06s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 281.67 seconds

```

Figura 5 - parte final do scan nmap

A seguir você poderá visualizar em formato de texto salvo durante o scan o resultado dele:

```
#Nmap 7.95 scan initiated Tue Dec 9 18:00:13 2025 as: /usr/lib/nmap/nmap --privileged -
sV -sC -oN resultado_scan.txt 192.168.182.129
```

Nmap scan report for 192.168.182.129

Host is up (0.0017s latency).

Not shown: 977 closed tcp ports (reset)

PORt STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

| ftp-syst:

| STAT:

| FTP server status:

| Connected to 192.168.182.130

| Logged in as ftp

| TYPE: ASCII

| No session bandwidth limit

| Session timeout in seconds is 300

| Control connection is plain text

| Data connections will be plain text

| vsFTPD 2.3.4 - secure, fast, stable

|_End of status

|_ftp-anon: Anonymous FTP login allowed (FTP code 230)

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

| ssh-hostkey:

| 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)

|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)

23/tcp open telnet Linux telnetd

25/tcp open smtp Postfix smtpd

|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN

53/tcp open domain ISC BIND 9.4.2

| dns-nsid:

|_ bind.version: 9.4.2

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

|_http-title: Metasploitable2 - Linux

111/tcp open rpcbind 2 (RPC #100000)

| rpcinfo:

| program version port/proto service

| 100000 2 111/tcp rpcbind

| 100000 2 111/udp rpcbind

| 100003 2,3,4 2049/tcp nfs

| 100003 2,3,4 2049/udp nfs

| 100005 1,2,3 51630/tcp mountd

| 100005 1,2,3 54861/udp mountd

| 100021 1,3,4 46957/udp nlockmgr

| 100021 1,3,4 55193/tcp nlockmgr

| 100024 1 43371/tcp status

|_ 100024 1 54089/udp status

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

512/tcp open exec netkit-rsh rexecd

513/tcp open login?

514/tcp open shell Netkit rshd

1099/tcp open java-rmi GNU Classpath grmiregistry

1524/tcp open bindshell Metasploitable root shell

2049/tcp open nfs 2-4 (RPC #100003)

2121/tcp open ftp ProFTPD 1.3.1

3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

| mysql-info:

| Protocol: 10

| Version: 5.0.51a-3ubuntu5

| Thread ID: 8

| Capabilities flags: 43564

| Some Capabilities: Support41Auth, SupportsTransactions, Speaks41ProtocolNew, SwitchToSSLAfterHandshake, LongColumnFlag, SupportsCompression, ConnectWithDatabase

| Status: Autocommit

|_ Salt: 1.3S,~Y\$B` =OS7W0+\$s8

5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX

| Not valid before: 2010-03-17T14:07:45

|_Not valid after: 2010-04-16T14:07:45

|_ssl-date: 2025-12-09T20:16:41+00:00; -47m06s from scanner time.

5900/tcp open vnc VNC (protocol 3.3)

| vnc-info:

| Protocol version: 3.3

| Security types:

|_ VNC Authentication (2)

6000/tcp open X11 (access denied)

6667/tcp open irc UnrealIRCd

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

|_ajp-methods: Failed to get a valid response for the OPTION request

8180/tcp open unknown

|_http-title: Apache Tomcat/5.5

|_http-favicon: Apache Tomcat

MAC Address: 00:0C:29:0B:15:D3 (VMware)

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:

|_smb2-time: Protocol negotiation failed (SMB2)

| smb-os-discovery:

| OS: Unix (Samba 3.0.20-Debian)

| Computer name: metasploitable

| NetBIOS computer name:

| Domain name: localdomain

| FQDN: metasploitable.localdomain

```
|_ System time: 2025-12-09T15:16:18-05:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
 |_ message_signing: disabled (dangerous, but default)
 |_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
 |_clock-skew: mean: 53m00s, deviation: 2h53m24s, median: -47m06s
```

Service detection performed. Please report any incorrect results at
<https://nmap.org/submit/>.

Nmap done at Tue Dec 9 18:04:54 2025 -- 1 IP address (1 host up) scanned in 281.67 seconds

Através desse resultado, podemos visualizar que existem diversos serviços e portas abertas que são vetores conhecidos de ataques que estão marcadas em **amarelo** para facilitar a visualização.

Mapeamento das vulnerabilidades

Agora que possuímos essas informações salvas para futuramente utilizarmos se necessário, vou utilizar o comando **nmap --script vuln 192.168.182.129** para utilizar os scripts padrões e identificar as vulnerabilidades do host investigado.

