Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 04:54 EDT

Nmap scan report for 192.168.56.5

Host is up (0.0055s 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://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd\_234\_backdoor.rb

| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523

| 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

|\_sslv2-drown: ERROR: Script execution failed (use -d to debug)

| smtp-vuln-cve2010-4344:

|\_ The SMTP server is not Exim: NOT VULNERABLE

| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566

| https://www.securityfocus.com/bid/70574

| https://www.imperialviolet.org/2014/10/14/poodle.html

|\_ https://www.openssl.org/~bodo/ssl-poodle.pdf

| ssl-dh-params:

| VULNERABLE:

| Anonymous Diffie-Hellman Key Exchange MitM Vulnerability

| State: VULNERABLE

| Transport Layer Security (TLS) services that use anonymous

| Diffie-Hellman key exchange only provide protection against passive

| eavesdropping, and are vulnerable to active man-in-the-middle attacks

| which could completely compromise the confidentiality and integrity

| of any data exchanged over the resulting session.

| Check results:

| ANONYMOUS DH GROUP 1

| Cipher Suite: TLS\_DH\_anon\_WITH\_RC4\_128\_MD5

| Modulus Type: Safe prime

| Modulus Source: postfix builtin

| Modulus Length: 1024

| Generator Length: 8

| Public Key Length: 1024

| References:

| https://www.ietf.org/rfc/rfc2246.txt

|

| Transport Layer Security (TLS) Protocol DHE\_EXPORT Ciphers Downgrade MitM (Logjam)

| State: VULNERABLE

| IDs: BID:74733 CVE:CVE-2015-4000

| The Transport Layer Security (TLS) protocol contains a flaw that is

| triggered when handling Diffie-Hellman key exchanges defined with

| the DHE\_EXPORT cipher. This may allow a man-in-the-middle attacker

| to downgrade the security of a TLS session to 512-bit export-grade

| cryptography, which is significantly weaker, allowing the attacker

| to more easily break the encryption and monitor or tamper with

| the encrypted stream.

| Disclosure date: 2015-5-19

| Check results:

| EXPORT-GRADE DH GROUP 1

| Cipher Suite: TLS\_DHE\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA

| Modulus Type: Safe prime

| Modulus Source: Unknown/Custom-generated

| Modulus Length: 512

| Generator Length: 8

| Public Key Length: 512

| References:

| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000

| https://weakdh.org

| https://www.securityfocus.com/bid/74733

|

| 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\_128\_CBC\_SHA

| Modulus Type: Safe prime

| Modulus Source: postfix builtin

| Modulus Length: 1024

| Generator Length: 8

| Public Key Length: 1024

| References:

|\_ https://weakdh.org

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:

| http://ha.ckers.org/slowloris/

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

| http-sql-injection:

| Possible sqli for queries:

| http://192.168.56.5:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?do=toggle-hints%27%20OR%20sqlspider&page=home.php

| http://192.168.56.5:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?do=toggle-security%27%20OR%20sqlspider&page=home.php

| http://192.168.56.5:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider

| http://192.168.56.5:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider

| http://192.168.56.5:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider

| http://192.168.56.5:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider

| http://192.168.56.5:80/dav/?C=N%3BO%3DD%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?do=toggle-hints%27%20OR%20sqlspider&page=pen-test-tool-lookup.php

| http://192.168.56.5:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?do=toggle-security%27%20OR%20sqlspider&page=pen-test-tool-lookup.php

| http://192.168.56.5:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=register.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=register.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?do=toggle-hints%27%20OR%20sqlspider&page=home.php

| http://192.168.56.5:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?do=toggle-security%27%20OR%20sqlspider&page=home.php

| http://192.168.56.5:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?do=toggle-security%27%20OR%20sqlspider&page=change-log.htm

| http://192.168.56.5:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?do=toggle-hints%27%20OR%20sqlspider&page=change-log.htm

| http://192.168.56.5:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=login.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/?page=credits.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider

| http://192.168.56.5:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider

| Possible sqli for forms:

| Form at path: /mutillidae/index.php, form's action: ./index.php?page=user-info.php. Fields that might be vulnerable:

|\_ username

|\_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)

|\_http-trace: TRACE is enabled

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

| 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-csrf:

| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.56.5

| Found the following possible CSRF vulnerabilities:

|

| Path: http://192.168.56.5:80/dvwa/

| Form id:

| Form action: login.php

|

| Path: http://192.168.56.5:80/mutillidae/index.php?page=source-viewer.php

| Form id: id-bad-cred-tr

| Form action: index.php?page=source-viewer.php

|

| Path: http://192.168.56.5:80/mutillidae/index.php?page=login.php

| Form id: idloginform

| Form action: index.php?page=login.php

|

| Path: http://192.168.56.5:80/mutillidae/?page=text-file-viewer.php

| Form id: id-bad-cred-tr

| Form action: index.php?page=text-file-viewer.php

|

| Path: http://192.168.56.5:80/mutillidae/index.php?page=text-file-viewer.php

| Form id: id-bad-cred-tr

| Form action: index.php?page=text-file-viewer.php

|

| Path: http://192.168.56.5:80/mutillidae/index.php?page=user-info.php

| Form id: id-bad-cred-tr

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

|

| Path: http://192.168.56.5:80/mutillidae/index.php?page=html5-storage.php

| Form id: idform

| Form action: index.php?page=html5-storage.php

|

| Path: http://192.168.56.5:80/mutillidae/index.php?page=set-background-color.php

| Form id: id-bad-cred-tr

|\_ Form action: index.php?page=set-background-color.php

|\_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

|\_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)

|\_ssl-ccs-injection: No reply from server (TIMEOUT)

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.openssl.org/news/secadv\_20140605.txt

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

|\_ http://www.cvedetails.com/cve/2014-0224

| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566

| https://www.securityfocus.com/bid/70574

| https://www.imperialviolet.org/2014/10/14/poodle.html

|\_ https://www.openssl.org/~bodo/ssl-poodle.pdf

| 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\_128\_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

5900/tcp open vnc

6000/tcp open X11

6667/tcp open irc

|\_irc-unrealircd-backdoor: Server closed connection, possibly due to too many reconnects. Try again with argument irc-unrealircd-backdoor.wait set to 100 (or higher if you get this message again).

8009/tcp open ajp13

8180/tcp open unknown

| 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

| 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

MAC Address: 08:00:27:A8:C0:29 (Oracle VirtualBox virtual NIC)

Host script results:

|\_smb-vuln-ms10-061: false

|\_smb-vuln-ms10-054: false

|\_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 525.78 seconds