```
(kali㉿kali)-[~]
└─$ nmap --script vuln 192.168.182.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 18:22 -03
Nmap scan report for 192.168.182.129
Host is up (0.0023s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
|_  ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: BID:48539  CVE:CVE-2011-2523
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|       Disclosure date: 2011-07-03
|       Exploit results:
|         Shell command: id
|         Results: uid=0(root) gid=0(root)
|       References:
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|         https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|         http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|         https://www.securityfocus.com/bid/48539
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
|_ smtp-vuln-cve2010-4344:
|   The SMTP server is not Exim: NOT VULNERABLE
53/tcp    open  domain
80/tcp    open  http
| http-slowloris-check:
|   VULNERABLE:
|     Slowloris DOS attack
|       State: LIKELY VULNERABLE
|       IDs: CVE:CVE-2007-6750
|         Slowloris tries to keep many connections to the target web server open and hold
|         them open as long as possible. It accomplishes this by opening connections to
|         the target web server and sending a partial request. By doing so, it starves
|         the http server's resources causing Denial Of Service.
|
|       Disclosure date: 2009-09-17
|       References:
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|         http://ha.ckers.org/slowloris/
|_ http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| http-sql-injection:
|   Possible sqli for queries:
```

Figura 6 - parte 1 mapeamento de vulnerabilidades

```

Possible sql for queries:
http://192.168.182.129:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
http://192.168.182.129:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
http://192.168.182.129:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
http://192.168.182.129:80/mutillidae/?page=login.php%27%20OR%20sqlspider
http://192.168.182.129:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
http://192.168.182.129:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
http://192.168.182.129:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
http://192.168.182.129:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
http://192.168.182.129:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
http://192.168.182.129:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
http://192.168.182.129:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
http://192.168.182.129:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
http://192.168.182.129:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
http://192.168.182.129:80/mutillidae/index.php?page=home.php&do=toggle-security%27%20OR%20sqlspider
http://192.168.182.129:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
http://192.168.182.129:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
http://192.168.182.129:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
http://192.168.182.129:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider
der
http://192.168.182.129:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
http://192.168.182.129:80/mutillidae/index.php?page=home.php&do=toggle-hints%27%20OR%20sqlspider
http://192.168.182.129:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
http://192.168.182.129:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
http://192.168.182.129:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-
network.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
| http://192.168.182.129:80/dav/?C=N%3B0%3DD%27%20OR%20sqlspider
| http://192.168.182.129:80/dav/?C=D%3B0%3DA%27%20OR%20sqlspider
| http://192.168.182.129:80/dav/?C=M%3B0%3DA%27%20OR%20sqlspider

```

Figura 7 - parte 2 mapeamento de vulnerabilidades

```
| http://192.168.182.129:80/dav/?C=S%3B0%3DA%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=home.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=login.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider
der
| http://192.168.182.129:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-
network.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=change-log.htm&do=toggle-hints%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=change-log.htm&do=toggle-security%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=home.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=login.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
```

Figura 8 - parte 3 mapeamento de vulnerabilidades

```

| http://192.168.182.129:80/mutillidae/?page=text-file-viewer.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=secret-administrative-pages.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=credits.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=set-background-color.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=browser-info.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=captured-data.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=view-someones-blog.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=show-log.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%200R%20sqlspi
der
| http://192.168.182.129:80/mutillidae/index.php?page=credits.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2How-to-access-Mutillidae-over-Virtual-Box-
network.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=register.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=installation.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=source-viewer.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=source-viewer.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=show-log.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=html5-storage.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=user-poll.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=user-info.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=login.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=capture-data.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=add-to-your-blog.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=text-file-viewer.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=dns-lookup.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=change-log.htm%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=add-to-your-blog.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=home.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=login.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=view-someones-blog.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=user-info.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=framing.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=text-file-viewer.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=secret-administrative-pages.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=credits.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=set-background-color.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=browser-info.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=captured-data.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=home.php%do=toggle-security%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=view-someones-blog.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=show-log.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%200R%20sqlspi

```

Figura 9 - parte 4 mapeamento de vulnerabilidades3

```

| http://192.168.182.129:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=home.php&do=toggle-hints%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=notes.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=html5-storage.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=usage-instructions.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-
network.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=register.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=installation.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=source-viewer.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=source-viewer.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=dns-lookup.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=show-log.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=php-errors.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=user-poll.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=user-info.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=credits.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=login.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=capture-data.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=add-to-your-blog.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=text-file-viewer.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=change-log.htm%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=add-to-your-blog.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=login.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=view-someones-blog.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=user-info.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=text-file-viewer.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=secret-administrative-pages.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=credits.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=set-background-color.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=browser-info.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=captured-data.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=view-someones-blog.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=show-log.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%200R%20sqlspi
der
| http://192.168.182.129:80/mutillidae/?page=register.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-
network.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=installation.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=register.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=framing.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=source-viewer.php%27%200R%20sqlspider

```

Figura 10 - parte 5 mapeamento de vulnerabilidades

```
| http://192.168.182.129:80/mutillidae/index.php?page=register.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=framing.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=source-viewer.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=source-viewer.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=dns-lookup.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=show-log.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=home.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=html5-storage.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=user-poll.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=user-info.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=credits.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=login.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=capture-data.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=add-to-your-blog.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=text-file-viewer.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=change-log.htm%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=add-to-your-blog.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=login.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=view-someones-blog.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=user-info.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=framing.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=text-file-viewer.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=secret-administrative-pages.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=credits.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=set-background-color.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=browser-info.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=captured-data.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=view-someones-blog.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=show-log.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-
network.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=installation.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=register.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=source-viewer.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=source-viewer.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=dns-lookup.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=show-log.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=home.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=html5-storage.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=user-poll.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=user-info.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=credits.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=login.php%27%200R%20sqlspider
```

Figura 11 - parte 6 mapeamento de vulnerabilidades

```

| http://192.168.182.129:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspi
der
| http://192.168.182.129:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=login.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspi
der
| http://192.168.182.129:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=register.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-
network.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=login.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider

```

Figura 12 - parte 7 mapeamento de vulnerabilidades

```
| http://192.168.182.129:80/mutillidae/?page=login.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=view-someones-blog.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=user-info.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=framing.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=text-file-viewer.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=secret-administrative-pages.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=credits.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=set-background-color.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=Browser-Info.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=captured-data.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=view-someones-blog.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=show-log.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%200R%20sqlspider
der
| http://192.168.182.129:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=Documentation%2FHow-to-access-Mutillidae-over-Virtual-Box-
network.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=register.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=installation.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=source-viewer.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=source-viewer.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=dns-lookup.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=show-log.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=html5-storage.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=user-poll.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=user-info.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=credits.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=login.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=capture-data.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=add-to-your-blog.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=text-file-viewer.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=change-log.htm%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=add-to-your-blog.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=home.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=login.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=view-someones-blog.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=user-info.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=framing.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=text-file-viewer.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=secret-administrative-pages.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=credits.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=set-background-color.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=Browser-Info.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=captured-data.php%27%200R%20sqlspider
```

Figura 13 - parte 8 mapeamento de vulnerabilidades

```
| http://192.168.182.129:80/mutillidae/index.php?page=captured-data.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=view-someones-blog.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=show-log.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%200R%20sqlspi
der
| http://192.168.182.129:80/mutillidae/index.php?page=rene-magritte.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-
network.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=installation.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=register.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=source-viewer.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=source-viewer.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=dns-lookup.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=show-log.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=html5-storage.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=user-info.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=user-poll.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=credits.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=login.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=capture-data.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=add-to-your-blog.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%200R%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=text-file-viewer.php%27%200R%20sqlspider
Possible sql for forms:
Form at path: /mutillidae/, form's action: ./index.php?page=user-info.php. Fields that might be vulnerable:
    username
http-trace: TRACE is enabled
http-CSRF:
Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.182.129
Found the following possible CSRF vulnerabilities:

Path: http://192.168.182.129:80/dvwa/
Form id:
Form action: login.php

Path: http://192.168.182.129:80/mutillidae/?page=login.php
Form id: id-loginform
Form action: index.php?page=login.php

Path: http://192.168.182.129:80/mutillidae/index.php?page=view-someones-blog.php
Form id: id-bad-blog-entry-tr
Form action: index.php?page=view-someones-blog.php

Path: http://192.168.182.129:80/mutillidae/?page=user-info.php
Form id: id-bad-cred-tr
Form action: ./index.php?page=user-info.php
```

Figura 14 - parte 9 mapeamento de vulnerabilidades

```
|   Path: http://192.168.182.129:80/mutillidae/?page=user-info.php
|   Form id: id-bad-cred-tr
|_  Form action: ./index.php?page=user-info.php
| http-enum:
| /tikiwiki/: Tikiwiki
| /test/: Test page
| /phpinfo.php: Possible information file
| /phpMyAdmin/: phpMyAdmin
| /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
| /icons/: Potentially interesting folder w/ directory listing
|_ /index/: Potentially interesting folder
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
| rmi-vuln-classloader:
| VULNERABLE:
| RMI registry default configuration remote code execution vulnerability
| State: VULNERABLE
| Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
|
| References:
|_ https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
| ssl-ccs-injection:
| VULNERABLE:
| SSL/TLS MITM vulnerability (CCS Injection)
| State: VULNERABLE
| Risk factor: High
| OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
| does not properly restrict processing of ChangeCipherSpec messages,
| which allows man-in-the-middle attackers to trigger use of a zero
| length master key in certain OpenSSL-to-OpenSSL communications, and
| consequently hijack sessions or obtain sensitive information, via
| a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
| References:
|_ http://www.cvedetails.com/cve/2014-0224
```

Figura 15 - parte 10 mapeamento de vulnerabilidades

```

|      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|_ http://www.openssl.org/news/secadv_20140605.txt
| ssl-dh-params:
|   VULNERABLE:
|     Diffie-Hellman Key Exchange Insufficient Group Strength
|       State: VULNERABLE
|         Transport Layer Security (TLS) services that use Diffie-Hellman groups
|         of insufficient strength, especially those using one of a few commonly
|         shared groups, may be susceptible to passive eavesdropping attacks.
| Check results:
|   WEAK DH GROUP 1
|     Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
|     Modulus Type: Safe prime
|     Modulus Source: Unknown/Custom-generated
|     Modulus Length: 1024
|     Generator Length: 8
|     Public Key Length: 1024
|   References:
|     https://weakdh.org
| ssl-poodle:
|   VULNERABLE:
|     SSL POODLE information leak
|       State: VULNERABLE
|       IDs: BID:70574 CVE:CVE-2014-3566
|         The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|         products, uses nondeterministic CBC padding, which makes it easier
|         for man-in-the-middle attackers to obtain cleartext data via a
|         padding-oracle attack, aka the "POODLE" issue.
|       Disclosure date: 2014-10-14
|   Check results:
|     TLS_RSA_WITH_AES_128_CBC_SHA
|   References:
|     https://www.securityfocus.com/bid/70574
|     https://www.openssl.org/~bodo/ssl-poodle.pdf
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|_ https://www.imperialviolet.org/2014/10/14/poodle.html
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See http://seclists.org/fulldisclosure/2010/Jun/277
8009/tcp open  ajp13
8180/tcp open  unknown
| http-cookie-flags:
| /admin/:
|   JSESSIONID:
|     httponly flag not set
|   /admin/index.html:

```

Figura 16 - parte 11 mapeamento de vulnerabilidades

```

|   JSESSIONID:
|_ httponly flag not set
| http-enum:
| /admin/: Possible admin folder
| /admin/index.html: Possible admin folder
| /admin/login.html: Possible admin folder
| /admin/admin.html: Possible admin folder
| /admin/account.html: Possible admin folder
| /admin/admin_login.html: Possible admin folder
| /admin/home.html: Possible admin folder
| /admin/admin-login.html: Possible admin folder
| /admin/adminLogin.html: Possible admin folder
| /admin/controlpanel.html: Possible admin folder
| /admin/cp.html: Possible admin folder
| /admin/index.jsp: Possible admin folder
| /admin/login.jsp: Possible admin folder
| /admin/admin.jsp: Possible admin folder
| /admin/home.jsp: Possible admin folder
| /admin/controlpanel.jsp: Possible admin folder
| /admin/admin-login.jsp: Possible admin folder
| /admin/cp.jsp: Possible admin folder
| /admin/account.jsp: Possible admin folder
| /admin/admin_login.jsp: Possible admin folder
| /admin/adminLogin.jsp: Possible admin folder
| /manager/html/upload: Apache Tomcat (401 Unauthorized)
| /manager/html: Apache Tomcat (401 Unauthorized)
| /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
| /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
| /admin/jscript/upload.html: Lizard Cart/Remote File upload
|_ /webdav/: Potentially interesting folder
MAC Address: 00:0C:29:0B:15:D3 (VMware)

Host script results:
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-061: false
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 329.33 seconds

```

Figura 17 - parte final mapeamento de vulnerabilidades

Através desse mapeamento completo das vulnerabilidades expostas e já conhecidas, conseguimos compreender a extensão completa de todos os possíveis vetores de ataques, suas técnicas e procedimento para realização. Abaixo você poderá visualizar o resultado desse mapeamento em forma de texto, podendo também se dirigir a página da vulnerabilidade para entender como o vetor de ataque pode afetar seu sistema, além de conseguir visualizar a importância sobre os tratamentos das CVE.

```
Nmap scan report for 192.168.182.129
Host is up (0.0023s latency).

Not shown: 977 closed tcp ports (reset)

PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: BID:48539 CVE:CVE-2011-2523
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|         Disclosure date: 2011-07-03
|         Exploit results:
|           Shell command: id
|           Results: uid=0(root) gid=0(root)
|         References:
|           https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|           https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|           http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|             https://www.securityfocus.com/bid/48539
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
| smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
53/tcp    open  domain
```

80/tcp open http

| http-slowloris-check:

| VULNERABLE:

| Slowloris DOS attack

| State: LIKELY VULNERABLE

| IDs: CVE:CVE-2007-6750

| Slowloris tries to keep many connections to the target web server open and hold them open as long as possible. It accomplishes this by opening connections to the target web server and sending a partial request. By doing so, it starves the http server's resources causing Denial Of Service.

|

| Disclosure date: 2009-09-17

| References:

| <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750>

|_ <http://ha.ckers.org/slowloris/>

|_http-vuln-cve2017-100100: ERROR: Script execution failed (use -d to debug)

| http-sql-injection:

| Possible sqli for queries:

| <http://192.168.182.129:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider>

| <http://192.168.182.129:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider>

|

| <http://192.168.182.129:80/mutillidae/?page=home.php%27%20OR%20sqlspider>

| <http://192.168.182.129:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider>

| <http://192.168.182.129:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider>

|

| <http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider>

|
| http://192.168.182.129:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=home.php&do=toggle-security%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|
http://192.168.182.129:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=home.php&do=toggle-hints%27%20OR%20sqlspider
|
http://192.168.182.129:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider

|
| http://192.168.182.129:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
| http://192.168.182.129:80/dav/?C=N%3BO%3DD%27%20OR%20sqlspider
| http://192.168.182.129:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
| http://192.168.182.129:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
| http://192.168.182.129:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider

|
http://192.168.182.129:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=login.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider

|
http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider

|
http://192.168.182.129:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=credits.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider

|
http://192.168.182.129:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider

|
| http://192.168.182.129:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=change-log.htm&do=toggle-hints%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=change-log.htm&do=toggle-security%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider

|
http://192.168.182.129:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=login.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider

|
http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider

|
http://192.168.182.129:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=credits.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider

|
| http://192.168.182.129:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=login.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=credits.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=home.php&do=toggle-security%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider

|
| http://192.168.182.129:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider
| | http://192.168.182.129:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
| | http://192.168.182.129:80/mutillidae/index.php?page=home.php&do=toggle-hints%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
| | http://192.168.182.129:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
| | http://192.168.182.129:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider
| | http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
| | http://192.168.182.129:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
| | http://192.168.182.129:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
| | http://192.168.182.129:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
| | http://192.168.182.129:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
| | http://192.168.182.129:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
| | http://192.168.182.129:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
| | http://192.168.182.129:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider

|
| http://192.168.182.129:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|
|
http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider

|

http://192.168.182.129:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=register.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider

|

http://192.168.182.129:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider

|

http://192.168.182.129:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider

|

http://192.168.182.129:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider

|

http://192.168.182.129:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider

|
| http://192.168.182.129:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=login.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider

```
|  
| http://192.168.182.129:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspide  
r  
| http://192.168.182.129:80/mutillidae/index.php?page=capture-  
data.php%27%20OR%20sqlspider  
| http://192.168.182.129:80/mutillidae/?page=add-to-your-  
blog.php%27%20OR%20sqlspider  
|  
| http://192.168.182.129:80/mutillidae/index.php?username=anonymous&page=password  
-generator.php%27%20OR%20sqlspider  
| http://192.168.182.129:80/mutillidae/index.php?page=text-file-  
viewer.php%27%20OR%20sqlspider  
| http://192.168.182.129:80/mutillidae/index.php?page=change-  
log.htm%27%20OR%20sqlspider  
| http://192.168.182.129:80/mutillidae/index.php?page=add-to-your-  
blog.php%27%20OR%20sqlspider  
| http://192.168.182.129:80/mutillidae/index.php?page=pen-test-tool-  
lookup.php%27%20OR%20sqlspider  
| http://192.168.182.129:80/mutillidae/?page=login.php%27%20OR%20sqlspider  
| http://192.168.182.129:80/mutillidae/index.php?page=view-someones-  
blog.php%27%20OR%20sqlspider  
| http://192.168.182.129:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider  
|  
| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.  
php%27%20OR%20sqlspider  
|  
| http://192.168.182.129:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspi  
der  
| http://192.168.182.129:80/mutillidae/?page=text-file-  
viewer.php%27%20OR%20sqlspider  
| http://192.168.182.129:80/mutillidae/index.php?page=secret-administrative-  
pages.php%27%20OR%20sqlspider  
| http://192.168.182.129:80/mutillidae/?page=credits.php%27%20OR%20sqlspider  
| http://192.168.182.129:80/mutillidae/index.php?page=set-background-  
color.php%27%20OR%20sqlspider  
| http://192.168.182.129:80/mutillidae/index.php?page=browser-  
info.php%27%20OR%20sqlspider
```

| http://192.168.182.129:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider

|
http://192.168.182.129:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=register.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider

|
http://192.168.182.129:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider

|
http://192.168.182.129:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider

|
http://192.168.182.129:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider

|
| http://192.168.182.129:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=login.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
| http://192.168.182.129:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider

|
| http://192.168.182.129:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|
| http://192.168.182.129:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider

|
http://192.168.182.129:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=rene-magritte.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider

|
http://192.168.182.129:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider

|
http://192.168.182.129:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider

| http://192.168.182.129:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider

|
http://192.168.182.129:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider

```
|  
| http://192.168.182.129:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspide  
r  
| http://192.168.182.129:80/mutillidae/index.php?page=capture-  
data.php%27%20OR%20sqlspider  
| http://192.168.182.129:80/mutillidae/?page=add-to-your-  
blog.php%27%20OR%20sqlspider  
| http://192.168.182.129:80/mutillidae/index.php?page=pen-test-tool-  
lookup.php%27%20OR%20sqlspider  
| http://192.168.182.129:80/mutillidae/index.php?page=text-file-  
viewer.php%27%20OR%20sqlspider  
| Possible sqli for forms:  
| Form at path: /mutillidae/, form's action: ./index.php?page=user-info.php. Fields that  
might be vulnerable:  
|_| username  
|_http-trace: TRACE is enabled  
| http-CSRF:  
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.182.129  
| Found the following possible CSRF vulnerabilities:  
|  
|_| Path: http://192.168.182.129:80/dvwa/  
|_| Form id:  
|_| Form action: login.php  
|  
|_| Path: http://192.168.182.129:80/mutillidae/?page=login.php  
|_| Form id: idloginform  
|_| Form action: index.php?page=login.php  
|  
|_| Path: http://192.168.182.129:80/mutillidae/index.php?page=view-someones-blog.php  
|_| Form id: id-bad-blog-entry-tr  
|_| Form action: index.php?page=view-someones-blog.php  
|  
|_| Path: http://192.168.182.129:80/mutillidae/?page=user-info.php  
|_| Form id: id-bad-cred-tr
```

|_ Form action: ./index.php?page=user-info.php

| http-enum:

| /tikiwiki/: Tikiwiki

| /test/: Test page

| /phpinfo.php: Possible information file

| /phpMyAdmin/: phpMyAdmin

| /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'

| /icons/: Potentially interesting folder w/ directory listing

|_ /index/: Potentially interesting folder

|_http-dombased-xss: Couldn't find any DOM based XSS.

|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

111/tcp open rpcbind

139/tcp open netbios-ssn

445/tcp open microsoft-ds

512/tcp open exec

513/tcp open login

514/tcp open shell

1099/tcp open rmiregistry

| rmi-vuln-classloader:

| VULNERABLE:

| RMI registry default configuration remote code execution vulnerability

| State: VULNERABLE

| Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.

|

| References:

|_ https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb

1524/tcp open ingreslock

2049/tcp open nfs

2121/tcp open ccproxy-ftp

3306/tcp open mysql

5432/tcp open postgresql

| ssl-ccs-injection:

| VULNERABLE:

| SSL/TLS MITM vulnerability (CCS Injection)

| State: VULNERABLE

| Risk factor: High

| OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h

| does not properly restrict processing of ChangeCipherSpec messages,

| which allows man-in-the-middle attackers to trigger use of a zero

| length master key in certain OpenSSL-to-OpenSSL communications, and

| consequently hijack sessions or obtain sensitive information, via

| a crafted TLS handshake, aka the "CCS Injection" vulnerability.

|

| References:

| <http://www.cvedetails.com/cve/2014-0224>

| <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224>

|_ http://www.openssl.org/news/secadv_20140605.txt

| ssl-dh-params:

| VULNERABLE:

| Diffie-Hellman Key Exchange Insufficient Group Strength

| State: VULNERABLE

| Transport Layer Security (TLS) services that use Diffie-Hellman groups

| of insufficient strength, especially those using one of a few commonly

| shared groups, may be susceptible to passive eavesdropping attacks.

| Check results:

| WEAK DH GROUP 1

| Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA

| Modulus Type: Safe prime

| Modulus Source: Unknown/Custom-generated

| Modulus Length: 1024

| Generator Length: 8

- | Public Key Length: 1024
- | References:
 - |_ <https://weakdh.org>
- | ssl-poodle:
 - | VULNERABLE:
 - | SSL POODLE information leak
 - | State: VULNERABLE
 - | IDs: BID:70574 CVE:CVE-2014-3566
 - | The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.
 - | Disclosure date: 2014-10-14
 - | Check results:
 - | TLS_RSA_WITH_AES_128_CBC_SHA
 - | References:
 - | <https://www.securityfocus.com/bid/70574>
 - | <https://www.openssl.org/~bodo/ssl-poodle.pdf>
 - | <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566>
 - |_ <https://www.imperialviolet.org/2014/10/14/poodle.html>
- 5900/tcp open vnc
- 6000/tcp open X11
- 6667/tcp open irc
 - |_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See <http://seclists.org/fulldisclosure/2010/Jun/277>
- 8009/tcp open ajp13
- 8180/tcp open unknown
 - | http-cookie-flags:
 - | /admin/:
 - | JSESSIONID:
 - | httponly flag not set

```
| /admin/index.html:  
| JSESSIONID:  
|   httponly flag not set  
| /admin/login.html:  
| JSESSIONID:  
|   httponly flag not set  
| /admin/admin.html:  
| JSESSIONID:  
|   httponly flag not set  
| /admin/account.html:  
| JSESSIONID:  
|   httponly flag not set  
| /admin/admin_login.html:  
| JSESSIONID:  
|   httponly flag not set  
| /admin/home.html:  
| JSESSIONID:  
|   httponly flag not set  
| /admin/admin-login.html:  
| JSESSIONID:  
|   httponly flag not set  
| /admin/adminLogin.html:  
| JSESSIONID:  
|   httponly flag not set  
| /admin/controlpanel.html:  
| JSESSIONID:  
|   httponly flag not set  
| /admin/cp.html:  
| JSESSIONID:  
|   httponly flag not set  
| /admin/index.jsp:
```

| JSESSIONID:
| httponly flag not set
| /admin/login.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/admin.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/home.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/controlpanel.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/admin-login.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/cp.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/account.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/admin_login.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/adminLogin.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html:
| JSESSIONID:

- | httponly flag not set
- | /admin/includes/FCKeditor/editor/filemanager/upload/test.html:
- | JSESSIONID:
- | httponly flag not set
- | /admin/jscript/upload.html:
- | JSESSIONID:
- |_ httponly flag not set
- | http-enum:
- | /admin/: Possible admin folder
- | /admin/index.html: Possible admin folder
- | /admin/login.html: Possible admin folder
- | /admin/admin.html: Possible admin folder
- | /admin/account.html: Possible admin folder
- | /admin/admin_login.html: Possible admin folder
- | /admin/home.html: Possible admin folder
- | /admin/admin-login.html: Possible admin folder
- | /admin/adminLogin.html: Possible admin folder
- | /admin/controlpanel.html: Possible admin folder
- | /admin/cp.html: Possible admin folder
- | /admin/index.jsp: Possible admin folder
- | /admin/login.jsp: Possible admin folder
- | /admin/admin.jsp: Possible admin folder
- | /admin/home.jsp: Possible admin folder
- | /admin/controlpanel.jsp: Possible admin folder
- | /admin/admin-login.jsp: Possible admin folder
- | /admin/cp.jsp: Possible admin folder
- | /admin/account.jsp: Possible admin folder
- | /admin/admin_login.jsp: Possible admin folder
- | /admin/adminLogin.jsp: Possible admin folder
- | /manager/html/upload: Apache Tomcat (401 Unauthorized)
- | /manager/html: Apache Tomcat (401 Unauthorized)

```
| /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html:  
OpenCart/FCKeditor File upload  
  
| /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog /  
FCKeditor File Upload  
  
| /admin/jscript/upload.html: Lizard Cart/Remote File upload  
  
|_ /webdav/: Potentially interesting folder  
  
MAC Address: 00:0C:29:0B:15:D3 (VMware)
```

Host script results:

```
_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)  
  
_smb-vuln-ms10-061: false  
  
_smb-vuln-ms10-054: false
```

Nmap done: 1 IP address (1 host up) scanned in 329.33 seconds

CVE & CVSS

Com o resultado demonstrado acima conseguimos enxergar de forma clara a extensão e também os diversos vetores de ataques que a máquina vulnerável possibilita por sua ineficiência de tratamento dessas CVE. Para identificarmos agora a classificação para priorização de tratamentos dessas vulnerabilidades utilizamos o CVSS (Common Vulnerability Scoring System), podendo também ser utilizada a calculadora NIST para CVSS ([link da calculadora NIST](#)). Vamos utilizar como exemplo uma das vulnerabilidades expostas na porta 21/tcp que possui o serviço **FTP** aberto, identificada na [CVE-2011-2523](#). A vulnerabilidade já é conhecida e conforme NIST (2011), a versão vsftpd 2.3.4 baixada entre 30-06-2011 e 03-07-2011 possuí uma backdoor que abre um shell na porta 6200/tcp. O score dessa vulnerabilidade é crítico com pontuação 9.8 sendo de extrema importância o tratamento dessa vulnerabilidade.

Description

vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.

Metrics	CVSS Version 4.0	CVSS Version 3.x	CVSS Version 2.0
<small>NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.</small>			
CVSS 3.x Severity and Vector Strings:			
 NIST: NVD	Base Score: 9.8 CRITICAL	Vector: CVSS:3.1/AV:N/AC:L/PR:N/U:N/S:U/C:H/I:H/A:H	

Figura 18 - Descrição da CVE-2011-2523

CVSS v3.1 Severity and Metrics:

Base Score: 9.8 CRITICAL

Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Impact Score: 5.9

Exploitability Score: 3.9

Attack Vector (AV): Network

Attack Complexity (AC): Low

Privileges Required (PR): None

User Interaction (UI): None

Scope (S): Unchanged

Confidentiality (C): High

Integrity (I): High

Availability (A): High

Figura 19 - metrica e severidade da CVE-2011-2523

No site onde você visualiza as informações da vulnerabilidade citada como exemplo, também existe um campo destinado a links importantes dos vendors (fabricantes, produtores, distribuidores etc) para que você possa acompanhar uma solução. Acessando o link do distribuir Debian ([clique aqui para visualizar](#)) podemos visualizar que ele já realizou o reparo na versão 3.0.3-12, sendo dessa forma a possível solução dessa vulnerabilidade.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

URL	Source(s)	Tag(s)
http://packetstormsecurity.com/files/162145/vsftpd-2.3.4-Backdoor-Command-Execution.html	CVE, Inc., Red Hat	
https://access.redhat.com/security/cve/cve-2011-2523	CVE, Inc., Red Hat	Third Party Advisory
https://packetstormsecurity.com/files/102745/VSFTPD-2.3.4-Backdoor-Command-Execution.html	CVE, Inc., Red Hat	Exploit Third Party Advisory VDB Entry
https://security-tracker.debian.org/tracker/CVE-2011-2523	CVE, Inc., Red Hat	Third Party Advisory
https://vigilance.fr/vulnerability/vsftpd-backdoor-in-version-2-3-4-10805	CVE, Inc., Red Hat	Third Party Advisory
https://www.openwall.com/lists/oss-security/2011/07/11/5	CVE, Inc., Red Hat	Mailing List Third Party Advisory

Figura 20 - NIST referências aos distribuidores, soluções e ferramentas

CVE-2011-2523



Name	CVE-2011-2523
Description	vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.
Source	CVE (at NVD ; CERT , ENISA , LWN , oss-sec , fulldisc , Debian ELTS , Red Hat , Ubuntu , Gentoo , SUSE bugzilla/CVE , GitHub advisories/code/Issues , web search , more)

Vulnerable and fixed packages

The table below lists information on source packages.

Source Package	Release	Version	Status
vsftpd (PTS)	bullseye	3.0.3-12	fixed
	bookworm	3.0.3-13	fixed
	trixie	3.0.5-0.2	fixed
	forky	3.0.5-0.3	fixed
	sid	3.0.5-0.4	fixed

The information below is based on the following data on fixed versions.

Package	Type	Release	Fixed Version	Urgency	Origin	Debian Bugs
vsftpd	source	(unstable)	(not affected)			

Notes

- vsftpd <not-affected> (backdoored version was never in the Debian archive)

Search for package or bug name: Go Reporting problems

Figura 21 - Confirmação do tratamento dessa vulnerabilidade pelo Debian

Conclusão

Este laboratório reforça que, mesmo diante de ferramentas avançadas de detecção e resposta, os principais vetores de ataque frequentemente se originam de falhas operacionais: má configuração de serviços, ausência de inventário de ativos críticos, e a falta de acompanhamento sistemático de vulnerabilidades conhecidas (como as listadas em CVEs) e seus respectivos riscos (expressos por meio de pontuações CVSS).

Em outras palavras, a maior lacuna não está na tecnologia, mas na gestão contínua da segurança dos ativos — uma responsabilidade compartilhada entre administradores, gestores de TI e equipes de segurança.